Attaining Information Reliability Over Web Through Quantum Key Distribution

Padmavathi Vurubindi[1(✉)], Sujatha Canavoy Narahari[2], Aashritha Rayala[1], and Shivani Sarikonda[1]

[1] Chaitanya Bharathi Institute of Technology Gandipet, Hyderabad, Telangana, India
padmavathiv_cse@cbit.ac.in
[2] Sreenidhi Institute of Science and Technology Ghatkesar, Hyderabad, Telangana, India
cnsujatha@sreenidhi.edu.in

Abstract. Over the years a boundless communication is happening over the web. It is too obvious to maintain and attain reliable information. Quantum key distribution (QKD) is an evolving technique which provides information reliability. It uses quantum mechanics-based cryptographic principles to a secure communication system and attain a reliable information over web. Two parties can create and share a key with QKD, which can then be used to encrypt and decrypt messages. In more precise terms, QKD refers to the process of sharing the key rather than the key itself or the messages that it permits users to transmit. This is due to a fundamental principle of quantum mechanics: any measurement of a quantum system affects it. The key must be measured in some way for a third party to try to eavesdrop on it, which introduces detectable irregularities. A communication system that can detect eavesdropping can be constructed by transmitting data in quantum states. The entity attempting to view the photons will alter the system by using the fundamental principles of quantum physics, making an incursion detectable. The suggested paradigm assists in attaining reliable information through the employment of quantum gates to perform quantum key distribution. A quantum gate, is a basic quantum circuit that employs qubits. They are the building blocks of quantum circuits, just like classical logic gates are the building elements of conventional digital circuits.

Keywords: reliable · qubit · QKD · quantum gate · web

1 Introduction

The sender and receiver should get assurance that they are communicating with alleged entity over web whom they ought to be. As a matter of fact, the information over web must be reliable. A contemporary method of computing known as quantum computing is based on the theory of quantum mechanics is brought into consideration inorder to attain information reliability. Information theory, computer science, mathematics, and physics are brilliantly combined in this work. It beats conventional computers in terms of processing capacity, energy consumption, and exponential speed by modifying the

O. Castillo et al. (Eds.): PerSOM 2023, LNICST 517, pp. 367–379, 2024.
https://doi.org/10.1007/978-3-031-66044-3_28

behaviour of tiny physical entities like atoms, electrons, and photons. Quantum key distribution (QKD) is a secure communication method that implements elements of quantum physics to carry out a cryptographic protocol to provide information reliability over web. It allows two parties to generate a secret shared key that is only known to them and can be used to encrypt and decode messages.

1.1 Principles of Quantum Mechanics

According to the uncertainty principle, "certain physical property pairs are related in a particular manner that the observer cannot simultaneously know the value of both properties when measuring one of them." A single photon's polarisation cannot be determined along two separate polarisation angle [10]. The No-Cloning Theorem [12] states, the principle of photon polarisation asserts that "an eavesdropper cannot copy unknown qubits, i.e., unknown quantum states." A quantum cannot be measured or copied without being changed.

1.2 Qubits

A quantum bit also known as a qubit, is the basic building block of quantum information. It represents subatomic particles such as atoms and electrons as the memory and their control mechanisms as the processor of a computer. It can have a value of 1, 0, or both at once. Qubit contains two quantum states that resemble the binary states of the past. The qubit may exist in any of the two states or in their superposed states simultaneously. Dirac notation, a method, can be used to depict these quantum states. In this, the state label is preserved between two symbols. In this format and >. State names are therefore written as 0 and 1. Any quantum bit wave function can be written as a two-state linear combination with a complex coefficient for each state, i.e., $|w| = x|0\rangle + y|1\rangle$, where x and y are the coefficients for both states. The size of the coefficient's squared value determines the state's probability. The odds of recognising the qubit state 0 are $|x|^2$ and the odds of identifying the qubit state 1 are $|y|^2$. According to mathematics, the sum of these probabilities must be 1, or 100%, therefore $|x|^2 + |y|^2 = 1$ [15, 16].

