A Novel Multi-User Quantum Communication System Using CDMA and Quantum Fourier Transform

M. Anand(✉) and Pawan Tej Kolusu

Centre for Development of Telematics, Bengaluru 560100, KA, India
{anand.m,pawantej_kolusu}@ieee.org

Abstract. Quantum Communication is an upcoming technology for the next generation communication network. Quantum Communication involves transmitting Quantum Bits (Qubits) instead of regular binary bits in the communication network. With absolute security guaranteed by laws of quantum physics, harnessing this emerging technology is necessary for securing future communication networks. In Quantum Communication, enabling Multi-User communication is needed to support multiple network topologies. There are many open challenges in Multi-User Quantum Communication like security between the transmitter or receiver and router, increasing the difficulty for eavesdroppers to guess the Qubit being exchanged across routers and enabling hierarchical network topology etc. In this paper, the idea is to use Code Division Multiple Access (CDMA) to ensure security between transmitter and transmit side router and also between receiver side router and receiver. The issue of eavesdroppers is solved by using Quantum Fourier Transform (QFT) which transforms incoming Qubits thereby securing them from eavesdroppers. QFT and the corresponding Inverse Quantum Fourier Transform (IQFT) makes the Qubit more secure in the network. QFT and IQFT is also scalable making it ideal for hierarchical network topology. This paper provides the mathematical proof of the security and scalability of the proposed Multi-User Quantum Communication System.

Keywords: Quantum computing · Multi-user quantum communication · Quantum circuits · Quantum internet · CDMA · Quantum Fourier transform

1 Introduction

1.1 Qubit and Quantum Communication

In quantum computing, a qubit or quantum bit is the basic unit of quantum information [1]. Qubit is the quantum version of the classical binary bit physically realized with a two-state device like the spin of the electron in which the two

N. Kumar et al. (Eds.): UBICNET 2021, LNICST 383, pp. 79–90, 2021.
https://doi.org/10.1007/978-3-030-79276-3_7

levels can be taken as spin up and spin down; or the polarization of a single photon in which the two states can be taken to be the vertical polarization and the horizontal polarization.

In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of both states simultaneously, a property which is fundamental to quantum mechanics and quantum computing [2].

Quantum communication is a field of applied quantum physics closely related to quantum information processing and quantum teleportation. Its most interesting application is protecting information channels against eavesdropping by means of quantum cryptography.

Similar to the way classical networks exchange communications and data between different inter-connected entities, a quantum network enables the secure transmission and exchange of quantum communications (quantum cryptographic keys) over fiber optic cable between distinct, physically-separated quantum processors, or endpoints.

1.2 Multi-User Quantum Communication

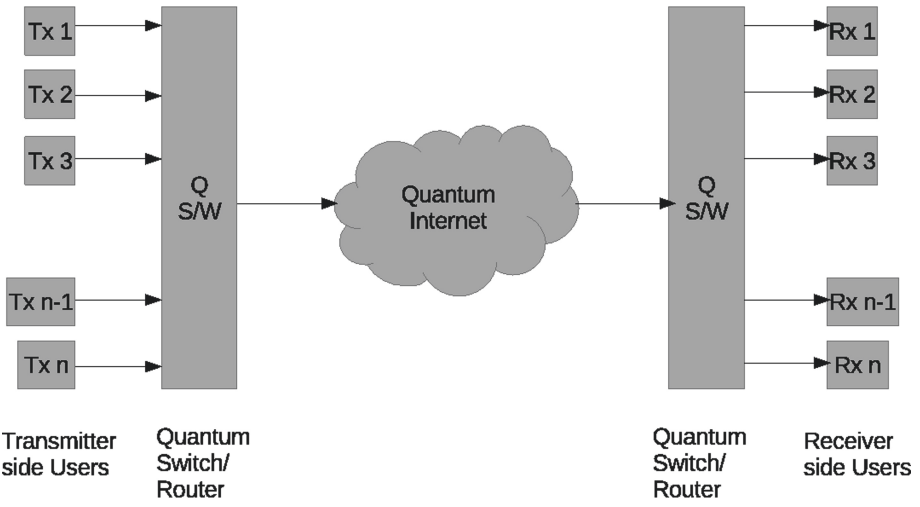

Fig. 1. A multi-user involved quantum communication network system for N transmitter users and N receiver users.

