Qubit Share Multiple Access Scheme (QSMA)

Pawan Tej Kolusu(✉) and M. Anand

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

Abstract. Quantum computing has shown great advancement in recent times. With significant properties like Quantum superposition and Quantum entanglement, the time required to evaluate a function in polynomial time has reduced significantly. The meta stable nature of the Quantum bits (Qubits), has opened doors for a wide research in network optimization and security. This paper proposes a novel Multi-user Qubit sharing scheme called the QSMA. Classical bits of information can be shared among multiple transmit and receive users using minimal number of Qubits. Protocols like superdense coding have been used to encode classical bits of information to Qubits. Mathematical transformation tools like the Quantum Fourier transform (QFT) have been incorporated to enhance the security of the QSMA system.

Keywords: Quantum computing · Multi-user quantum communication · Quantum circuits · Quantum internet · QSMA · Quantum Fourier transform · Superdense coding

1 Introduction

Quantum computation, derived from Quantum physics, is an emerging field which has shown significant progress and applications in the field of networking and security. Its inbuilt properties like superposition and entanglement have made way for Quantum computers which can solve polynomial equations much faster than a classical computer. The other important application called the Quantum key distribution is widely used for security purpose.

1.1 Qubits and Measurement

Quantum computing is based on the Quantum bits or Qubits. They are a linear combination of computational basis states. The spin of an electron or a photon polarization can be considered as examples of Qubit. Mathematically, a Qubit is defined as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ are orthogonal computational basis states. α and β are complex numbers. The Qubit exists simultaneously in $|0\rangle$ and $|1\rangle$ states which is called the 'superposition'. This is said to be in a quasi

N. Kumar et al. (Eds.): UBICNET 2021, LNICST 383, pp. 91–104, 2021.
https://doi.org/10.1007/978-3-030-79276-3_8

stable state and when 'Measured', gives a stable state $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2$ or $|\beta|^2$ respectively. Also,

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1}$$

Alternately, a qubit can be written in vector form as

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{2}$$

Multiple Qubits can be represented by tensor product of individual Qubits. A system with n-Qubits can be represented as

$$|x_0 x_1 x_2 ... x_{n-1}\rangle = \sum_{k=0}^{n-1} \alpha_k |x_k\rangle \tag{3}$$

where,

$$\sum_{k=0}^{n-1} |\alpha_k|^2 = 1 \tag{4}$$

In vector form qubits can be written as

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ ... \\ \alpha_{n-1} \end{bmatrix} \tag{5}$$

1.2 Quantum Gates and Circuits

Just like classical gates, quantum computing uses quantum gates. For our reference, we have used the following quantum gates, Identity, Hadamard, Pauli-X, Pauli-Z, Controlled-NOT and Controlled-Z gates. The matrix form of the gates can be found in [1].

1.3 Quantum Fourier Transform (QFT)

In quantum computing, the quantum Fourier transform (QFT) is a linear transformation on quantum bits, and is the quantum analogue of the inverse discrete Fourier transform.

The quantum Fourier transform can be performed efficiently on a quantum computer.

In case that $|x\rangle$ is a basis state, the quantum Fourier Transform can be represented as

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{xk} |k\rangle \tag{6}$$

In case N = 4, the transformation matrix becomes

$$F_4 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \tag{7}$$

1.4 Inverse Quantum Fourier Transform (IQFT)

The inverse quantum Fourier transform (IQFT) is a linear transformation on quantum bits, and is the quantum analogue of the discrete Fourier transform.

In case that $|k\rangle$ is a basis state, the inverse quantum Fourier Transform can represented as

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{-nk} |x\rangle \tag{8}$$

In case N = 4, the transformation matrix becomes

$$IQFT_4 = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \tag{9}$$

1.5 Challenges in Multi-user Quantum Communication and Quantum Internet

Security: The classical bits which are encoded to qubits must be secure throughout the communication channel away from the risk of decoding by an evesdropper. The main challenge is to ensure security at each intermediate node. Hence the security algorithms used to encode must be complex and random in nature. The idea is to transform the qubits over a computationally large eigen basis.