1.3 Quantum Gates

The building blocks of quantum circuits, like classical logic gates are for traditional digital circuits, are known as quantum logic gates (or simply quantum gates) [16]. The most appropriate way to know linear combinations is the matrix representation, and it so happens that the suitable state on the matrix that represents the gate is unitary matrix U. That is U†U = I, where U† interpreted as U dagger, adjoint of U, complex conjugate of transposition matrix. The identity matrix U and I has a dimension of 2 by 2. Tensor product is used to construct the quantum gate matrix representation [13, 16]. The most common quantum gates include: Pauli gates: X, Y, and Z are the three single-qubit gates referred to as the Pauli gates. The X gate is equal to a conventional NOT gate, the Y gate rotates around the Y-axis of the Bloch sphere, and the Z gate rotates around the Z-axis of the Bloch sphere [16]. Hadamard gate: The Hadamard gate is a single-qubit gate that

maps the basis states $|0\rangle$ and $|1\rangle$ to the equal superposition state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and the minus superposition state $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, respectively. Quantum Fourier transformations and superposition states are produced using the Hadamard gate [13, 16]. CNOT gate: The two-qubit CNOT (Controlled-NOT) gate uses a control bit and a target bit as its first and second qubits, respectively. f the first qubit is in the state 0, it flips the second qubit. The Deutsch-Jozsa algorithm and quantum error correcting codes both use the CNOT gate as a crucial part of their algorithms [16]. SWAP gate: A two qubit gate called the SWAP gate exchanges the states of two qubits. Quantum algorithms for sorting and searching employ the SWAP gate [16].

1.4 Quantum Key Distribution

Considering that public key cryptosystems might be cracked by quantum computers, a key distribution strategy is necessary to fend against quantum assaults. Thus, Quantum Cryptography presents an effective key distribution scheme called as Quantum Key Distribution (QKD) based on the principles of quantum mechanics. Stephen Wiesner, who initially proposed the concept of information transfer by polarised photons, is credited with introducing the concept of QKD. This concept was used by Bennett and Brassard in 1984 to establish the first QKD protocol, also known as the BB84 protocol, which allows for the creation of unconditionally safe shared keys between two entities who are geographically separated. The selling point of QKD is that if the principles of quantum mechanics are true, the security of the protocol is assured. Comparing this to previous classical protocols that rely on the adversary's weak computing capabilities, this represents a significant advancement. The protocol's practical use has advanced to the point that a number of tests have been carried out using installed telecom cables, daylight free-space channels in cities, and satellite-to-ground channels [11, 16].

2 Related Work

The crucial sifting stage and the crucial reconciliation stage will be where contributions to the planned endeavor will be split into two stages. A unique key sifting technique for the quantum key distribution has first been created in order to compare the proposed system's processing time to the traditional key sifting step in BB84. Second, Two TPM devices have been used to weigh the sifting key. Constructed on both the transmitter and recipient sides. After that, Hebbian, Anti-Hebbian, and Random-Walk learning algorithms were used to synchronize the two TPM machines. Here, the efficiency of synchronization using different learning techniques has been investigated. As a result, an alternative to the modified key sifting system based on basis distribution BB84 protocol's conventional key sifting method [1].

An algorithm known as Qubit4Sync, a synchronization method for QKD installations, based on the identical qubits transferred throughout the protocol and needing no extra hardware aside from that needed to create and monitor the quantum states. According to our understanding, the approach introduces a novel cross-correlation methodology with the lowest computing complexity for large channel losses. We demonstrate the resilience of our approach in a real world QKD implementation. Since the suggested

model eliminates the need for extra hardware for the asynchronization sub-system, resulting in less expensive equipment and a lower chance of hardware failure, it facilitates the execution of a QKD setup effectively. The synchronization process is immune to eavesdropper denial-of-service attacks since the QKD fails before the synchronization [2].