A multi-user involved quantum communication network system for N transmitter users and N receiver users. Routers and switches are used to create a hierarchical network within the quantum internet as shown in Fig. 1. Security of all data flowing across users needs to be ensured end-to-end by all nodes involved. There are many publications in this domain [5–9].

Challenges in Multi-User Quantum Communication:

Security between the transmitter or receiver and router. In the quantum internet each node which is transmitter must encode the data in Qubits which the untrusted Switch or Router cannot decode. This is the primary level of security to be ensured by the transmitter. Similarly the receiver must ensure that the qubits received is as expected and no tampering is done to them. This challenge is particularly high when the transmitter is not connected in a peer-to-peer fashion.

Increasing the difficulty for eavesdropper to guess the Qubit being exchanged across routers. The Switch or router at the transmitter and receiver side must be designed in a fashion to ensure that any eavesdropper in the quantum internet cannot decode the data being transmitted. This node is typically not co-located with the receiver or transmitter. Rather the routers and switches are in the custody of untrusted 3rd parties. This increases the need of securing the Qubits across these routers and switches. Proper algorithms and quantum circuits are needed to Increase the difficulty for eavesdroppers to guess the Qubit being exchanged across routers.

Enabling hierarchical network topology. In a multi-user quantum communication system, there is a need for a hierarchical network topology for a scalable quantum internet. This scaling is possible only when the switches and routers are designed using scalable algorithms and circuits.

In this paper the author creates quantum circuits for the transmit side, receive side and the quantum switch. The technologies used are using the basic building blocks of CDMA technology and Quantum Fourier Transform (QFT) and Inverse Quantum Fourier Transform (IQFT) technique, thereby enabling multi-user quantum communication using CDMA and QFT.

The paper is arranged as follows. In Sect. 2 the proposed multi-user quantum communication system model using QFT is described. This section includes the transmitter side modulation and receiver side demodulation. Mathematical treatment is provided in Sect. 3. Section 4 lists the advantages of the proposed system. Results and discussion are in Sect. 5. Section 6 provides the conclusion and future works planned for this proposed system. Section 7 provides acknowledgment followed by references used in this paper.

2 Proposed Multi-User Quantum Communication System Using QFT

Explanation for the Fig. 2 is as follows

User data are sent in Qubits D_1 and D_2 for user 1 and user 2 respectively. CDMA codes for User 1 is represented by 2 Qubits, together marked as C_1. This is used for doing CDMA encoding and decoding. CDMA codes for User 2 is represented by 2 Qubits, together marked as C_2. This is used for doing CDMA encoding and decoding. The first 2 dotted box on the left side in the image represent the quantum circuit inside transmitter side user 1 and user 2 respectively. This performs the CDMA endoing procedure. The next 2 dotted box in the middle of

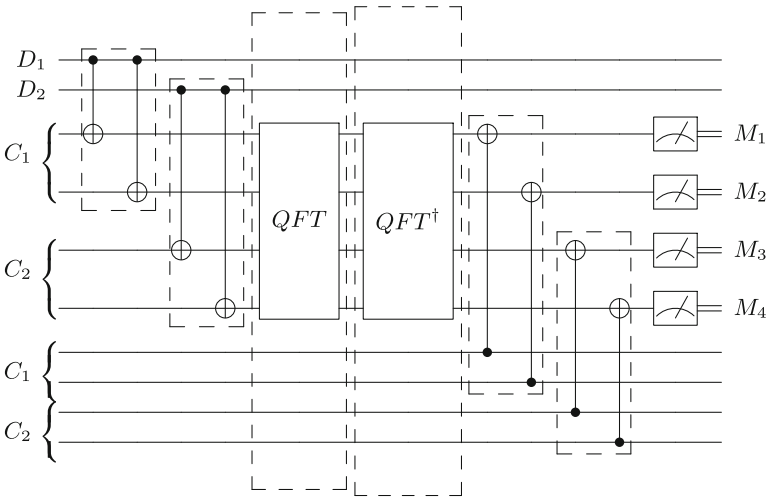

Fig. 2. Proposed Multi-User Quantum circuit.