Scalability: The multi-user quantum communication system must be flexible for upgradation to higher order system using minimal changes.

Optimization: The multi-user quantum communication system involves large number of mathematical transformations. Hence more number of gates are required to evaluate when compared to a classical communication system.

1.6 The Paper is Arranged as Follows

The proposed Multi-User Quantum Communication System Model using QSMA is illustrated in Sect. 2. This section includes basic architecture for a n-user system using QSMA. QSMA for 2-user system is described in Sect. 3. Mathematical model for2-user system is provided in Sect. 4. Simulations are present in Sect. 5. Section 6 lists the advantages of the proposed system. Results and Discussion are in Sect. 7. Section 8 provides the conclusion and future works planned for this proposed system. The last section provides acknowledgment followed by references used in this paper.

2 Multi-user Quantum Communication Using QSMA

A multi-user quantum communication network system for 2K transmitter users and 2K receiver users is proposed. Figure 1 shows K transmitter side users sending Classical Binary Bits to QSMA Transmitter 1 which converts these binary bit sequence to Qubit using Super Dense Coding. The output of these are sent to transmitter side switch which does QFT operation. At the receiver side the IQFT is performed by Receiver side Switch and send the recovered qubits to QSMA receivers, which in turn does Superdense decoding and send binary bits to respective users.

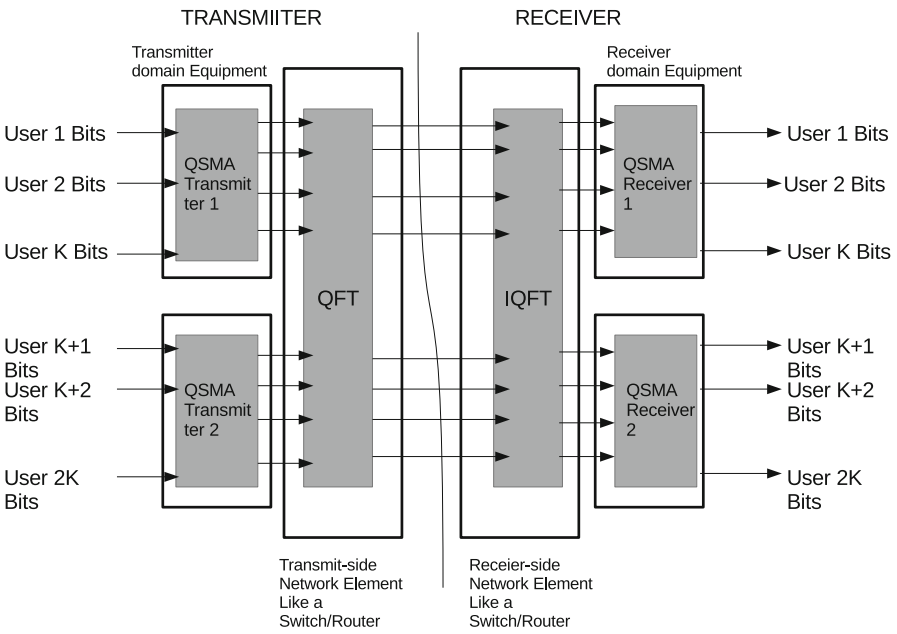

Fig. 1. Multi user QSMA system

2.1 Qubit Share Multiple Access Scheme (QSMA)

The idea of QSMA is to multiplex the classical user bits using the proposed QSMA circuit. The QSMA circuit contains multiple Superdense coding circuits based on the number of Users. For example, let us consider the case where 4 classical data bits is considered. We need 2 superdense coding circuits to implement the same. Our Qubit sharing idea starts with a multiplexing unit say M embedded in our QSMA circuit. Our theory is based on the fact that these four data bits can come from different number of cases/Users as shown below

1. Two users with two classical bits each.
2. Three Users, with U1- 1bit, U2- 1 bit and U3- 2 bits.
3. Four Users with each one classical bit.

As we can see, all the above 3 cases can be accommodated using our proposed QSMA circuit for 4 classical bits. Our following sections describe in detail about case-1.

2.2 Super Dense Coding

The superdense coding can be divided into three steps as given below [4].

