JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution

[1]Princy Kshirsagar, [2]Ritesh Gangurde
[1]Student, [2]Student,
[1]SOE (ADYPU)
[1] Ajeenkya DY Patil University, Pune, India

Abstract : **As we move further into the era of digital transformation, cloud services are becoming a cornerstone across industries such as healthcare, agriculture, and Industry 4.0. These sectors increasingly rely on cloud environments to collect, process, and store vast amounts of data, often integrated with smart devices. While ensuring high availability and efficiency remains vital, the paramount concern is maintaining data security. This challenge becomes even more pressing in a world where quantum computers pose a serious threat to traditional cryptographic methods. Classical encryption schemes, particularly those relying on computational hardness assumptions, are susceptible to quantum attacks. This paper proposes a solution by combining the theoretically unbreakable One-Time Pad (OTP) encryption with quantum-safe key exchange protocols. Through the integration of Quantum Key Distribution (QKD) and post-quantum cryptographic techniques, we outline a robust framework designed to secure communication in the coming quantum era.**

Index Terms **– QKD, Cloud services, Cryptography, Quantum Computing.**

I. INTRODUCTION

The hastiest advancement in quantum computing puts at risk the traditional foundational methods of cybersecurity infrastructure. Security mechanisms that are quantum-resistant are imperative alongside the impending threats that Shor's algorithm poses to RSA and ECC encryption by factoring large numbers rapidly, as well as Grover's algorithm which accelerates brute force attacks. Quantum computing takes advantage of the principles of quantum mechanics. It utilizes a qubit which can inhabit the state of superposition where it is 0 and 1 at the same time as well as entanglement which allows one qubit's state to be connected to another, regardless of how far apart they are. Our goal is to advance protocols in order to defend against these threats, and lay a strong foundation for quantum-proof communication. We present a definitive answer through the application of One-Time Pad with BB84 Quantum Key Distribution (QKD) protocol. The One-Time Pad is theoretically secure if it is used correctly — meaning a truly random key of equal length to the message and used just once. The cryptographic challenge lies in sharing the keys securely. This is where BB84 protocol comes in, utilizing quantum superposition and entanglement. Merely trying to eavesdrop on the key exchange would disrupt the quantum states, which will signal the communicating parties.

II. BACKGROUND

2.1 Quantum Computing Threats

Quantum computing will create significant security problems by breaking the RSA and ECC methods of encryption if they are indeed developed, which could undermine data privacy as well as PKI (Public Key Infrastructure) and digital signatures. This threatens blockchain, cryptocurrencies, and secure communications techniques with wide repercussions in areas such as national security, business competition secrets, etc. To mitigate those risks requires the development and use of quantum-resistant cryptographic algorithms, international cooperation at an unprecedented scale, as well as significant funding for research done so far in security biosecurity resilience program priorities (planetary cyber- physical systems) enriched with greater public awareness-raising capacity.[5]

2.2 AWS Braket

AWS Braket is a managed quantum computing service by Amazon Web Services, offering access to quantum computers and simulators from providers like D-Wave, IonQ, and Rigetti. It supports hybrid algorithms that combine classical and quantum computing, integrates with other AWS services, and provides SDKs and tools for developing quantum programs. Key use cases include optimization problems, machine learning, cryptography, and material science. Users can start by creating an AWS account, accessing the Braket console, developing quantum programs using the Braket SDK, and running them on quantum hardware or simulators, with results monitored and stored using AWS services.[23]

2.3 One- Time Pad (OTP)

One-time pad is a secure key to protect classified information also called Vernam cipher. This technique proposed by Frank Miller and Gilbert Vernam. In this technique the length of secret key (pad) and plaintext message is equal. Previously OTP is used

only once and random. One-time-pad quantum key cannot be copied, or eaves rapped. But in quantum era, random OTP can be use repeatedly as long as there is no eavesdropped. An OTP needs a key that is truly random, at least as long as the message is used only once.[6]
Alice and Bob are secret agents who wish to communicate a message to each other using a one-time pad. They meet in person to agree on a random key "XMCKL" to be used once. Alice encrypts the message. "HELLO" by changing the letters into number values, adding the key numbers, and obtaining the result "EQNVZ," which she sends to Bob. Bob decrypts "EQNVZ" by subtracting the key numbers from the ciphertext to obtain the original message "HELLO.". Given that the key is random, secret, and used only once, this process will assure perfect secrecy.[6]

2.4 Quantum Noise

One application of quantum noise, or quantum randomness, is the generation of keys for a one-time pad encryption scheme by the intrinsic indeterminacy of quantum processes for true randomness. A quantum random number generator generates a random binary sequence from quantum phenomena, such as the measurement of photon polarization. It is this sequence that makes it perfect secrecy if each bit of the plaintext is exactly X-ORed with the key bit to get ciphertext. This very key is used in decrypting the same data, just by simple reversal of the XOR operation. The use of quantum noise sources for OTP keys combines the absolute security of the one-time pad with the real, true randomness brought about by quantum indeterminacy.[7] Nevertheless, the creation of some form of distribution method for this might be inefficient. Quantum key distribution protocols, among which is BB84, reduce this problem.[24]

III. Related Work

3.1Quantum key Distribution (QKD)

Quantum Key Distribution uses the laws of quantum physics to establish safe keys. Some of the most famous QKD protocols are BB84 Protocol: Andrew Bennett and Gilles Brassard proposed this quantum protocol in 1984. If someone tries to eavesdrop, the quantum states change and it is plain that somebody has been listening. E91 Protocol - Quantum entanglement proposed by Ekert in 1991. The entangled states help to detect any measurement by an eavesdropper. [8]

3.1.1 Key Exchange Protocols with QKD

This section of the research paper delves into two pioneering QKD protocols: BB84 and E91, both of which illustrate the unique capabilities and challenges of quantum cryptography. BB84's reliance on polarization states and Heisenberg's Uncertainly Principle provides a practical and well-understood method of key- distribution. In contrast, the E91 protocol's use of entanglement and Bell's theorem offers a more theoretically robust approach with greater implementation challenges.

3.1.1.1 BB84 Protocol

They will have to generate some random key: Alice and Bob achieve it using BB84, *K* K The nature of the protocol makes sure that all forms of eavesdropping are discovered

Key Verification: Post keys generation, Alice and Bob deploy a verification step to hold the security of each of their key [8].

3.2 Hash-Based Cryptography

Hash-based cryptography utilizes cryptographic hash functions to construct secure digital signatures and other primitives. The Lamport signature scheme is a notable example of a one-time signature scheme. Hash- based cryptography is valued for its strong security proofs and quantum resistance.[11] Nonetheless, it faces challenges such as large key and signature sizes and limited scalability, especially for schemes like the Merkle-Winternitz OTS.

IV. Methodology

4.1 Existing System

- Most cryptographic systems are based on PRNGs that generate keys and other cryptographic parameters. They are not truly random but deterministic; however, they are designed with the goal of providing an approximation of randomness good enough for all practical purposes.

