MULTIPARTY QUANTUM TELECOMMUNICATION USING QUANTUM FOURIER TRANSFORMS

DO NGOC DIEP[1,2]

Abstract. Consider the problem: Alice wishes to send the same key to $n-1$ users (Bob, Carol,. . . , Nathan), while preventing eavesdropper Eve from acquiring information without being detected. The problem has no solution in the classical cryptography but in quantum telecommunication there are some codes to solve the problem. In the paper [3], Guo-Jyun Zeng, Kuan-Hung Chen, Zhe-Hua Chang, Yu-Shan Yang, and Yao-Hsin Chou from one side and Cabello in [1] from other side, used Hadamard gates, Pauli gates in providing the quantum communication code for two-partity telecommunication with 3 persons and then generalized it to the case of arbitrary number of participants, indicating the position of measurements of participants. We remark that the Hadamard gate with precising the position of measurement is the same as Fourier transform for two qubits and hence use the general Fourier transform for n entangled qubits, in place of Hadamard gates. The result is more natural for arbitrary n qudits.

1. Introduction

The paper is devoted to the following problem of multiparty quantum telecommunication, see [1] for more details: Alice wishes to send a sequence of random classical bits (a key) to Bob, and at the same time preventing that Eve acquires information without being detected.

This problem, as known has no solution by classical cryptography, but it can be solved in quantum telecommunication by using the quantum computing. There are some tools to solve the problems: Some peoples use the non-cloning principle, some ones use entanglement particles, some others combine quantum techniques with classical private amplification and compression techniques, or split out the information in several qubits to which eavesdropper Eve has only a sequential access.

In the works [1] and [3] the problem was solved by a procedure that we will remind in the next sections 2. In those code, the Hadamard gates were used to makes measurement of entangled Bell states and/or general entangled GHZ-states some times with indication of position to

make measurements and directions[3]. We remark that in the last the Hadamard gates $\boxed{\mathrm{H}}$ can be replaced by a more general quantum Fourier transform $\boxed{F_n}$ and the Fourier coefficients can be considered as the results of measurement, which is called *quantum Fourier measurements*. In section 3 we show how to measure the quantum Fourier transform coefficients. and in section 4 we show how to use it to solve the general problem of multipartite quantum telecommunication. Our main results are Definition 3.1 and Theorem 4.1. In section 5 we remind of security estimation and in Section 6 we illustrate the codes with the holographic softwares and finally in Section 7 we make some final conclusion is made.

2. The two-party quantum telecommunication

The problem of two-party quantum teleportation between 3 persons can be formulated as follows. There three persons, Alice and Bob and Carol, who want to exchange their idea, Alice is some leader and Bob and Carol are participants. In other word, Alice, Bob and Carol have the secret key S_A, S_B and S_C respectively. And the final key is $S_A \oplus S_B \oplus S_C$ and that each participant can change the key by their idea, see [1], [3] for more details.

In practice the problem appears in some specialized context, namely [1]:

A. Hillery-Buek-Berthiaume secret sharing using GHZ states "Alice wants to have a secret action taken on her behalf in a distant part. There she has two agents, Bob and Carol, who carry it out for her. Alice knows that one and only one of them is dishonest, but she does not know which one. She cannot simply send a secure message to both of them, because the dishonest one will try to sabotage the action, but she knows that if both carry it out together, the honest one will keep the dishonest one from doing any damage."

B. Multiparty key distribution based on Bell-state entanglement swapping and and Pauli actions Supposed to consider the same situation but produce another protocol for secret sharing using Bell states instead of GHZ states is proposed, but also some Pauli gates σ_z, σ_x. This was later develloped in the work [3].

C. Secret sharing using Bell-state and GHZ entanglement swapping Supposed to consider the same situation but produce a protocol such that once Bob and Carol knows the results of the public measurement, he/she can infer the first bit of the result of Alices secret measurement and then use the public measurements from Alice they in cooperating together, can infer the second.

The four steps solution of the problem from can be summerized as follows, see [1] for more details.