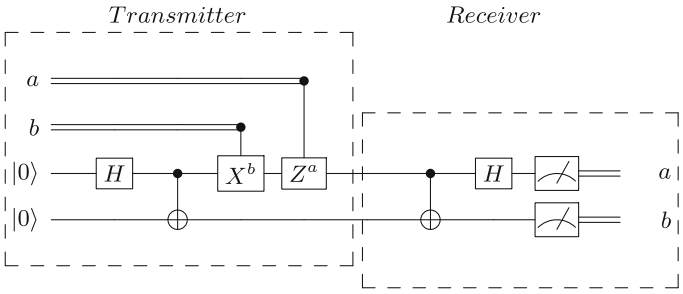

Fig. 2. Superdense coding circuit

Step1: Entangled Bell Pair. The Superdense coding starts with a third party say Charlie which has two Qubits. These two Qubits are processed to form an entangled Bell pair. The step by step procedure to form an entangled Bell pair state is given below. Both the Qubits are initially set to $|00\rangle$. Then, a Hadamard gate (H) is applied on the first Qubit $|0\rangle$ to create the superposition $|+\rangle$. So we get the state as,

$$|+0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{10}$$

After that, a CNOT gate (CX) is applied using the first Qubit $|+\rangle$ as a control and the second Qubit $|0\rangle$ as the target. Here we get the entangled bell pair state as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{11}$$

Step2: Superdense Encoding. Charlie sends the entangled Bell pair Qubits to two people, say Alice and BOB. Alice receives the first Qubit and BOB receives the second Qubit. The main idea of this protocol is for Alice to send 2 classical bits of information to Bob using her qubit. But before Alice sends, she needs to apply a set of quantum gates to her qubit depending on the 2 bits of classical information she wants to send to BOB. This is achieved using a controlled Z and a controlled NOT gate in sequence as shown in Fig. 2.

The Table 1 shows the Quantum gates required for encoding each pair of classical bits:

There are 4 cases based on two-bit strings a and b:

Table 1. Superdense encoding table

a	b	Quantum gate	Final state
0	0	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) = \|\beta_{00}\rangle$
0	1	X	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle) = \|\beta_{01}\rangle$
1	0	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle) = \|\beta_{10}\rangle$
1	1	XZ	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle) = \|\beta_{11}\rangle$

Step3: Superdense Decoding. Alice then sends its encoded qubit to BOB and BOB uses his qubit to decode Alice's message. Bob applies a CNOT gate using the Alice's qubit as control and Charlie's Qubit as target. BOB then applies a Hadamard gate and performs a measurement on both qubits to extract Alice's message. The step by step decoding process is shown in Table 2.

Table 2. Superdense decoding table

Initial state	After CNOT	After H	a	b
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\|00\rangle$	0	0
$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|11\rangle)$	$\|01\rangle$	0	1
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\|10\rangle$	1	0
$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|11\rangle)$	$\|11\rangle$	1	1

3 Proposed Qubit Share Multiple Access Scheme for 2-Users

3.1 Transmitter Side Modulation

For demonstration purpose we consider a 2-User system with two classical bits each. Let a_1 and b_1 be the classical bits of User1 and a_2 and b_2 be the classical bits of User2.

Superdense Encoding. Let the 3rd party provide four Qubits $|Q_1Q_2Q_3Q_4\rangle$ for encoding the four classical data bits using super dense coding. For a n User system we use n-Superdense coding circuits. Initially

$$|Q_1Q_2Q_3Q_4\rangle = |0000\rangle \tag{12}$$

We use two superdense encoding circuits for 2-users as shown in Fig. 3. Based on Sect. 2.2, let the classical bits $[a_1b_1]$ of User-1 be encoded using the Qubits $|Q_2Q_1\rangle$ using the quantum gates as specified in Table 1. Similarly let the classical bits $[a_2b_2]$ of User-2 be encoded using the Qubits $|Q_3Q_4\rangle$. Let the system state after superdense encoding be