An improvised QKD verification mechanism. Alice and Bob provide their IDs and seek a "secure" connection during the first stage. Information centres employ "public key authentication" to confirm that they are authorised users of the "public key" framework. Following the public key has been successfully authenticated, the data centres create random numbers. Additionally, the data centres transmit special KEY POOL's that have been encrypted using private keys. KPA belongs to Alice, while KPB belongs to Bob. For verification, use QKD: The first information centre creates a quantum communication link and sends copies of the key pools to both parties. A copy of the keys are exchanged between Alice and Bob through the information centre during their initial communication. Otherwise opens a quantum communication channel without the transfer of POOL. The steps involved in the mutual authentication phase are: Bob was publicly asked by Alice for the POOL KPA's key. Bob uses KPB to check that key. Only when the keys coincide does the transmission take place. Bob formally requests a key from the POOL KPB from Alice. Alice uses KPA to verify that key. Only when the keys coincide does the transmission take place. Every transmission is followed by a repeat of this process. Thus, this ensures that neither party is spying on the other. Since only Alice and Bob are aware of the specifics of their keys from the KEY POOL, this also guarantees that mutual 100 percent user authentication is accomplished [3].

A QKD network exists where a quantum layer including a reliable symmetric key is established has to define QKD networks. a layer for maintaining and validating already-created keys. a level of communication where data security is achieved using the established key [4].

Networks using quantum key distribution (QKD) provide interesting alternatives for private communication. In this study, they created 1xN QKD network systems utilising an optical route length compensation method with subns precision using a realistic plug-and-play QKD architecture and small, field- programmable gate array (FGPA)-based timing control modules. The problem of accounting for variations in optical path length in QKD network systems is addressed by the user-independent compensation mechanism suggested in this research. The technique can achieve sub-ns timing resolution without active user input by utilizing a delay line and interferometer. This could make it simpler to put QKD networks into practice and could assist in resolving one of the main issues the area is now experiencing [5].

Privacy amplification (PA) It is a method to extract a highly private key from a string that is just marginally safe. The creation of a theoretically unconditional secure key is a crucial step in QKD. This work proposes a GNU multiple precision arithmetic library (GMP)-based CPU platform-based high throughput modular arithmetic hash PA method. According to the experimental data, this scheme's throughput is nearly an order of magnitude greater than the throughput of the comparable method on the same CPU platform with block sizes of 106 and 108 at 135 Mbps and 69 Mbps, respectively, on an Intel i3–2120 CPU. The difficulty of implementing privacy amplification in QKD

can be overcome using the high- speed privacy amplification approach suggested in this study employing GMP. The approach can accomplish high-speed privacy amplification for huge key sizes without compromising security by utilizing bit-wise operations with the GMP library. As a result, secure communication systems that rely on QKD may be developed, making QKD more effective and practical [6].

Quantum encryption is still a young field. We cannot, however, ignore the dangers and difficulties it offers for the existing cyberspace's security. Since quantum cryptography and protocols combine conventional cryptography with quantum physics, this study examines them. Designing is the most effective among DV-QKD PA cryptographic protocols and algorithms that assaults from quantum computers is the primary objective of research into quantum cryptography. The QKD protocol objective for future Internet cyberspace security is the main topic of this paper's analysis and exploration. The results of the experimental investigation presented in this paper show how sniffer detection and quantum cryptography's constant security make it suitable for the next-generation Internet [7].

Semi-quantum key distribution (SQKD) is a significant research topic that enables one quantum participant with cutting-edge quantum equipment to safely communicate a shared secret key with one limited-capability classical user. Alice gives Bob and Charlie, respectively, two particle sequences from Bell state. Once the particles have been processed and returned, Alice may use Bell-state measurement to simultaneously identify reflected particles from Bob and Charlie and produce two distinct raw keys. This protocol may be expanded to the m + 1 party communication technique by using the m-particle GHZ state, enabling more players to share keys. When compared to the conventional SQKD system, this expanded model dramatically lowers communication complexity in large-scale communication networks. This work suggests a SQKD system that enables a quantum user to simultaneously send two separate private secret keys to two conventional users. To disseminate m keys concurrently, this approach is extended. It offers a useful concept for creating a network for distributing quantum keys. Attacks such as the modification attack, the entangle measurement attack, and other frequent attacks can be defeated by the proposed SQKD protocol [8].