- It means that pseudo-random key generation is applied to most systems requiring secure encryption. This includes symmetric encryption, for example, AES; public key infrastructure, for example, RSA; VPNs, for example, IPsec and SSL/TLS; wireless security, for example, WPA2; disk encryption, and BitLocker. Other examples include secure messaging, for instance, Signal Protocol; two-factor authentication, like TOTP; cloud security, for example, AWS KMS; blockchain and cryptocurrencies, particularly wallet key generation; and lastly, in secure software development specifically code signing. Therefore, these systems are dependent upon PRNGs to generate keys that will enable data and communications confidentiality, integrity, and authenticity. [21]

- The limitations to PRNGs, therefore, are in their determinism, dependency on a seed that is expected to be secure and unpredictable, and the finiteness of the period that allows repetitions of the sequence. Bias can also be present in the output, and attacks are possible, particularly if either the algorithm or seed is compromised. Moreover, PRNGs do not produce real randomness; it is less appropriate in high-security applications, where one would want either a cryptographically safe pseudo-random number generator or a real non-deterministic random number generator.

4.2 Security Flaws

4.2.1 DUHK Attack

- DUHK (Don't Use Hard-coded Keys) assault on WPA2, where hardware sellers have utilized a hardcoded seed key for ANSI X9.31 RNG algorithm [19], expressing "an aggressor can constraining decode information to find the rest of the encryption parameters and derive the master encryption key used to secure web sessions or virtual private network (VPN) associations.

4.2.2 Japanese PURPLE Cipher Machine

• One well-known case is that during the Second World War, Japan had used a cipher machine for diplomatic communications, which the United States was able to break and read its messages; probably mostly since the "key values" used were insufficiently random. [18]

4.3 Proposed Experiment Framework

- We give an entirely different framework, one that consists of the following components: random key generation using AWS Braket, one-time pad using ANUQRNG as a third-party alternative for true random number generation which will be then used as a key encryption, and BB84 protocol for secure key distribution. This framework combines quantum computing with classical cryptographic techniques to help improve the security of the outcome: a robust quantum platform for the generation of perfectly random keys, a one-time pad enabling perfect secrecy and hence unbreakable encryption, and BB84 for secure key exchange and detecting any eavesdropping attempts due to the peculiarities of quantum principles.

4.3.1 Random Number Generation

- AWS Braket is the quantum computing platform from Amazon Web Services that enables the design, testing, and running of quantum algorithms on a variety of quantum processors, including those based on gate-based quantum computing. It gives access to quantum computers by different vendors and simulators to explore quantum computing concepts and develop quantum algorithms.[24] AWS Bracket uses noise- based randomness. In the context of quantum computing, "noise" may refer to the basic uncertainty in the measurement of quantum mechanics. This in turn can be used as a source of randomness in generating cryptographic keys and would be fundamentally different from classical pseudo-random number generation.

4.3.2 Generating Quantum Circuits with a Hardware Circuit

- AWS Braket enables the construction of quantum circuits that run on a hardware quantum processor. One might
- design two different quantum circuits, each processing the qubits in some distinct fashion. These circuits could be created to produce a pair of quantum states that are weak or poor in some sense, and the aim is to enhance or "amplify" the result into a more useful or stronger quantum state.

4.3.3 Designing Two Quantum Circuits:

- Circuit 1: This could be a simple quantum circuit that initializes qubits into a superposition state. For example, applying a Hadamard gate to each qubit will create a superposition where each qubit has an equal probability of being in state $|0\rangle$ or $|1\rangle$.

- Circuit 2: This circuit might apply additional gates, such as controlled-NOT (CNOT) gates or phase gates, to entangle the qubits or introduce specific correlations between them.

- These two circuits generate a "weak" string of qubits—a quantum state that has not yet reached its full potential in terms of coherence, entanglement, or information content.

4.3.4 Strengthening the Weak String with a Toeplitz Matrix

- One of the common techniques to convert this weak string of qubits into a "strong" string is by a Toeplitz matrix. The Toeplitz matrix is a structured matrix in which each diagonal descending from left to right is constant; it can be used in quantum error correction processes and randomness extraction.

- Toeplitz Matrix Randomness Extraction: This technique extracts good quality randomness from a weak quantum string. A Toeplitz matrix, multiplied by a weak qubit string, "spreads out" the randomness in it, making the resulting qubit string stronger; it has some properties much closer to cryptographic applications and thus closer to being a truly random string. The Toeplitz matrix could also be part of a quantum error correction scheme that provides an enhancement of the fidelity of the quantum state, in a way that assures protection from noise and potential errors on the qubit string.

- Since generating keys on AWS Braket can be costly, we explored alternative options and utilized the ANUQRNG as a more economical third-party solution for true random number generation which will then be used as a key for the encryption of the message.

4.4 ANUQRNG

- The Australian National University Quantum Random Number Generator realizes the real random numbers based on the principle of quantum vacuum fluctuations, one of the fundamental quantum processes. Different from pseudo random number generators, the random light intensity is detected with photodiodes, which truly offers its real randomness in the ANUQRNG. Hence, this device is suited for the purposes of cryptography, scientific research, and those demanding premier-quality randomness. Today, these numbers can be found online and are quite vital for the purpose of ensuring security and guaranteeing correctness in several digital and computational systems.[22]

- By doing so with ANUQRNG, we remove the limitation restricted in AWS Braket on the number of keys to be generated. ANUQRNG provides a continuous and cost-effective source for the production of a supply of true random numbers, underpinning an unlimited quantity of possible symmetric encryption keys. This improves the scalability and flexibility of secure communication systems, ensuring that key generation is not constrained by any computational or resource limits that might previously have been encountered with quantum computing platforms like AWS Braket.

4.5 One-time Pad

- The one-time pad is an encryption method that achieves perfect secrecy by using a truly random key that is as long as the message and used only once. Each bit of the plaintext is combined with the corresponding bit of the key using XOR or modular addition to produce ciphertext, which can be decrypted by reversing the process with the same key. While it offers unbreakable security if the key is random, secret, and used only once, its practical challenges include the difficulty of key distribution and management, making it less practical for most applications compared to other encryption methods.[6]

- We have used HMAC or Keyed-Hashing for Message Authentication, which will enhance your secure transmissions and provide data integrity and message authenticity through hash functions and a secret key. HMAC verifications prevent tampered data and confirm the message source within protocols like FTPS, SFTP, and HTTP

4.6 HMAC

- Data integrity checks are integrally linked with secure communications. They allow parties that communicate with each other to verify the integrity and authenticity of messages they receive. In secure file transfer protocols such as FTPS, SFTP, and HTTPS, data integrity/message authentication is attained via a mechanism called HMAC—Hash-based message authentication code.[25]

4.7 Quantum Key Distribution

- The key distribution is done by using the BB84 Protocol, the BB84 protocol details quantum key distribution and shares a cryptographic key between two parties: a sender and a receiver. Alice randomly prepares qubits in one of the two possible bases and sends them to Bob, who randomly measures these qubits in his bases. They would then classically compare their bases and would discard any nonmatching pairs. The remaining bits keep as their shared key. Security of BB84 follows from the fact that any

- eavesdropper trying to intercept the qubits would introduce detectable errors due to the disturbance of quantum states.[26] The following is the process of BB84:

    a. Alice generates a random string of bits, and, correspondingly, for each bit, randomly selects a basis in which to encode it.

    b. Alice encodes the bits onto the qubits according to her chosen bases and sends the qubits through a quantum communication channel to Bob's quantum computer.

    c. Bob randomly selects a basis to decode each qubit in. He measures the qubits in his chosen bases.

    d. Alice classically communicates to Bob the choice of the bases she used; she also communicates the values of the first few bits she sent.

e. Bob measures these first few bits to get an estimate of whether Eve has tapped into their quantum communication channel and intercepted Alice's qubits.

f. If Eve didn't intercept the qubits, they take all of the qubits that they happened to have picked the same polarizations for and use those bits as their key. If Eve did intercept the qubits, they repeat the process all over again. However, there are certain requirements for this protocol to work:

1. A private quantum computer is required both for Alice and Bob.

2. They must be linked by a channel through which qubits can be transmitted. It could be some kind of fibre-optic cable that transmits polarized photons.