the image represent transmitter side and receiver side quantum switch or router respectively. The last 2 dotted box towards the right in the image represent the quantum circuit implemented at receiver side user 1 and user 2 respectively. This performs the CDMA decoding procedure. A small operation on M_1 and M_2 is needed to recover the user 1 data D_1 and similarly, a small operation on M_3 and M_4 is needed to recover the user 2 data D_2. More details and explanations are provided in subsequent sections. All quantum circuits in this paper is drawn using qcircuit latex package [10].

2.1 Transmitter Side Modulation

Code Division Multiple Access (CDMA) Encoding

Each classical bit d is encoded as a single Qubit D.

Classical $0 -> |0\rangle$ and Classical $1 -> |1\rangle$

For demonstration purpose this paper will consider a 2-User system henceforth. Let d_1 and d_2 be the classical bits of User1 and User2 respectively. Let D_1 and D_2 be the corresponding Qubits of d_1 and d_2.

Each transmit User is assigned a 2-Qubit Walsh hadamard code-word C.

Let C_1 and C_2 be the walsh hadamard codes assigned to each User.

$$U_1 : C_1 = |C_{1x}C_{1y}\rangle = |01\rangle \tag{1}$$

$$U_2 : C_2 = |C_{2x}C_{2y}\rangle = |00\rangle \tag{2}$$

The CDMA encoding includes a XOR operation using a C−NOT gate. Each User Qubit D is used as a Control bit for doing XOR operation on the respective User code-word C as shown in Fig. 3.

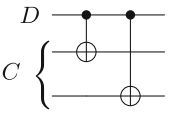

Fig. 3. CDMA encoding for single User

The CDMA encoded Qubits for individual Users is computed as shown in Fig. 4

$$E_1 = |E_{1x}E_{1y}\rangle \, where, \; E_{1x} = C_{1x} \oplus D_1 \, and \, E_{1y} = C_{1y} \oplus D_1 \tag{3}$$

$$E_2 = |E_{2x}E_{2y}\rangle \, where, \; E_{2x} = C_{2x} \oplus D_2 \, and \, E_{2y} = C_{2y} \oplus D_2 \tag{4}$$

Using equations (1),(2), (3) and (4) we get

$$E_1 = |D_1 D_1'\rangle \tag{5}$$

$$E_2 = |D_2 D_2\rangle \tag{6}$$

The CDMA encoded data for both Users is given by (7)

$$E = |E_{1x}E_{1y}E_{2x}E_{2y}\rangle = |D_1 D_1' D_2 D_2\rangle \tag{7}$$

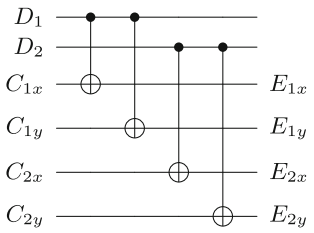

Fig. 4. CDMA encoding for 2 User system

Quantum Fourier Transform (QFT)
Quantum fourier transform is used as a channel encoding method to modulate the CDMA encoded data. For a n User system we use $2n$-Qubit QFT model. For example for a 2 User system, we use 4 Qubit QFT model. The CDMA encoded data E is passed through the QFT block as shown in Fig. 5.