To strengthen the defence against quantum computing assault of conventional cryptographic keys, QKD is being developed. The durability of classical cryptography's keys, which were almost impenetrable in the pre-quantum era, can be improved through QKD. This article presents a comparative analysis of several QKD techniques and examines trends and restrictions in classical cryptography of key management techniques. It also emphasises how QKD's security implementation features help to address risks that can arise in a situation involving quantum computing in order to make the cryptographic keys resistant to quantum effects [9].

3 Proposed Methodology

The suggested paradigm assists in attaining reliable information through the employment of quantum gates to perform quantum key distribution. Pauli-X gate and Hadamard gate is used to carry out the proposed methodology.

3.1 Pauli-X Gate

Pauli-X gate [16] is a single qubit gate that flips 0 to 1 and vice versa. It can be represented in the form of matrix as,

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We merely multiply the state vector of the qubit by the gate to observe the impact of gate on the qubit. We may observe that X-gate changes the amplitude of states $|0\rangle$ to $1\rangle$ [16]

$$\mathrm{A} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

3.2 Hadamard Gate

The Hadamard Gate [16] operates on a single qubit similarly to the Pauli-X gate and can also be represented as a 2 x 2 matrix. Simply applying a certain gate to a qubit will cause it to enter a superposition state. This can be accomplished through the well-known quantum computing gate known as the Hadamard Gate.

3.3 Quantum Key Distribution

A key establishment technology that offers unwavering security is Quantum Key Distribution (QKD) [11]. In entanglement-based methods, quantum key distribution either violates Bell's inequality or employs Heisenberg's uncertainty principle to detect the presence of an opponent. Heisenberg's uncertainty-based protocol states that a quantum state is altered by measurement. As a result, the eavesdropper will inject an error into the information flow through a quantum channel, which the protocol can identify. When using entanglement-based protocols, information is created if an outsider measures the entangled quanta. The eavesdropper attempts to violate Bell's inequality by adding an additional quanta to the protocol. As a result, the eavesdropper's presence will also be detected [11].

In QKD process, Alice, the sender, and Bob, the receiver, generate the secret key using a quantum channel and a conventional channel. The classical channel can be any connection to a traditional network, such the internet or a phone network, but the quantum channel can be an optical fibre or a direct line of-sight free space link. While Bob measures these photons on the receiving side to produce raw key bits, Alice prepares and sends single polarised photons known as quantum bits or "qubits" from the sending side using a laser source. Shared secret keys are produced after information exchange over the traditional route [13]. Any data, audio, or video can be encrypted to achieve reliable information using the secret keys generated by QKD.

3.4 Quantum Transmission

Following are the steps involved quantum channel exchange between Alice, the sender and Bob, the receiver.

1. Preparation: Alice prepares a string of random bits and encodes each bit as a photon using a randomly selected polarization (either horizontal/vertical or diagonal/anti-diagonal).
2. Qubit generation: To generate polarised photons, or qubits, Alice chooses a random base sequence.
3. Quantum gate application: Alice applies the qubits to Hadamard and Pauli X-gates and transmits them to Bob.
4. Transmission: Alice sends the encoded photons to Bob over a quantum channel (e.g. fiber optic cable or air).
5. Bob's construction of bits: Using the polarised photons that Alice transmitted, Bob chooses some random bases and measures them, then uses the measured polarised photons to construct a set of random bits.

3.5 Public Exchange

Here are the steps involved in the public exchange of the BB84 protocol:

1. Reception: Bob receives the photons and randomly measures the polarization of each photon using his chosen basis.
2. Announcement: Alice announces to Bob which polarization basis she used for each photon.
3. Comparison: Bob discards all the photons that were measured in the wrong basis (i.e. when Alice and Bob choose different bases). Alice and Bob compare their measurement outcomes for the remaining photons in public. (but not the values themselves).
4. Confirmation: A subset of the remaining bits is chosen at random by Alice and Bob and compare them to check for errors. If there are no errors, they can be confident that they have a shared secret key.
5. Key distillation: Alice and Bob perform an error correction protocol to correct any errors in their shared key, and then they implement a privacy amplification approach to limit the quantity of data that may have been obtained through eavesdropping.
6. Key verification: Alice and Bob check that their final shared key matches exactly, ensuring that no information was lost or intercepted during the exchange.