3. They must be connected by a classical communication channel (e.g. a telephone cable). As perfect security can never be assumed, it should be assumed that any of these channels will be tapped by Eve the Eavesdropper.

V. IMPLEMENTATION

• Implementing OTP using quantum key distribution (QKD) principles on AWS Braket provides a modern approach to leveraging quantum computing for secure communication. AWS Braket is a fully managed quantum computing service that provides a development environment for building quantum algorithms. AWS Braket enables the simulation and execution of quantum algorithms on various quantum processors, including gate-based and annealing quantum computers. This section outlines the steps to simulate a one- time pad encryption system using AWS Braket, focusing on quantum principles for key generation and secure communication. AWS Braket generate random keys using noise in quantum computers, along with an alternative option of utilizing the ANUQRNG as a more economical third-party solution for true random number generation than AWS braket. Furthermore, we use BB84 protocol for key distribution completing the framework for a secure communication system

5.1 Random Key generation using AWS Braket

- We can design a quantum circuit with entangled state preparation and measurements. You can do this using Braket Python SDK.
- Execute: Optionally, execute the quantum circuits on a Braket state simulator or devices you have access to.
- Analysis of Result: Fetch and analyze the result to create one-time key.

5.2 One-Time Pad Encryption

- It is important that the length of a key should be at least equal to the text which requires encryption. Encryption Process: XOR the plaintext message with one-time key to produce the ciphertext.
- For the decryption process reverses this: the receiver XORs back with the same one-time key to recover

- plaintext.

5.3 Key Distribution using BB84 Encryption and Decryption Process Preparation and Transmission:

Quantum Bits (Qubits): Alice prepares a series of qubits, each in one of four possible polarization states:

0° (|0⟩), 90° (|1⟩), 45° (|+⟩), and 135° (|−⟩). These states are represented in two bases: the rectilinear basis (0° and 90°) and the diagonal basis (45° and 135°). Random choice: Alice chooses the basis randomly for each qubit and transmits the qubits to Bob through a quantum channel. Measurement: Random Initial Basis: Alice randomly selects an encoding basis (rectilinear or diagonal) but refuses to tell Bob which one she used. Measurements: Bob measures the qubits and records what he measured as well as which bases were used. Basis Reconciliation: Public Discussion (bases): Alice and Bob publicly reveal the bases they selected for each qubit (excluding measurement outcomes) via a classical channel Matching Bases - They take results only from the same bases and discard those with different ones. Key Sifting: Raw Key: The identical raw key shared by Alice and Bob is formed with the measurement outcomes matched. Error Correction and Privacy Amplification: During error correction, Alice and Bob use their generated raw keys to correct any errors between their keys due to Quantum Noise or Mismatch at measurement side. Privacy Amplification - They utilize privacy amplification methods to decrease any potential partial information an eavesdropper (Eve) may have acquired, which in turn reduces the long final key into a shorter highly secure one. Encrypting and Decrypting the Key Encryption: And as soon as Alice and Bob are successful in generating the shared secret key via BB84 protocol, then finally Alice can encrypt her message using classical encryption algorithm - here One-Time Pad (OTP). In OTP, Alice XORs each bit of her plaintext with the corresponding bit from collectively agreed key to get ciphertext. Decryption: Bob receives the ciphertext and decrypts it using that exact same shared secret key. In case of OTP, Bob is brute-forcing each bit of ciphertext with each corresponding bit in shared key to obtain original message.

VI. RESULT

In this Section, we present the results of implementing a quantum safe communication system using a onetime pad combined with BB84 quantum key distribution protocol. The BB84 protocol, combined with a one-time pad, gives a secure and efficient method for the protection of communication systems against quantum computing advances in the future. Future work will focus on optimizations in the efficiency of such protocols and their real-world communication network applications.

6.1 Random Key generation

We used AWS Braket to generate random key using quantum circuits designed to tap into quantum properties such as superposition and entanglement. Quantum circuits designed to exploit these quantum properties have been created in order to obtain high-quality random bits, which are at the very heart of secure key generation and cryptographic applications.

Figure 1

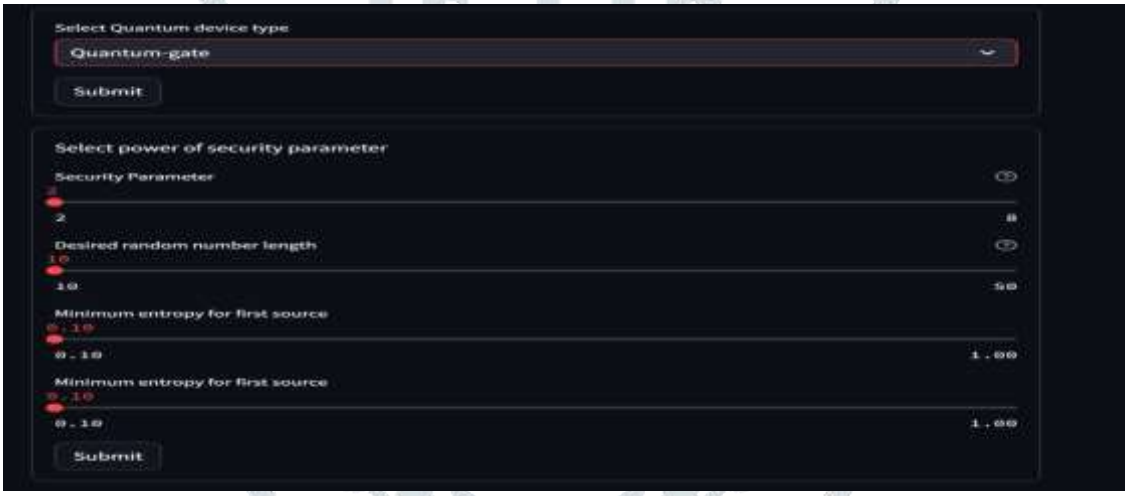

Figure 2.

The Quantum Device type has 2 Quantum Device type

1. Quantum gate – Quantum Computers
2. Classic gate – Local System

Figure 3.

- **Results** Figure 2: Random bit sequences that were the outcome from the quantum circuits run on AWS Braket. In detail, it generated random bit sequences with a very high degree of unpredictability and entropy. The randomness of the generated sequences was checked by deeper statistical tests, which showed the results to be quite close to the true randomness. This strongly suggests that the quantum-generated numbers are highly suitable for cryptographic use.
- **Analysis** By using AWS Braket in random number generation, the inherent indeterminism of quantum processes is used to obtain a robust randomness source against classical methods. Such created random numbers are safe against classical predictability techniques and even quantum attacks; hence, they are appropriate for encryption keys and many other cryptographic applications. This makes the quantum computing functionality of AWS Braket integrate to present a promising approach in producing true random numbers, so bolstering secure communication systems in the quantum era.