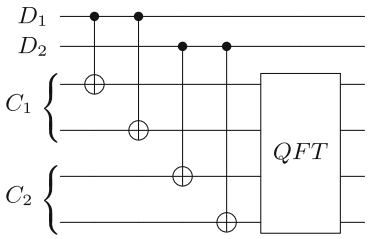

Fig. 5. QFT of CDMA encoded data of 2 Users

2.2 Receiver Side Demodulation

Inverse Quantum Fourier Transform (IQFT)

The received signal is passed through the IQFT block as shown in Fig. 6. The initially CDMA encoded signal $E = |D_1 D_1' D_2 D_2\rangle$ is recovered after this block.

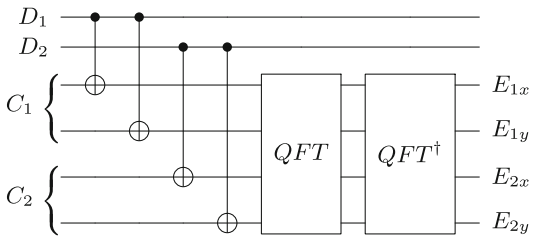

Fig. 6. Inverse Quantum Fourier Transform circuit

Code Division Multiple Access (CDMA) decoding

Each receiver will have the same walsh hadamard codes C_1 and C_2 respectively. The CDMA decoding part consists of a XOR operation using a C−NOT gate. Each User code Qubits are used as Control bits for doing XOR operation on the IQFT decoded Qubits as shown in Fig. 7.

Let F = $|F_{1x}F_{1y}F_{2x}F_{2y}\rangle$ be the CDMA decoded Qubits, then as per Fig. 7

$$F_{1x} = C_{1x} \oplus E_{1x};\ F_{1y} = C_{1y} \oplus E_{1y};\ F_{2x} = C_{2x} \oplus E_{2x}\ and\ F_{2y} = C_{2y} \oplus E_{2y} \quad (8)$$

Measurement and User bit recovery

As a next step, we measure all the CDMA decoded Qubits $F_{1x}, F_{1y}, F_{2x}\ and\ F_{2y}$. Let $M_1, M_2, M_3\ and\ M_4$ be the measured values respectively. The User classical data bits can be recovered by performing an Logical AND operation on the measured values.

$$d_1 = M_1 \wedge M_2\ and\ d_2 = M_3 \wedge M_4 \quad (9)$$

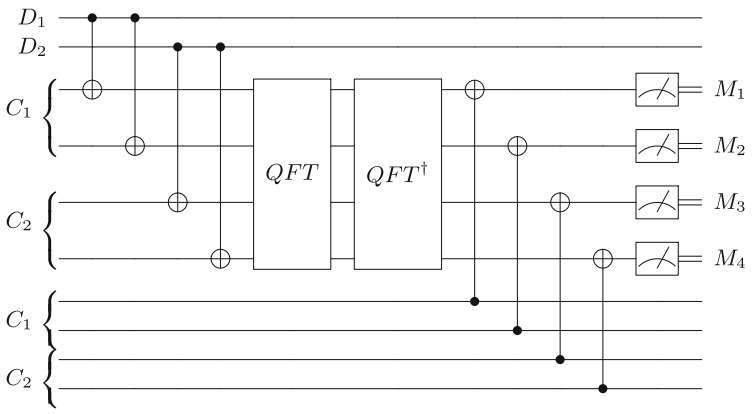

Fig. 7. Quantum circuit for CDMA Decoding

3 Mathematical Example for Single User System

Considering a single User system, where the transmit User classical bit is $d_1 = '1'$. Converting the classical bit to Qubit we get $D_1 = |1\rangle$. In the real world the $|0\rangle$ may be represent on spin-up of electron and $|1\rangle$ may be represent on spin-down of electron. Alternatively $|0\rangle$ may be represent on vertical polarization of photon and $|1\rangle$ may be represent horizontal polarization of photon.

3.1 CDMA Encoding

Let $C_1 = |C_{1x}C_{1y}\rangle = |01\rangle$ be the walsh hadamard code assigned to User1.