$$|Q_{1S}Q_{2S}Q_{3S}Q_{4S}\rangle \tag{13}$$

Quantum Fourier Transform (QFT). Quantum fourier transform is used as a channel encoding method to modulate the superdense encoded Qubits. For a n-User system we use n-Qubit QFT model. For example for a 2-User system, we use 2- Qubit QFT model. The superdense encoded Qubits $|Q_{2S}\rangle$ and $|Q_{3S}\rangle$ are passed through the QFT block as shown in Fig. 3. Please note that we send only these two Qubits for QFT encoding as the transformation is required only on these two Qubits. Then, the system state after QFT encoding becomes

$$|Q_{1S}Q_{2SE}Q_{3SE}Q_{4S}\rangle \tag{14}$$

3.2 Receiver Side Demodulation

Inverse Quantum Fourier Transform (IQFT). The received signal is passed through the IQFT block as shown in Fig. 3. After IQFT, the superdense encoded Qubits $|Q_{2s}\rangle$ and $|Q_{3s}\rangle$ are recovered. So, the system state after IQFT decoding becomes

$$|Q_{1S}Q_{2S}Q_{3S}Q_{4S}\rangle \tag{15}$$

3.3 Superdense Decoding

Based on Sect. 2.2, we decode the classical bits of User-1 and User-2. We use two superdense decoding circuits as shown in Fig. 3. Let the system state after superdense decoding be

$$|Q_{1SD}Q_{2SD}Q_{3SD}Q_{4SD}\rangle \tag{16}$$

3.4 Measurement and User Bit Recovery

After measuring the four Qubits $|Q_{1SD}\rangle$, $|Q_{2SD}\rangle$, $|Q_{3SD}\rangle$ and $|Q_{4SD}\rangle$ we get the classical bits b_1, a_1, a_2 *and* b_2 respectively as shown in Fig. 3.

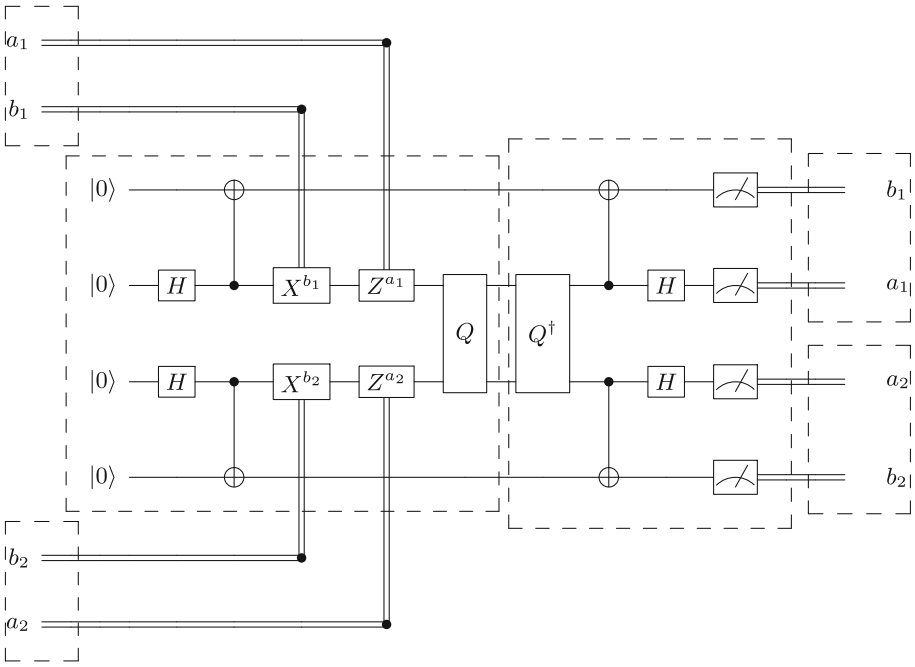

Fig. 3. Proposed QSMA circuit for 2-users

4 Mathematical Example for 2-User System

Considering a 2-User system, where the transmit User-1 classical bits are $[a_1 b_1] = [01]$ and transmit User-2 classical bits are $[a_2 b_2] = [10]$.