6.2 One-time pad Encryption

We implemented a one-time pad encryption scheme, using ANUQRNG to generate a truly random key. This technique is theoretically unbreakable if the key is perfectly random, the message is never reused, and it is used only once. We encrypted the message into ciphertext by performing bitwise modulo 2 addition between the plaintext and the key, which we could transmit securely to the recipient.

Encryption :

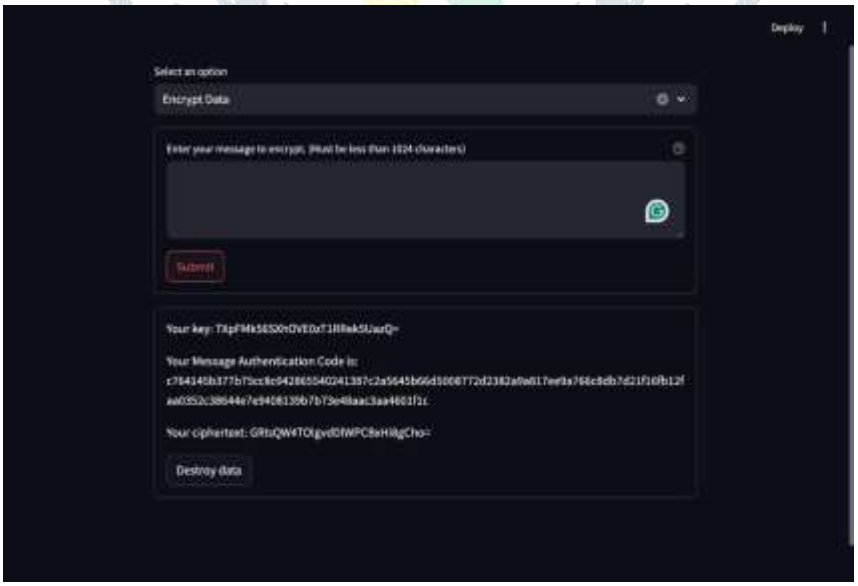

Figure 4.

The Key used is generated by ANUQRNG, then this key is used to encrypt the message along with a message Authentication code.

Decryption:

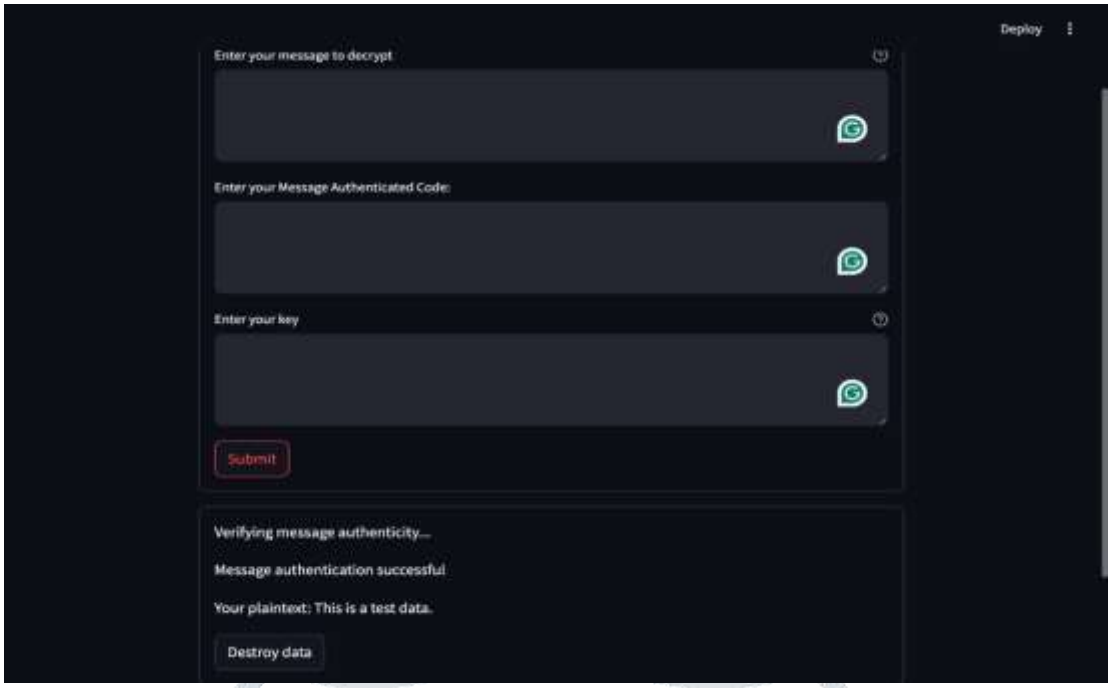

Figure 5.

Results:

As shown in Figure 4, the result of the encryption process was totally incomprehensible random ciphertext; without the key, it could not be deciphered. The decryption process returns the plaintext to its original form, thus evidencing once more the reliability and efficiency of the one-time pad with a securely distributed key.

Analysis:

The one-time pad, along with the key generated by means of ANUQRNG, is resistant to both classical and quantum attacks. In the case of a one-time pad, when the key is never used more than once and never exposed to the communicating parties, it provides unbreakable encryption. Thus, with this principle, highsecurity communications in the quantum era are ensured, and a future-proof solution against emerging threats is provided.

6.3 Key-Exchange Process (BB84)

The basics of quantum mechanics are used by the BB84 protocol for the secure distribution of cryptographic keys between the two parties, normally called Alice and Bob. In this way, any attempt to intercept the key will introduce anomalies detectable by both parties, warning them of an eavesdropper.

Generating random quantum bits for alice which will serve as our keys.