The CDMA encoded Qubits for User1 is computed as

$$E_1 = |E_{1x}E_{1y}\rangle \tag{10}$$

where,

$$E_{1x} = C_{1x} \oplus D_1 = |0\rangle \oplus |1\rangle = |1\rangle \tag{11}$$

and

$$E_{1y} = C_{1y} \oplus D_1 = |1\rangle \oplus |1\rangle = |0\rangle \tag{12}$$

$$Hence\, E_1 = |10\rangle \tag{13}$$

Vector representation of $E_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$

3.2 QFT

Since the mathematical example is for 1 user, 2 Qubit QFT is needed. The QFT matrix for 2 qubit system is represented by QFT_4 which is represented in matrix form as shown in equation below:

$$QFT_4 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \tag{14}$$

The operation of QFT over the output of CDMA encoded Data E_1 is represented by the equation below:

$$QFT * E_1 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 1/2 \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = G_1 \tag{15}$$

3.3 IQFT

Since the mathematical example is for 1 user, 2 Qubit IQFT is needed. The TQFT matrix for 2 qubit system is represented by $IQFT_4$ which is represented in matrix form as shown in equation below:

$$IQFT_4 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \tag{16}$$

The operation of IQFT over the output of QFT modulated Data G_1 is represented by the equation below:

$$IQFT * G_1 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} .1/2 \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = E_1 \tag{17}$$

3.4 CDMA Decoding

Ket representation of $E_1 = |10\rangle$

$$F_{1x} = C_{1x} \oplus E_{1x}; = |0\rangle \oplus |1\rangle = |1\rangle \tag{18}$$

$$F_{1y} = C_{1y} \oplus E_{1y}; = |1\rangle \oplus |0\rangle = |1\rangle \tag{19}$$

3.5 Measurement and User Bit Recovery

After Measuring we have $M_1 = 1 \, and \, M_2 = 1$.

$$d_1 = M_1 \wedge M_2 = 1 \wedge 1 = 1. \tag{20}$$

4 Simulation of 2 User System

The proposed quantum communication network was simulated using Quirk quantum simulator tool [10] for 2 transmit users and 2 receive users.

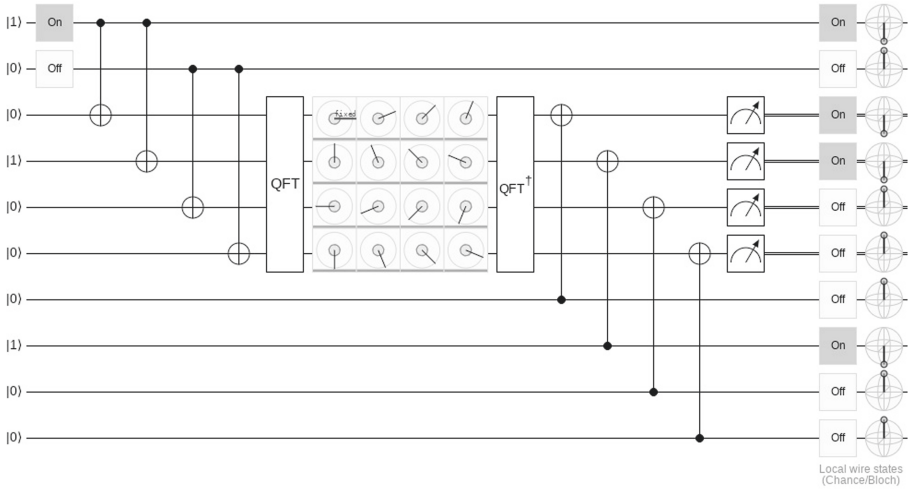

Fig. 8. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $d_1 = 1$ and $d_2 = 0$.