4.1 Superdense Encoding

Each User has a superdense coding circuit. Hence for each User, computation can be done separately using two Qubits. The upper section

$$|Q_2 Q_1\rangle \tag{17}$$

is for User-1 and the lower section

$$|Q_3 Q_4\rangle \tag{18}$$

is for User-2.

Note: For Upper section as per Fig. 3, the superdense coding circuit is upside down. Hence the order $|Q_2 Q_1\rangle$ is considered henceforth.

For User-1, the initial state is

$$|Q_2Q_1\rangle = |00\rangle \tag{19}$$

After applying Hadamard gate and C-NOT gate, we get the entangled state as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{20}$$

After applying 'X' gate on $|Q_2\rangle$, we get the state as

$$|Q_{2S}Q_{1S}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{21}$$

For User-2, the initial state is

$$|Q_3Q_4\rangle = |00\rangle \tag{22}$$

After applying Hadamard gate and C-NOT gate, we get the entangled state as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{23}$$

After applying 'Z' gate on $|Q_3\rangle$, we get the state as

$$|Q_{3S}Q_{4S}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{24}$$

4.2 QFT

2-Qubit QFT is applied to the two superdense encoded Qubits $|Q_{2S}\rangle$ and $|Q_{3S}\rangle$. let the system state after QFT be

$$|Q_{1S}Q_{2SE}Q_{3SE}Q_{4S}\rangle \tag{25}$$

4.3 IQFT

IQFT on the received signal will give the initial superdense coded Qubits because $QFT * IQFT = I$ as shown in Fig. 4 So, then the system state after IQFT will be

$$|Q_{1S}Q_{2S}Q_{3S}Q_{4S}\rangle \tag{26}$$

After IQFT, For User-1, the state is

$$|Q_{2S}Q_{1S}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{27}$$

After IQFT, For User-2, the state is

$$|Q_{3S}Q_{4S}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{28}$$

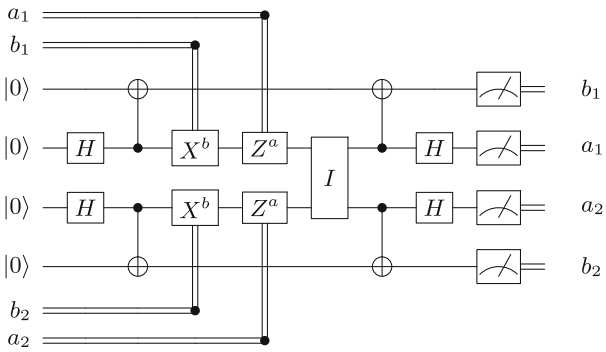

Fig. 4. Indentity property of QFT and IQFT blocks

4.4 Superdense Decoding

For Superdense decoding, first a controlled-NOT is applied
For User-1, the state becomes

$$\frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \tag{29}$$

For User-2, the state becomes

$$\frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \tag{30}$$

Then, after applying Hadamard gate,
For User-1, the state becomes

$$|Q_{2SD}Q_{1SD}\rangle = |01\rangle \tag{31}$$

For User-2, the state becomes

$$|Q_{3SD}Q_{4SD}\rangle = |10\rangle \tag{32}$$

4.5 Measurement and User Bit Recovery

After measuring the four Qubits $|Q_{2SD}\rangle$, $|Q_{1SD}\rangle$, $|Q_{3SD}\rangle$ and $|Q_{4SD}\rangle$ we get the classical bits a_1 = '0', b_1 = '1', a_2 = '1' and b_2 = '0' respectively.

5 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.

In this simulation the classical data for user 1 is shown in the top two lines. The classical data for user 2 is shown in the bottom two lines. Lines 3 and 4