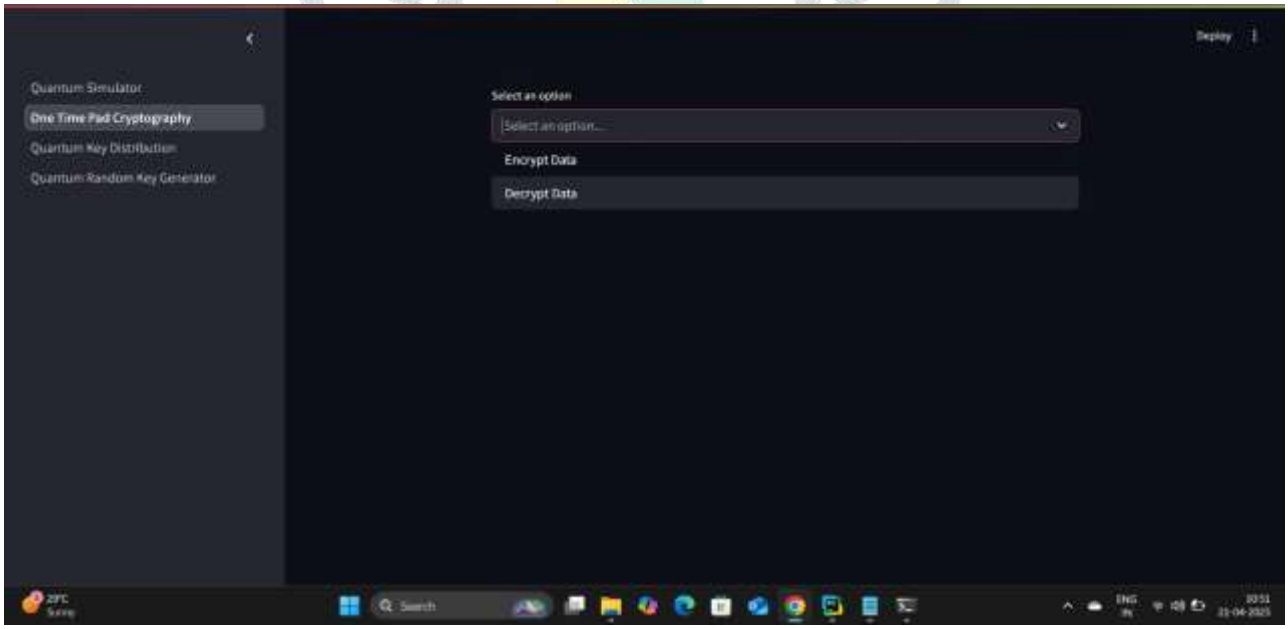

Figure 6

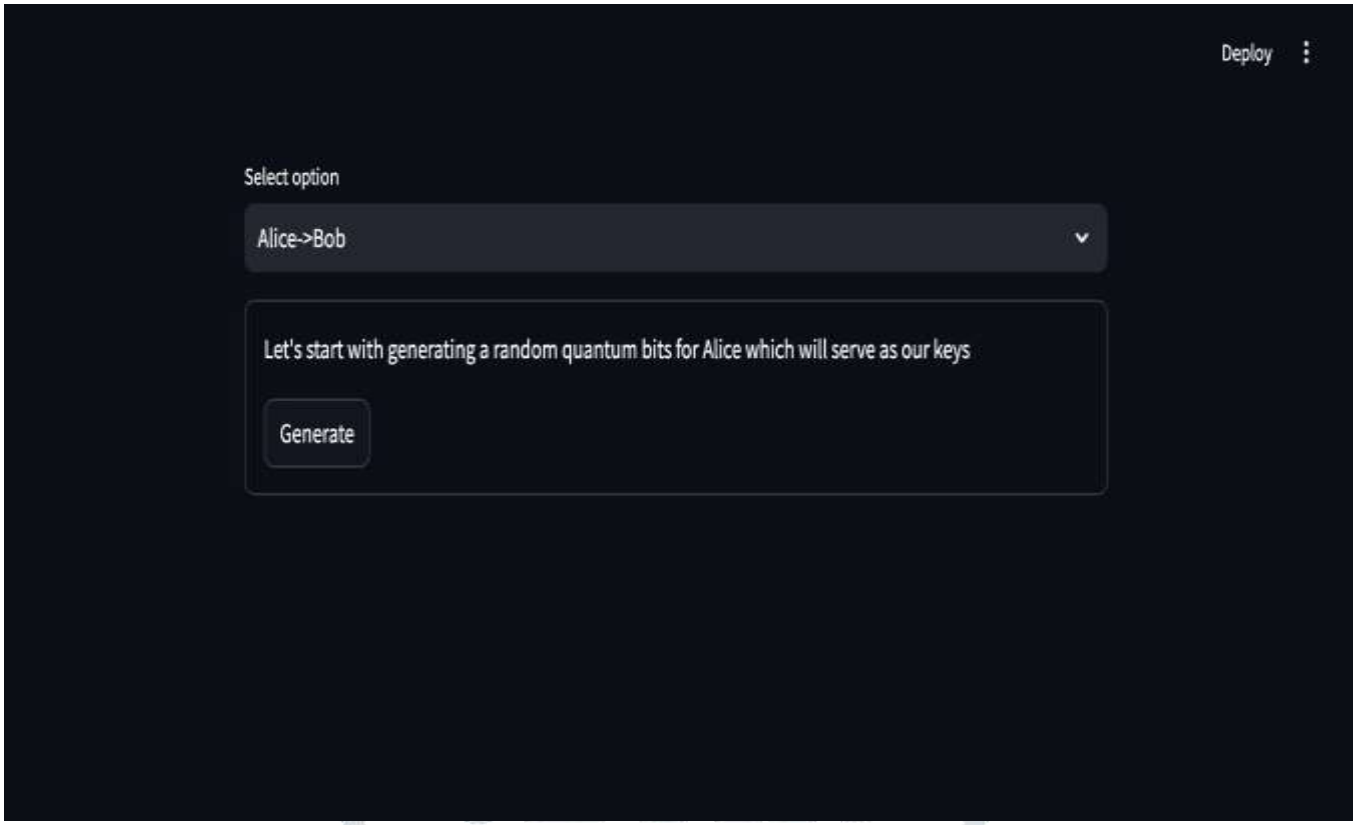

Figure 7.

Alice randomly chooses of each bit (either the Z-basis or the X-basis). She can do this by flipping a coin and mapping each landing (heads or tails) with either one of the basis. But for our use case we are using a random number generator.