In this simulation shown in Fig. 8. The data for user 1 is shown in the first line. The data for user 2 is shown in the 2nd line. In this simulation shown in figure the user 1 want to transmit binary data 1, which is mapped to quantum bit (qubit) $|1\rangle$. The measurement of this qubit would be high or on state represented by the box which shows "On". This box is a hypothetical measurement result. Similarly user 2 want to transmit binary data 0, which is mapped to quantum bit (qubit) $|0\rangle$. The measurement of this qubit would be low or off state represented by the box which shows "Off". This box is a hypothetical measurement result.

The next 2 lines are the Code for user 1. CDMA code for user 1 is $|10\rangle$ which is represented in the 2 lines with qubit values $|1\rangle$ and $|0\rangle$. Similarly the next 2 lines are the Code for user 2. CDMA code for user 2 is $|00\rangle$ which is represented in the 2 lines with qubit values $|0\rangle$ and $|0\rangle$. The CDMA encoding is done using C-NOT gates. This operation is represented by first 2 vertical lines drop shown

in figure. The output of this operation is the CDMA encoded data. Similarly the next 2 vertical lines drop shown in figure are CDMA encoding for user 2.

These 4 encoded outputs are fed to the QFT module at the switch. The Output of the QFT is transmitted to the receiver side router or switch over the quantum internet. The simulation shows the spreading of data. It is very difficult to guess or decode the user data. At the receiver side router or switch, Inverse QFT is performed and the first 2 qubits are sent to User 1 at receiver and the next 2 Qubit to user 2 at receiver side. At user 1 at receiver, C-NOT operation is again performed using the same code as done during the encoding phase. The resulting Qubit is measured. The 2 measured outputs are in binary bits. Binary logic "AND" gate operation is performed on these 2 bits. For user 1 the values are "on" which means 1. AND operation of two 1's is 1 which is the user 1's binary data. Similar operation is performed by user 2.

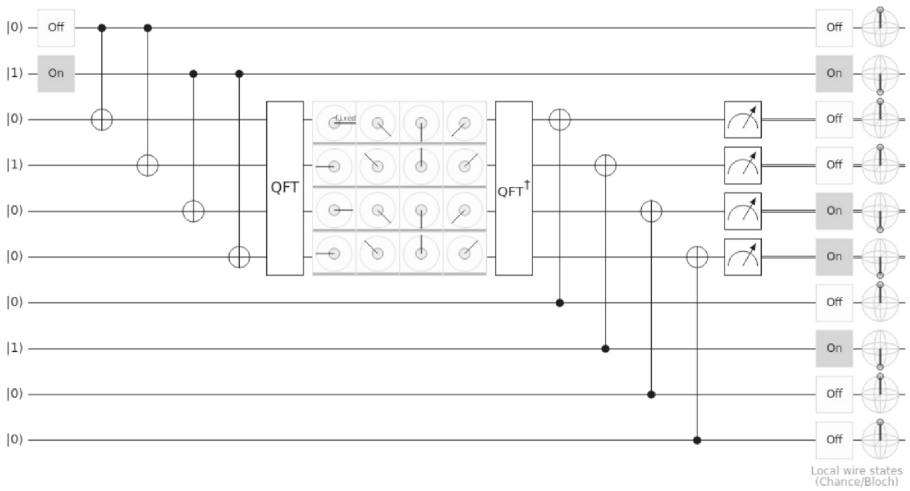

Fig. 9. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $d_1 = 0$ and $d_2 = 1$.

Similar simulation is done with user 1 binary data 0 and user 2 binary data 1 using the same CSMA codes as shown in Fig. 9. The result of measurement for user 1 produces 2 "off" sates representing 0 and 0. The data for user 1 is retrieved using binary "AND" operation which results in 0 meaning user 1 data is 0. Similarly the result of measurement for user 2 produces 2 "on" sates representing 1 and 1. The data for user 2 is retrieved using binary "AND" operation which results in 1 meaning user 2 data is 1.

These simulation provides proof that the proposed multi-user quantum communication system using QFT is robust, secure and scalable.

5 Advantages of the Proposed System

The following are the advantages of the proposed system.