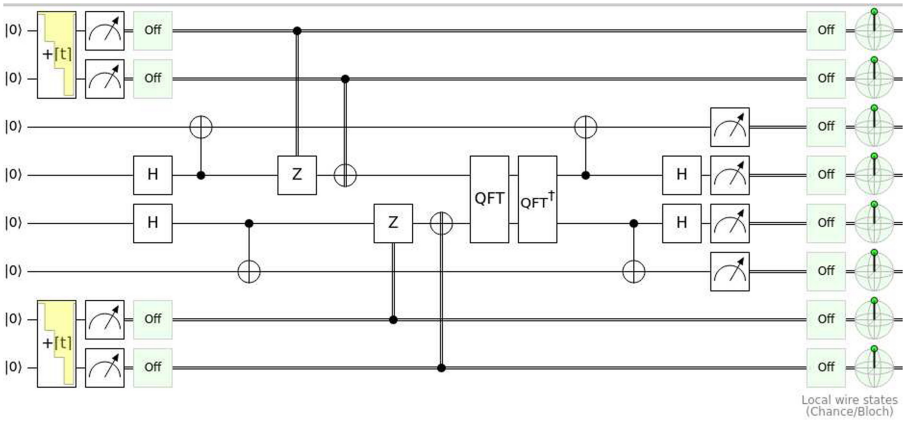

Fig. 5. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $a_1 = 0$ and $b_1 = 0$ and $a_2 = 0$ and $b_2 = 0$.

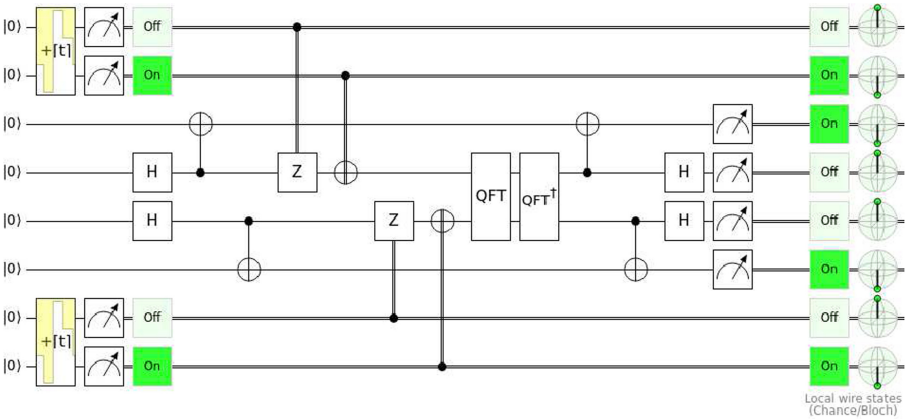

Fig. 6. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $a_1 = 0$ and $b_1 = 1$ and $a_2 = 0$ and $b_2 = 1$.

simulate the superdense codingcircuit for user-1 and lines 5 and 6 simulate the superdense coding circuit for user-2. The 2 encoded qubits on one lines 4 and 5 are fed to the QFT module at the switch. The Output of the QFT is transmitted to the receiver side router/switch over the Quantum Internet. At the receiver side router/switch, Inverse QFT is performed and the first 2 qubits on lines 3 and 4 are sent to User 1 at receiver and the next 2 Qubits on lines 5 and 6 are sent to user 2 at receiver side. At the receiver, C-NOT operation followed by Hadamard is performed on lines 3,4,5 and 6. The resulting Qubits on lines 3,4,5 and 6 are measured. The 4 measured outputs are in classical form. As expected, the receiver data is matching with classical data sent. These simulation results show that the proposed multi-user Quantum Communication system using QFT

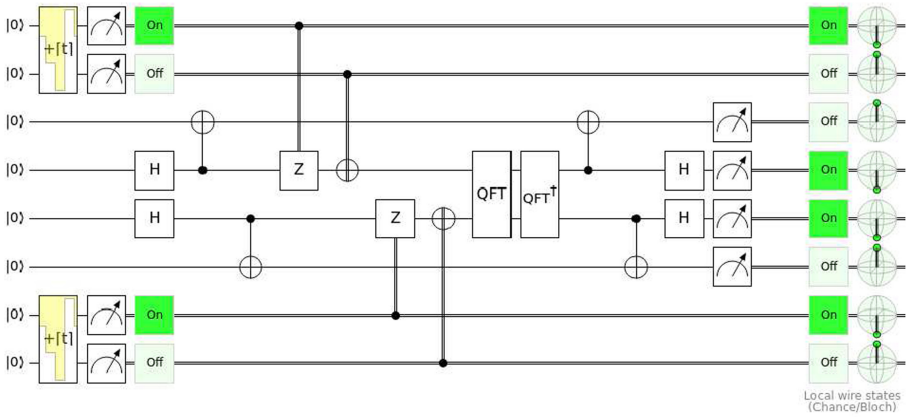

Fig. 7. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $a_1 = 1$ and $b_1 = 0$ and $a_2 = 1$ and $b_2 = 0$.