The random output bits and bases

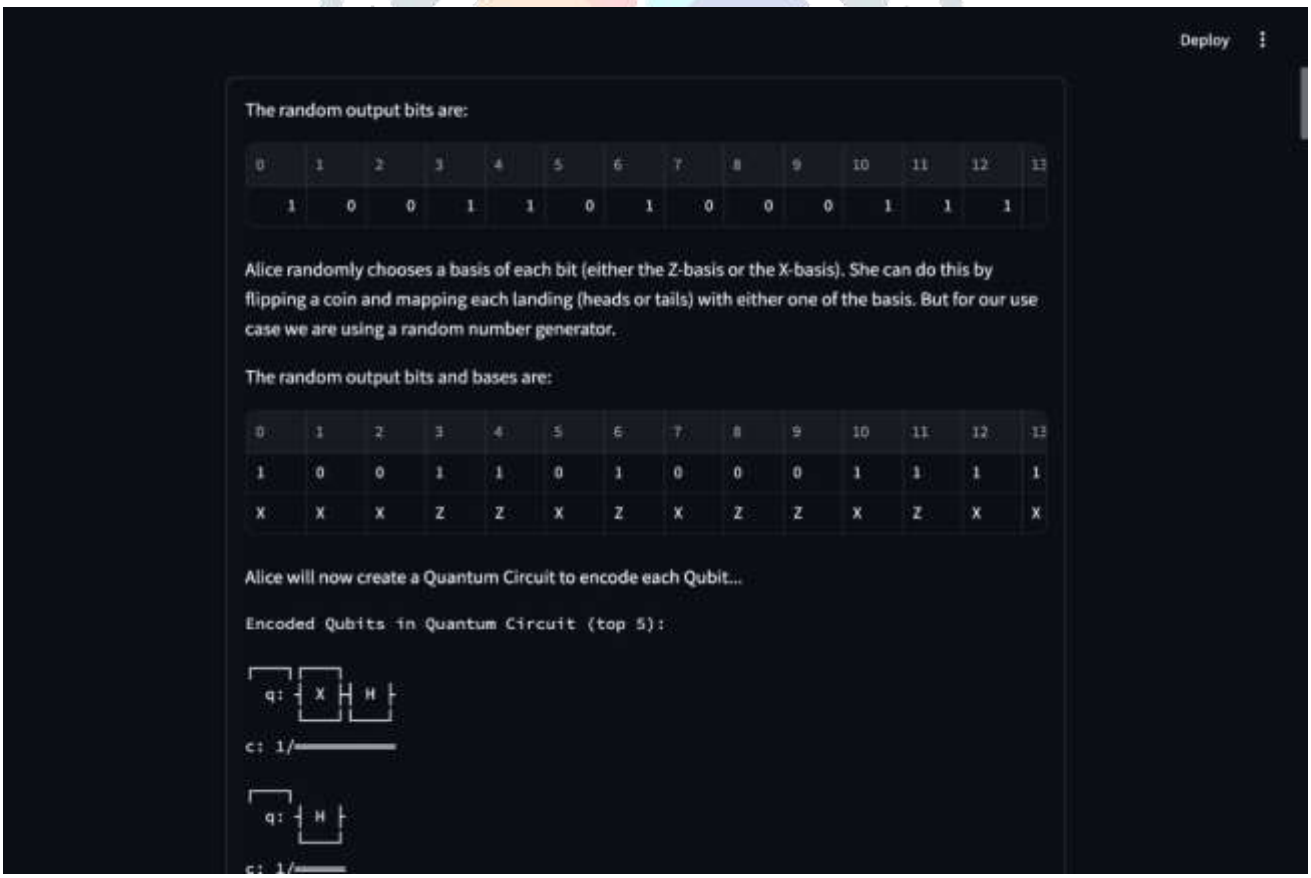

Figure 8 .

Alice will now create a Quantum circuit to encode each Qubit.

Figure 9 .

Generate Random bases for Bob and then comes the verification part. Alice announces the bases she used over a Classical Channel. Both Bob and Alice only keep the bases they share in common.

The indices of the first 10 bases they share in common are :[4, 6, 7, 10, 11, 15, 16, 18, 19, 20]

Figure 10 .

Alice and Bobs first 10 bits.

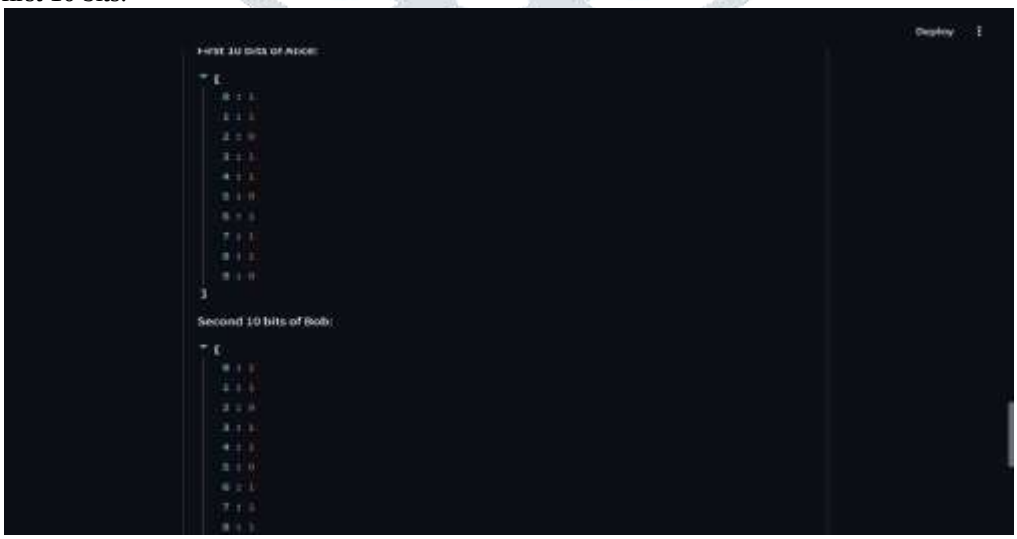

Figure 11.

Alice and Bob Seem to have the same bits. Since they publicly they have to be discarded. The final remaining key with them are:

Figure 12.

Results:

The successful implementation of the **BB84 Quantum Key Distribution (QKD) protocol** indicates that the key exchange between the two communicating parties—Alice and Bob—was completed without any detectable interference. During the comparison phase, Alice and Bob revealed a subset of their chosen bases and corresponding bits over a classical channel. The absence of discrepancies in these revealed bits strongly suggests that there was no eavesdropping attempt (such as from a third-party adversary like Eve) on the quantum channel.

This seamless comparison phase is critical. In BB84, any attempt by an eavesdropper to intercept and measure the quantum bits (qubits) would inevitably introduce errors due to the **no-cloning theorem** and the **uncertainty principle** in quantum mechanics. These errors would manifest as mismatches in the subset of bits that Alice and Bob compare. The fact that no such anomalies were detected validates the **integrity and confidentiality** of the exchanged key.

As a result, the final key—comprising the bits corresponding to the positions where Alice's and Bob's bases matched—is considered secure and valid. This key is derived exclusively from qubits measured using the same bases and was never publicly disclosed in full, preserving its secrecy.

Thus, the final key serves as:

- **A shared secret** known only to Alice and Bob.
- **A secure foundation** for subsequent encryption using the One-Time Pad.
- **Proof of channel integrity**, as no tampering or measurement disruption was identified.

6.4 Security Features

Because of the NO-Cloning Theorem of Quantum Mechanics, Eve cannot copy the Qubits over from the quantum channel. Thus, Bob will never receive the qubits, making it obvious to him and Alice that their message was intercepted. To prevent them from realizing what has happened, Eve must create her own decoy qubits to send to Bob

Tampered Encoded Qubits (by Eve):

Figure 12.

No-Cloning Theorem: The quantum no-cloning theorem prevents an eavesdropper from creating perfect copies of the transmitted qubits, ensuring that any eavesdropping attempt introduces detectable anomalies.[13]

The Qubits are intercepted by Eve. The bases and bits intercepted by eve:

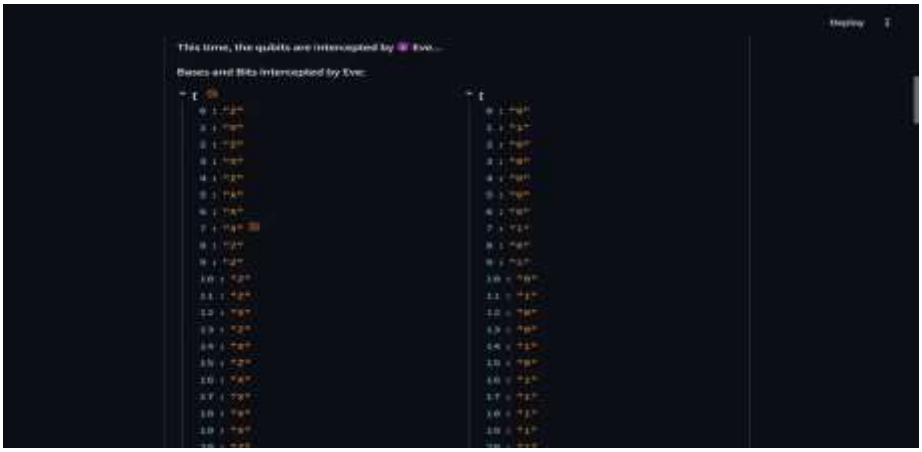

Figure 13.