By following these procedure, Alice and Bob can create a shared secret key that is only known to them and cannot be read by a third-party.

3.6 Key Sifting

This protocol uses two bases—one of which is a diagonal basis and the other is a rectilinear basis—to produce four polarization states. The rectilinear basis encodes logic 0 as a photon with a 0° polarization and logic 1 as a photon with a 90° polarization. According to the diagonal basis, logic 1 is symbolized by a 135°-polarized photon, while

logic 0 is symbolized by a 45°-polarized photon. The polarised photons are delivered from Alice (Sender) to Bob (receiver) across the quantum channel [13, 15].

Figure 6 illustrates generation of sifted key with an example. In the quantum transmission channel, Alice randomly generates a sequence of 15-bits and creates polarized photons which are a sequence of random bases and sent those qubits to Bob. Before sending them to Bob, these qubits are applied to Hadamard and Pauli-X gates. Bob chooses a random sequence of bases to measure with Alice's bases along with random bits accordingly to his random bases [13].

In the Public channel exchange, Bob sends his random bases to Alice. Alice reports matched bases with their respective positions to Bob. Now, a sifted key is generated successfully [13].

4 Results

The proposed methodology is implemented using IBM Qiskit framework [17] for simulating the results. It provides Quantum Computer Lab which offers a strong framework for creating quantum key distribution (QKD) protocols using quantum gates like Pauli X gate and Hadamard gate. Following are the illustrations of our simulation results showing each step of this protocol starting from server's generation of sequence of random bits to establishment of secure communication with a shared secret key between server(sender) and user (receiver).