1. Increased Security between the transmitter or receiver and router using CDMA codes. Using simple C-NOT gates at the transmitter and receiver side has greatly increased the security between end-users and routers.
2. Increasing the difficulty for eavesdropper to guess the Qubit being exchanged across routers by using Quantum Fourier Transform. Using Quantum Fourier Transform which transforms the Qubit from one-base to another greatly increases security by spreading the each user information across multiple new basis vectors. This QFT is typically carried out in Quantum computers. The eavesdropper must also have an equal or more stronger Quantum Computer to get the CDMA encoded data. Still the user data is secure from eavesdropping.
3. Enabling hierarchical network topology by using QFT scaling. QFT can be scaled linearly from N to N+1 Qubits order unlike classical DFT where scaling happens on powers of 2.

6 Results and Discussion

In this paper a novel Multi-user Quantum Communication system using CDMA and QFT has been proposed. The proposed system uses qubits to exchange data between transmitter and receiver in the Quantum internet using quantum switches or routers.

The proposed network architecture provides security and scalability. The security between the transmitter or receiver and router is by using CDMA codes and the mathematical proof has been provided for the same.

The need for increasing the difficulty for eavesdroppers to guess the qubit being exchanged across routers done by using Quantum Fourier Transform and its inverse IQFT. The mathematical treatment for the same has been provided in this paper.

The scalability is also derived from the fact that QFT can be scaled linearly. The proposed system is robust and can be implemented with minimal requirement of C-NOT gate at the user side and QFT at the router or switches thereby making it an elegant Multi-User Quantum Communication System.

7 Conclusion and Future Works

In conclusion, the paper has provided a new out-look on the quantum internet for a multi-user scalable network. The physical realization is still some time away and there are many new on-going methods to optimize the QFT system. The future works would include optimizing the overall system on the number of quantum gates and simplifying the QFT system.

Acknowledgment. The authors would like to acknowledge the time resource provided by Centre for Development of Telematics, Bengaluru, India.

References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information, 2nd edn. Cambridge University Press/Massachusetts Institute of Technology, Cambridge (2000)
2. Qubit Wikipedia. https://en.wikipedia.org/wiki/Qubit. Accessed 9 Oct 2020
3. Quantiki. https://www.quantiki.org/wiki/quantum-gates. Accessed 9 Oct 2020
4. Science Direct. https://www.sciencedirect.com/topics/computer-science/quantum-circuit. Accessed 9 Oct 2020
5. Sharma, V., Banerjee, S.: Quantum communication using code division multiple access network. Opt. Quant. Electron. **52**, 381 (2020). https://doi.org/10.1007/s11082-020-02494-3
6. Tan, X., Cheng, S., Li, J., Feng, Z.: Quantum key distribution protocol using quantum fourier transform. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, pp. 96–101 (2015). https://doi.org/10.1109/WAINA.2015.8
7. Kumavor, P.D., Beal, A.C., Yelin, S., Donkor, E., Wang, B.C.: Comparison of four multi-user quantum key distribution schemes over passive optical networks. J. Lightwave Technol. **23**(1), 268–276 (2005). https://doi.org/10.1109/JLT.2004.834481
8. Brassard, G., Bussieres, F., Godbout, N., Lacroix, S.: Multiuser quantum key distribution using wavelength division multiplexing. In: Proceedings of SPIE 5260, Applications of Photonic Technology 6, (2003). https://doi.org/10.1117/12.543338
9. Xue, P., Wang, K., Wang, X.: Efficient multiuser quantum cryptography network based on entanglement. Sci. Rep. **7**, 45928 (2017). https://doi.org/10.1038/srep45928
10. Quirk - A drag-and-drop quantum circuit simulator. https://algassert.com/quirk. Accessed 9 Oct 2020
11. qcircuit - Macros to generate quantum ciruits. https://ctan.org/pkg/qcircuit. Accessed 9 Oct 2020