VELS
KNOWLEDGE IS POWER

VELS
INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES (VISTAS)
(Deemed to be University Estd. u/s 3 of the UGC Act, 1956)
PALLAVARAM - CHENNAI
ACCREDITED BY NAAC WITH 'A' GRADE
Marching Beyond 25 Years Successfully

iNURTURE
Education Solutions
TOMORROW'S HERE

Secure File storage using hybrid cryptography

First Review

- **Presented by**

Hamza Mohammed Khan	- 20139129
Arun	- 20139103
Midhunisha	-2019123

Supervisor
Mrs.Sathya.A
[Senior IT Faculty]

ABSTRACT

Hybrid cryptography is a combination of two or more cryptographic techniques to achieve a greater level of security. It is used to protect sensitive data while also ensuring the data is accessible to the intended recipients.

Secure file storage using hybrid cryptography is a method of protecting data by combining public key cryptography and symmetric key cryptography. This ensures that the data is both secure and accessible, making it an ideal choice for many applications.

Introduction

- Hybrid cryptography, as the name suggests, combines different cryptographic techniques or protocols to leverage the strengths of each approach and provide enhanced security for data communication or storage.
- Hybrid cryptography are believed to be resistant to attacks by quantum computers.
- Hybrid cryptography is implementing itself with the quantum mechanics to safeguard and protect systems form the vulnerabilities around.

BLOCKCHAIN

SCOPE

- Blockchain technology: Blockchain is a distributed and decentralized ledger technology that provides transparency, immutability, and security to data transactions.
- Secure Multi-party Computation (SMPC): SMPC is a variant of multi-party computation that focuses on securely computing a function on private inputs from multiple parties.
- Multi-party computation (MPC): MPC is a cryptographic technique that allows multiple parties to securely compute a function over their private inputs without revealing their inputs to each other.

Methodology

Phase1

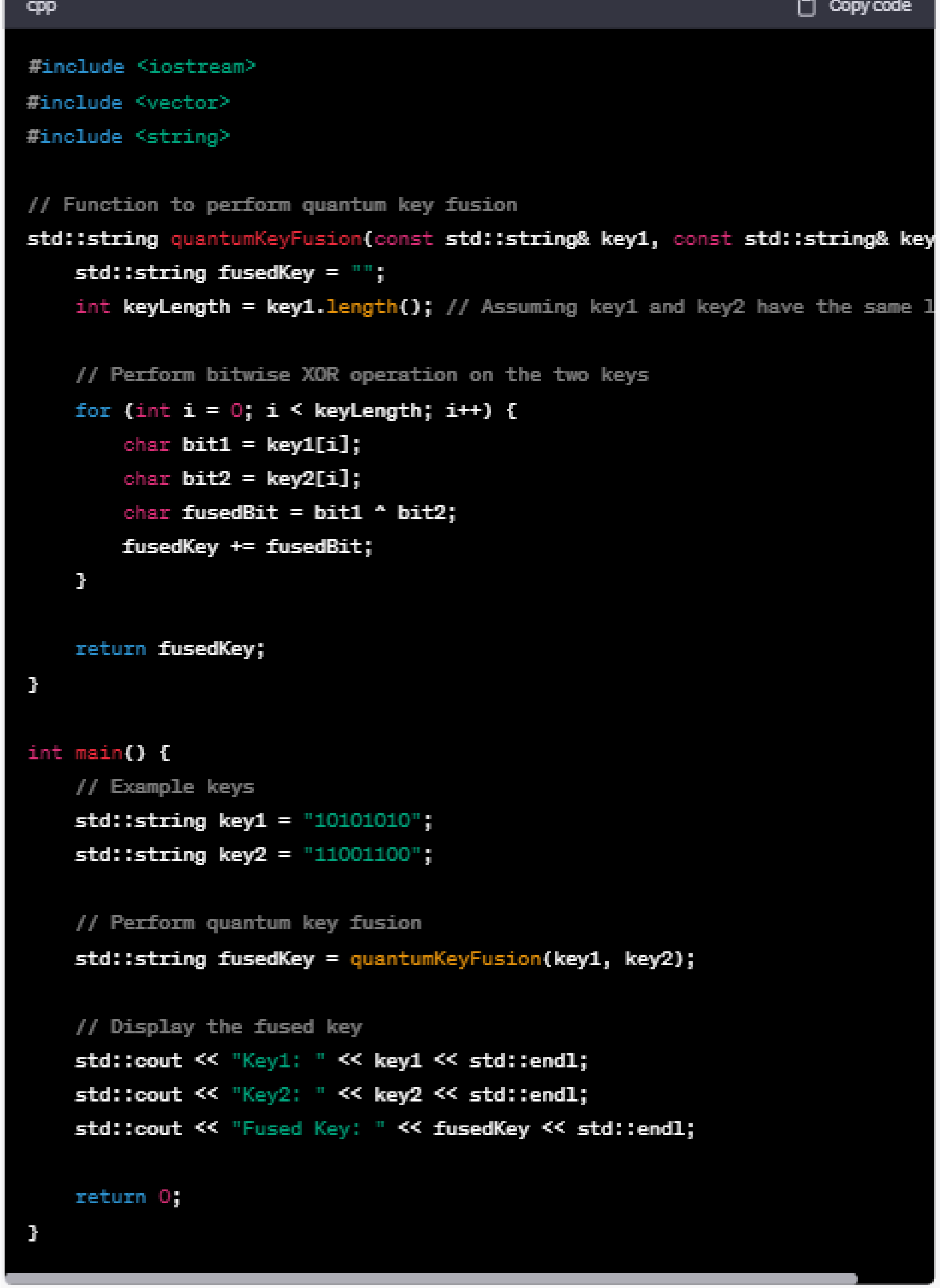
- Encryption
- Key generation: In hybrid cryptography, the first phase involves generating cryptographic keys that will be used for encryption and decryption.