1. Server generates a random sequence of 100-bits.

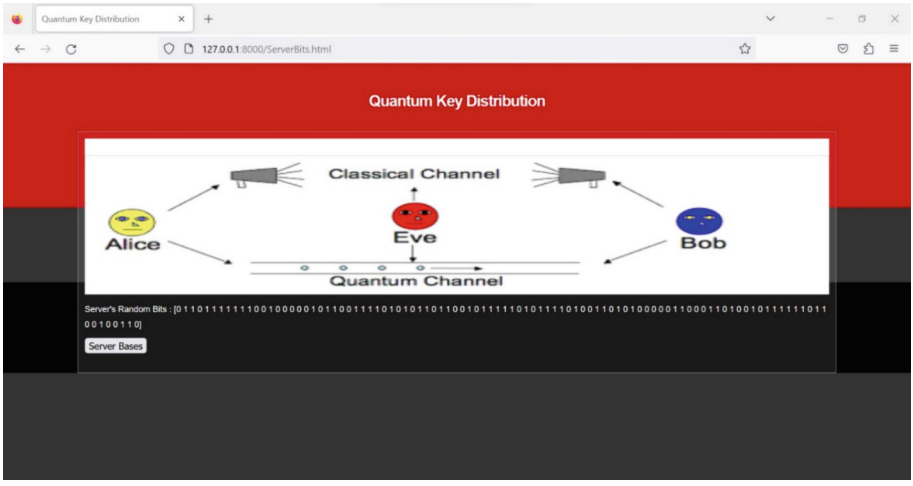

Fig. 1. Server's Random bits

2. Server chooses random bases to convert bits to qubits and sends to User.

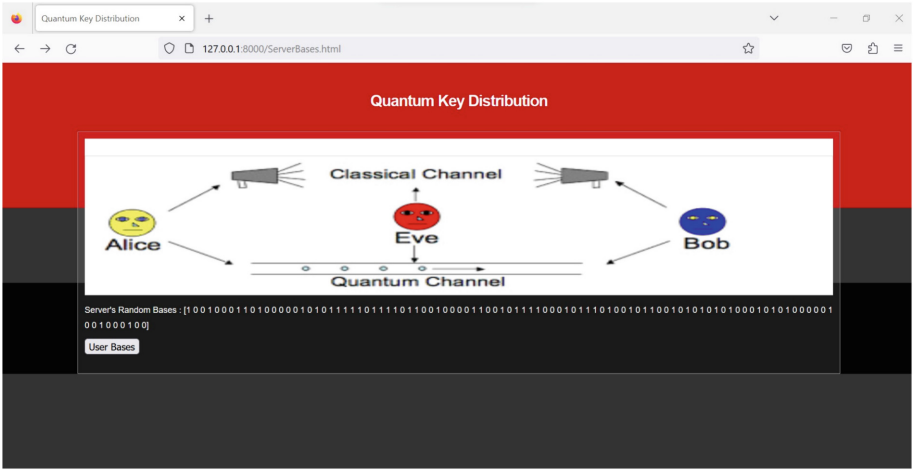

Fig. 2. Server's Random bases

3. User generates its random bases for 100 qubits.

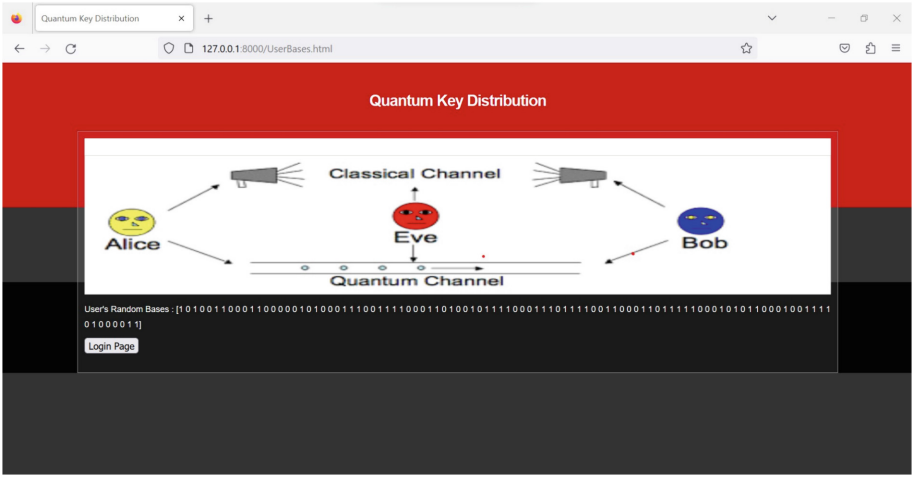

Fig. 3. User's random bases

4. User registration

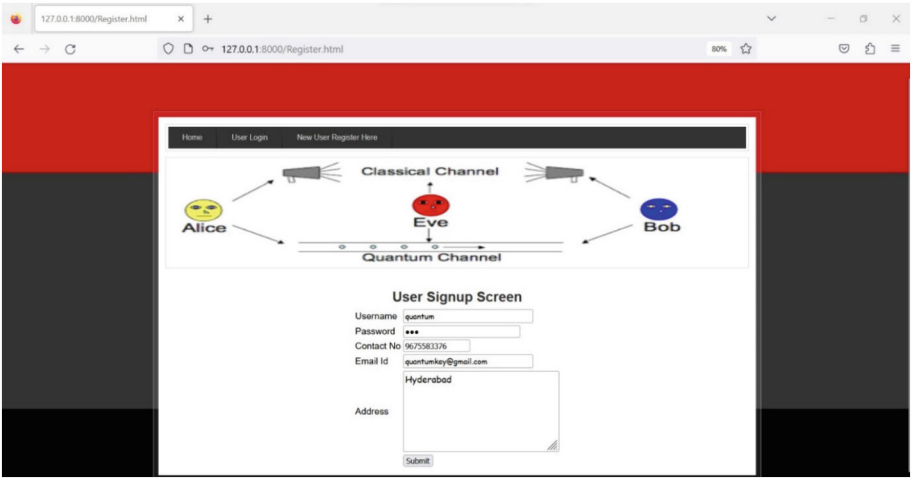

Fig. 4. User Registration

5. User logs in and the communication between server and user starts. Server measures the bases sent by user. They both generate their secret keys based on the matched bases. After removing garbage bits and if both server key and user key are same then generation of sifted key is successful.