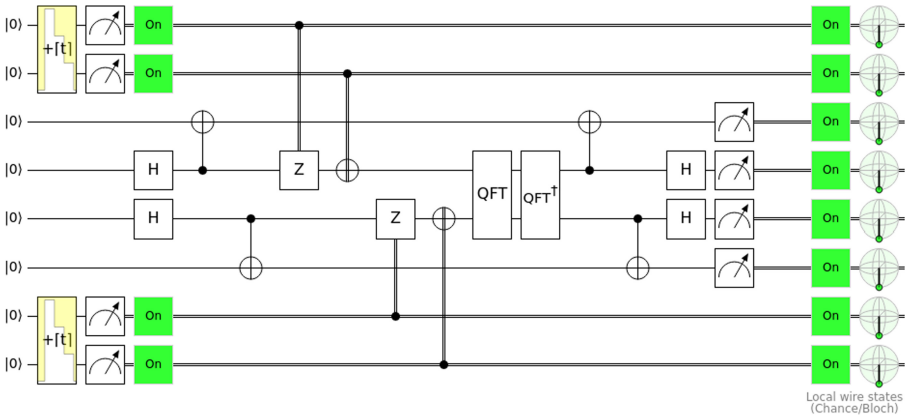

Fig. 8. Quantum communication network simulation for 2 transmit users and 2 receive users with user data bits $a_1 = 1$ and $b_1 = 1$ and $a_2 = 1$ and $b_2 = 1$.

is secured and can be scaled for more number of users. Simulation results for 4 different combinations of classical bits are shown in Fig. 5, Fig. 6, Fig. 7 and Fig. 8.

6 Advantages of the Proposed System

The following are the advantages of the proposed Multi User system.

1. Optimization: Minimal number of Qubit operations are required for implementation. With the help of super dense coding, only one qubit is modified by the User Alice using quantum gates and QFT.

2. Added security: The quantum fourier transform (QFT) adds additional security over the standard super dense coding. It becomes highly difficult for the evesdropper to decode the qubits.

3. Scaling: The proposed 2-User system can be scaled to a n-User system linearly. One has to only use higher number of superdense coding circuits and higher order QFT and IQFT blocks.

4. User data multiplexing using QSMA: The user data bits can be multiplexed in various combinations using the proposed QSMA scheme. This enhances the robustness of the Multi-user system.

7 Results and Discussion

In this paper, a multi user communication system is proposed using QSMA. It is shown that the user classical bits can be transmitted and received using superdense coding. The QFT/ IQFT encoding/decoding at the core network provides extra security making it difficult for the evesdropper to decode the user bits. Simulation results for various combination of classical bits are also shown. The mathematical model for the proposed system is also shown. The QSMA system for higher number of users can be implemented as the proposed system is scalable. One has to only use higher number of superdense coding circuits and higher order QFT and IQFT blocks. Different ways of combining user data using a multiplexing unit is also shown.

8 Conclusion and Future Works

In conclusion, the paper has provided a novel multi-user scalable network for the quantum internet. Though the practical implementation might take time, but owing to the recent advancement in quantum physics, one can be optimistic for realizing a physical system in near future. The future works would include optimizing the total number of qubits used in the core network system. This would reduce the complexity and time while keeping the security of classical bits intact.

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 1 Nov 2020
3. Quantiki. https://www.quantiki.org/wiki/quantum-gates. Accessed 1 Nov 2020

4. QISKIT Super dense coding. https://qiskit.org/textbook/ch-algorithms/superdense-coding.html. Accessed 1 Nov 2020
5. Science Direct. https://www.sciencedirect.com/topics/computer-science/quantum-circuit. Accessed 1 Nov 2020
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 1 Nov 2020