Phase 2

- Key Exchange
- Key distribution: Once the cryptographic keys are generated, they need to be distributed securely to the intended recipients..

Phase 3

- Authentication
- Encryption: With the secure keys in place, the sender uses a classical encryption algorithm to encrypt the data or message using the agreed-upon encryption key



```cpp
#include <iostream>
#include <vector>
#include <string>

// Function to perform quantum key fusion
std::string quantumKeyFusion(const std::string& key1, const std::string& key
    std::string fusedKey = "";
    int keyLength = key1.length(); // Assuming key1 and key2 have the same l

    // Perform bitwise XOR operation on the two keys
    for (int i = 0; i < keyLength; i++) {
        char bit1 = key1[i];
        char bit2 = key2[i];
        char fusedBit = bit1 ^ bit2;
        fusedKey += fusedBit;
    }

    return fusedKey;
}

int main() {
    // Example keys
    std::string key1 = "10101010";
    std::string key2 = "11001100";

    // Perform quantum key fusion
    std::string fusedKey = quantumKeyFusion(key1, key2);

    // Display the fused key
    std::cout << "Key1: " << key1 << std::endl;
    std::cout << "Key2: " << key2 << std::endl;
    std::cout << "Fused Key: " << fusedKey << std::endl;

    return 0;
}
```

EXISTING SYSTEM

- Quantum key distribution is become one of the most advanced technology which is till in implementation and the concepts can be found in science textbooks .

- Cryptography is used to protect data in transit, at rest, and during processing. It is also used to authenticate users and maintain the integrity of data in the existing system

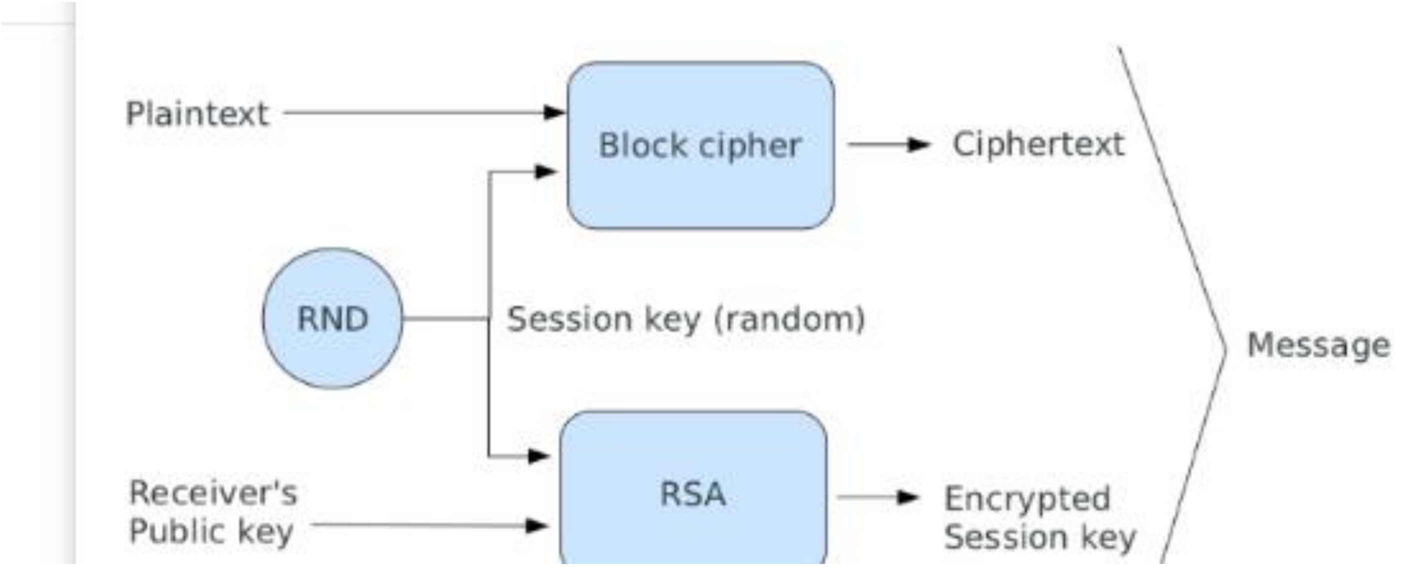
Proposed System

- The Quantum Enigma Cipher is a hybrid encryption scheme that combines principles of quantum mechanics with traditional cryptographic techniques to provide a high level of security against both classical and quantum attacks.
- These algorithms are used in cryptographic software to secure data and communications, and are designed to be difficult to break, even with powerful computers.
- It leverages the properties of quantum entanglement and superposition to create a unique encryption mechanism.

Tools Used

- Quantum Key fusion.
- Docker
- QEKG (Quantum enhanced key generation.
- Quantum Hybrid Key Generator
- Quantum Computers and Cryptography.
- QKV Quantum Key Verification
- Hybrid Key Generator

Architecture Diagram



Future Work

1. Post-quantum hybrid cryptography
2. Efficiency improvements
3. Scalability and adaptability
4. Security analysis and formal proofs
5. Standardization and interoperability
6. Usability and user experience

Conclusion

- The concepts which were discussed above are in the implementation stage and will be launched in the next 10 years depending on the success rate of the products. The quantum mechanics is a very advanced implementation technique which can only be discussed in books or by authors but the implementation might cost them billions of dollars. The future is here but at what is cost is the biggest question mark. But once implemented it could be a revolutionary idea which will change the way in which the information technology sector functions.

THANK YOU