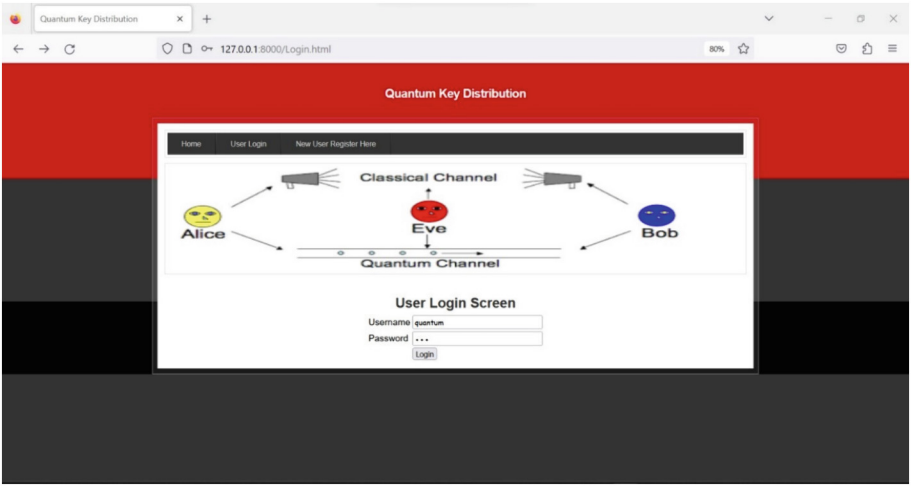

Fig. 5. User Login

6. Shared Key: Sifted key generation is successful. Since shared key is established which is in the size of 15 bits and they can have a secured communication.

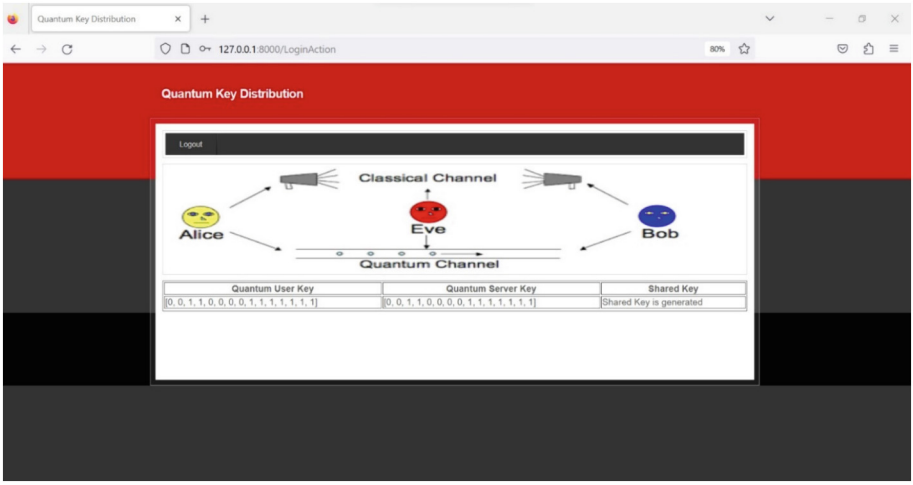

Fig. 6. Shared Key

5 Analysis

From the results it is clear that a secure and authenticated communication channel can be established between user and server following the QKD protocol. QKD protocol offers perfect secrecy by ensuring that the key cannot be known by any kind of third-party which can intercept and measure all the qubits transmitted between the parties. Server has generated random of 100-bits and 100-bases and User measured his random sequence of 100 bases with Server's. The advantage of QKD is it allows the generation of long keys in contrast to the classical which are limited by the length of the key that can be shared through the communication channel [14].

We used Pauli-X and Hadamard gates in our protocol. We applied Pauli-X gate to encode the qubit with the value of the classical bit being transmitted. i.e.; if the corresponding classical bit is 1, the X gate is applied to the qubit to flip its state from $|0\rangle$ to $|1\rangle$. This is because the state $|1\rangle$ is orthogonal to the state $|0\rangle$, which makes it easier to distinguish between them during the measurement stage of the protocol. While measuring the bases, if the base is 0 then the qubit is measured in Z-basis and measured and if the base is 1 then the qubit is first transformed to X-basis by applying Hadamard gate and then measured in Z- basis. By applying the Hadamard gate, the qubit is placed in a superposition of the Z-basis and X-basis, so Bob's measurement is equally likely to yield 0 or 1, regardless of which basis Alice used.