The tampered qubits now is being received by Bob. Unbeknownst, he carries on with the usual procedure.
The random bases of Bob:

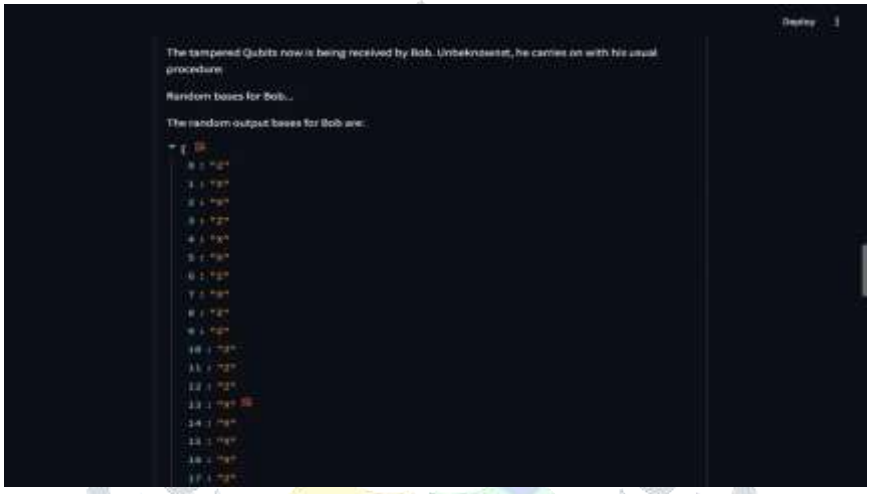

Figure 14.

The bits are received by Bob. Alice announces her bases she chose to encode her qubits in, Bob and Alice again only keep the bits corresponding to their common bases and discard the rest.
The first 10 bits of Alice and Bob:

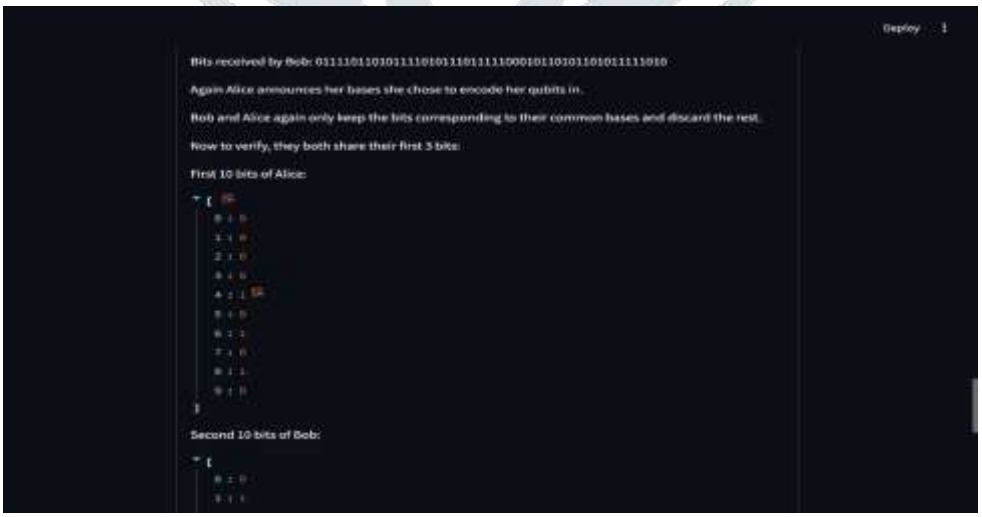

Figure 15.
At least one bit is different. The remaining key received by Bob and Alice also would not match.

Figure 16.

Detection of Eavesdropping: Any attempt by Eve to intercept and measure the qubits will disturb their quantum states, introducing detectable errors in the key reconciliation process. If the error rate exceeds a certain threshold, Alice and Bob can infer the presence of an eavesdropper and abort the key generation process.

Security Analysis

Theoretical Security

Security Analysis Combined Approach: The security of this method depends on the strength of the key exchange protocol used. QKD allows anyone to easily verify whether eavesdropping has occurred or not so long as there is no practical means by which a hacker with physical access could possibly defeat the trust link. It prevents the data against quantum attacks with mathematical problems are generic difficulty for Quantum computing, this is known as post-quantum cryptographic techniques.

Practical Security Considerations

Practical Considerations Key Management: Key management and storage must be efficient. Keys should not be stored in Mac or PC; if we can create keys with proper management so that the key does not reuse, else it would take a 10-20 minute to hack every-time when mac is unlocked. You will need special hardware to generate and detect quantum states, which you can regard as some sort of infrastructure. Infrastructure - QKD requires particular equipment for generating and detecting quantum states; this could be quite expensive in practice Scalability: Post-quantum cryptographic algorithms provide much greater scalability than QKD, which will need to be deployed ubiquitously for post quantum resilience.

Integration with Existing Systems

To ensure the effectiveness of new cryptographic systems, they must be compatible with existing infrastructure and protocols, necessitating careful integration and transition strategies for post-quantum algorithms. Usability is crucial, as cryptographic solutions must be user-friendly and not overly complex for end-users and administrators. Key management involves secure storage of cryptographic keys and efficient methods for key distribution, rotation, and revocation. Protection against side-channel attacks, which exploit physical or implementation weaknesses, is essential. Additionally, it is important to consider various adversarial models and attack vectors, including those involving sophisticated quantum capabilities, to assess practical security.

The security analysis of cryptographic systems involves both theoretical and practical considerations. Theoretical security provides a foundation based on mathematical hard problems and formal proofs, ensuring resilience against attacks. Practical security addresses real-world implementation challenges, including efficiency, integration, key management, and protection against various attack vectors. Together, these aspects ensure that cryptographic methods offer robust protection in both theoretical and practical scenarios, paving the way for secure communication in the quantum era. 7.1 CASE STUDY: Organizations Adopting Quantum-Resistant Measures

1. Financial:

JPMorgan Chase:

- Initiatives: Joint development on Quantum Computing and Quantum-safe crypto with IBM.
- Best Practice: PQC algorithms should be tested with pilot projects first, then integrated into transaction systems.
- Lessons Learned: Importance of cross-industry collaboration and incremental implementation to manage risks.[15]

2. Health care:

Overview: Mayo Clinic:

- Initiate: Academia-industry collaboration in research and development for PQC to protect patient data and EHRs.
- Best Practice: Attention to data integrity and data privacy by using quantum-resistant encryption regarding the protection of sensitive health data.
- Lessons Learned: The key to security lies in the adoption of PQC and its continuous updating process for cryptographic protocols.[15]

3. Defense:

Lockheed Martin:

- Initiatives: Quantum computing research and deployment of quantum-resistant cryptography in the defence structure.
- Best Practice: Proper testing of PQC algorithms against a wide array of scenarios to ensure robustness and reliability.
- Lessons Learned: Deployments of PQC in a defense context must be developed in coordination with governments and adhere to emerging standards.[15]

Limitations

This section introduces the barriers of Quantum computing to be applicable in industry as well as the limitations of the study. Quantum Computing works on the concepts of quantum mechanics which use the outstanding factors of 'quantum bits' or qubits to perform a computation. Qubits, on the other hand, can be in a superposition of being both 0 and 1 at once. Qubits additionally can be entangled, such that the state of one qubit relies upon the condition of another regarding how far separated they are. Although theoretically unbreakable, the one-time pad has a number of shortcomings in practice.[14]

Key Creation and Distribution

The length of the key: the key is as long in bits as are all possible messages, making it difficult to generate and distribute large keys. Randomness: The key must be purely random. Getting true random numbers is hard and may need special hardware. The Key Distribution: Once a key is set, the issue now arises on how it should be passed to its recipient without any interception.

Key Management Persistence

Storing big keys in a safe way can be difficult, especially if working on many communications. Disposable:

To use each of the keys once and then throw them away. Reusing keys makes your security wilt.

Synchronized Key Usage: The two end parties i.e. sender and receiver must use the same key simultaneously, synchronization involves coordination

Restrictions on Quantum Key Distribution (QKD)

Although QKD provides the key distribution with ultimate security in principle, it still suffers from a few practical limitations.

- Needs for Infrastructure Specialized Hardware-QKD requires custom quantum hardware designed to prepare, manipulate and detect qubits. This gear can also be expensive, and hard to care for Range Limitations - The distance over which QKD can be implemented is restricted by photon loss and decoherence in optical fibres. Quantum repeaters, an experimental technology for long-distance key distribution
- Implementation Challenges Environmental Sensitivity-Quantum states are very sensitive to environmental disturbances and this can introduce errors which would compromise the security of key exchange.
- Key-Optimized Error Correction: QKD needs secure error correction and privacy amplification protocols to correct transmission errors.

Cost

Can be expensive to implement if the underlying technology and related infrastructure is not already available, as specialized hardware may need to be installed. Description of Barriers High costs (determines no one), limited usage in daily life situations. Requirement for new Infrastructure Very few people have the required infrastructure to use a quantum-safe OTP system out of their homes nations.

VII. Conclusion

In this project, we have addressed the urgent need for secure communication methods in the emerging quantum era. By combining One-Time Pad (OTP) encryption with quantum-safe key exchange protocols, we proposed a theoretically sound and highly secure solution against threats posed by the advancement of practical quantum computing technologies. The OTP ensures perfect secrecy when combined with a securely shared key, and the key distribution via Quantum Key Distribution (QKD) offers provable security based on the fundamental laws of quantum mechanics. Moreover, QKD can be further combined with post-quantum cryptographic (PQC) techniques, leading to a hybrid secure communication framework that can serve both classical and quantum processing systems. This integration can significantly enhance the accessibility, robustness, and practical deployment of quantum-secure communication networks.

VIII. Acknowledgment

We would like to thank our **Professor Jayeshree Mahale**, for her patience, supervision, encouragement and passionate sup-port. His knowledge and attention have been an inspiration for keeping our work on track.

We would also like to extend our thanks to our friends for offering us help whenever we had issues and providing us assistance with the resources needed to get this paper complete.

References

[1] O. Grote, A. Ahrens, and C. Benavente-Peces, "Small Quantum-safe Design Approach for Longterm Safety in Cloud Environments," in *Proc. 2021 Int. Conf. Eng. Emerg. Technol. (ICEET)*, Oct. 2021, doi: 10.1109/ICEET53442.2021.9659632.

[2] J. Y. Haw *et al.*, "Maximization of Extractable Randomness in a Quantum Random-Number Generator," *Phys. Rev. Appl.*, vol. 3, no. 5, May 2015, doi: 10.1103/PhysRevApplied.3.054004.

[3] T. Liu *et al.*, "Transfer of quantum entangled states between superconducting qubits and microwave field qubits," *Front. Phys.*, vol. 17, no. 6, Jul. 2022, doi: 10.1007/s11467-022-1166-1.

[4] D. Umar, "Cybersecurity Threats and Mitigation Strategies in the Age of Quantum Computing," *J. Technol. Syst.*, vol. 6, no. 5, pp. 1–14, Aug. 2024, doi: 10.47941/jts.2145.

[5] V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, Mar. 2018, doi: 10.14569/IJACSA.2018.090354.
[6] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, May 2004, doi: 10.1103/PhysRevA.69.052319.
[7] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 1–1, 2022, doi: 10.1109/COMST.2022.3144219.
[8] Y. Begimbayeva and T. Zhaxalykov, "Research of Quantum Key Distribution Protocols: BB84, B92, E91," *Sci. J. Astana IT Univ.*, no. 10.37943/QRKJ7456, Jun. 2022, doi: 10.37943/QRKJ7456.
[9] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?," in *IEEE Xplore*, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8791343/
[10] M. K. Singh, *Code-Based Cryptography: A Comparative Study of Key Sizes*, 2023.
[11] Ya. A. Derevianko, Ye. G. Kachko, and I. D. Gorbenko, "Hash-based cryptography, its security and feasibility in modern cryptosystems," *Radiotekhnika*, no. 213, pp. 7–17, Jun. 2023, doi: 10.30837/rt.2023.2.213.01.
[12] R. Au-Yeung, N. Chancellor, and P. Halffmann, "NP-hard but no longer hard to solve? Using quantum computing to tackle optimization problems," *Front. Quantum Sci. Technol.*, vol. 2, Feb. 2023, doi: 10.3389/frqst.2023.1128576.
[13] M. Z. Chowdhury, Md. Shahjalal, S. Ahmed, and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1–1, 2020, doi: 10.1109/OJCOMS.2020.3010270.
[14] M. Fellous-Asiani, J. H. Chai, R. S. Whitney, A. Auffèves, and H. K. Ng, "Limitations in Quantum Computing from Resource Constraints," *PRX Quantum*, vol. 2, no. 4, Nov. 2021, doi: 10.1103/PRXQuantum.2.040335.
[15] L. Li, "Reskilling and upskilling the future-ready workforce for industry 4.0 and beyond," *Inf. Syst. Front.*, vol. 24, no. 3, pp. 1–16, 2022, doi: 10.1007/s10796-022-10308-y.
[16] H. De Raedt, K. De Raedt, and K. Michielsen, "Event-based simulation of single-photon beam splitters and Mach-Zehnder interferometers," *EPL (Europhys. Lett.)*, vol. 69, no. 6, pp. 861–867, Mar. 2005, doi: 10.1209/epl/i2004-10443-7.
[17] M. Delina, B. H. Iswanto, H. Permana, and S. Muhasyah, "The Simulation of one-time-pad quantum key distribution," *J. Phys.: Conf. Ser.*, vol. 1402, no. 4, p. 044107, Dec. 2019, doi: 10.1088/1742-6596/1402/4/044107.
[18] V. P. Srinidhi, B. Vineetha, K. Shabarinath, and P. B. Honnavali, "Performing Cryptanalysis on the Secure Way of Communication Using Purple Cipher Machine," in *Lecture Notes in Electrical Engineering*, vol. 928, pp. 149–159, Dec. 2022, doi: 10.1007/978-981-19-5482-5_14.
[19] V. Reddy and G. Prakash, "Enhanced key establishment technique for secure data access in cloud," in *Proc. 2019 Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, Ghaziabad, India, 2019, pp. 1–4, doi: 10.1109/ICICT46931.2019.8977720.