After the server sends the qubits to User they are measured against user bases and a shared key is generated by using the matched bases and removing the garbage bits from bits that were measured in different bases by sender and user. Therefore, a highly secured communication channel is established between server and user which is resistant to attacks from any third-party.

6 Conclusion

Our simulation results show that the proposed implementation of QKD using Pauli-X and Hadamard gates established a successful shared secret key between two-parties. Thus attaining information reliability over web. Qiskit programming offers a strong framework for creating quantum key distribution (QKD) protocols, such as using a Pauli X gate and a Hadamard gate. Qiskit provides an easy-to-use interface for simulating the behavior of quantum circuits and testing the performance of QKD protocols under different conditions, such as the presence of noise and errors in the quantum channel. By using Qiskit, researchers and developers can explore the potential of quantum computing for secure communication and cryptography, and build new applications that leverage the power of quantum mechanics.

QKD is currently a very new and expensive technology, and its actual application confronts a number of difficulties despite its theoretical security guarantees. These include the requirement for specialised hardware and the susceptibility of various QKD methods to side-channel assaults or attacks based on faulty components. Although QKD is a promising technology for secure communication, outside of specialised applications, it is not yet extensively employed. Even said, there is still a lot of research being done in this field, and quantum technology advancements may one day make it more useful for everyday use.

References

1. Biswas, C., Haque, M.M., Gupta, U.D.: A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography. IEEE Access **10**, 72743–72757 (2022)
2. Calderaro, L., Stanco, A., Agnesi, C., Avesani, M., Dequal, D., Villoresi, P., Vallone, G.: Fast and simple qubit-based synchronization for quantum key distribution. Phys. Rev. Appl. **13**(5), 054041 (2020)
3. Kumar, A., Dadheech, P., Singh, V., Poonia, R.C., Raja, L.: An improved quantum key distribution protocol for verification. J. Disc. Math. Sci. Cryptograp. **22**(4), 491–498 (2020)
4. Mehic, M., Nemec, M., Rass, S., Ma, J., Peev, M.: Quantum key distribution: a networking perspective. ACM Comput. Surv. **53**(5), 96 (2020)
5. Park, B.K., Woo, M.K., Kim, Y.S., Cho, Y.W., Moon, S., Han, S.W.: User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a $1 \times N$ quantum key distribution network system. Photonics Res. **8**(3), 296–302 (2020)
6. Yan, B., Li, Q., Mao, H., Xue, X.: High-speed privacy amplification scheme using GMP in quantum key distribution. IEEE Photonics J. **12**(3), 1–13 (2020)
7. Zhou, T., Shen, J., Li, X., Wang, C., Shen, J.: Quantum cryptography for the future internet and the security analysis. Secur. Commun. Netw. **2018**(1), 8214619 (2018)
8. Wanqing, W., Sun, C.Y.: Semi-quantum key distribution with two classical users (2022)
9. Adhikari, T., Ghosh, A., Khan, A.: quantum resistance for crypto- graphic keys in classical cryptosystems: a study on QKD protocols. In: 12th International Conference on Computing Computation and Networking (2021)
10. Wiesner, S.: Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983)
11. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp. 175–179 (1984)

12. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982)
13. Padmavathi, V., Vardhan, B.V., Krishna, A.V.N.: Provably secure quantum key distribution by applying quantum gate. Int. J. Netw. Secur. **20**(1), 88–94 (2018)
14. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
15. Padamvathi, V., Vishnu Vardhan, B., Krishna, A.V.N.: Quantum cryptography and quantum key distribution protocols: a survey. In: IEEE the 6th International Conference on Advanced Computing (IACC), pp. 556–562 (2016)
16. M. A. Nielsen and I. Chuang, Quantum Computation and Quantum Information, 10th Anniversary Edition, Cambridge University Press, 2002
17. IBM Quantum (2021). https://quantum-computing.ibm.com/