Step i. Initialization: Alice uses 5 qubits: 1 and 2 (unmoving) in Bell state, and 3 (unmoving), A and B (moving for interchange) in GHZ state
Carol has 2 qubits: 4(unmoving) and C(moving) in Bell state
Bob has 2 qubits: 5(unmoving) and D (moving) in Bell state

↓ Alice measures the Bell state in qubits 1 and 2,
Alice measures GHZ state in qubits 3, A and B,
Carol measures the Bell state in qubits 4 and C
Bob measures the Bell state in qubits 5 and D

After that the system is for example, namely in the initial state:
$|\psi_i\rangle = |000\rangle_{3AB} \otimes |00\rangle_{12} \otimes |00\rangle_{4C} \otimes |00\rangle_{5D}$

Step ii. Bell-state measurements

↓ - Alice sends qubit A to Bob, qubit B to Carol
- Bob performs a Bell-state measurement on qubits 5 and D
- Carol performs a Bell-state measurement on qubits 4 and C

After that it is easy to see that the system is in the state:
$|\psi_{ii}\rangle = |AP\rangle_{12} \otimes |BP\rangle_{5D} \otimes |CP\rangle_{4C}$

Step iii. Secret Bell-state measurements.

↓ - Alice performs a *secret* Bell-state measurement on qubits 2 and 3
- Bob performs a *secret* Bell-state measurement on qubits 5 and A
- Carol performs a *secret* Bell-state measurement on qubits 4 and B

After that it is easy to see that the system is in the state:
$|\psi_{iii}\rangle = |AP\rangle_{1CD} \otimes |AS\rangle_{23} \otimes |BS\rangle_{5A} \otimes |CS\rangle_{4B}$

Step iv. Secret sharing

↓ - Bob (resp., Carol) sends qubit D (resp., C) out to Alice
- Alice performs a complete GHZ-state measurement on qubits 1, C, and Dand publishes

After that it is easy to see that the system is in the state:
$|\psi_{iv}\rangle = |AP\rangle_{1CD} \otimes |AS\rangle_{23} \otimes |BS\rangle_{5A} \otimes |CS\rangle_{4B}$

This four steps are illustrated on Figure 1.

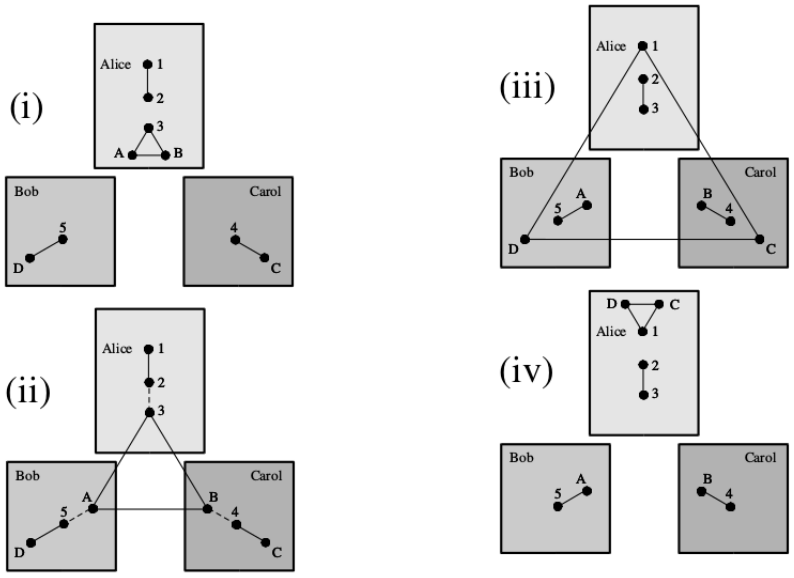

FIGURE 1. Steps 1-4:

3. Quantum Fourier Transforms as Quantum Measurements

The main tools are the entangled Bell state measurements and the entangled GHZ state measurements, which can be described as follows [3].

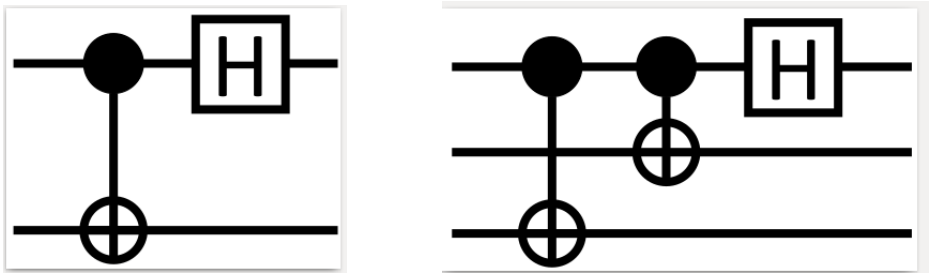

FIGURE 2. The entangled measurement (a) The entangled Bell states measurement (b) The entangled GHZ states measurement.

We remark that the schemes for entangled Bell state measurments are the same as the Fourier transform $\boxed{F_2}$ on these two qubits and entangled GHZ state measurments are the same as the Fourier transform

$\boxed{F_3}$ on three entangled qubits. The next section is devoted to the general measurements of entangled GHZ states, using the quantum Fourier transforms $\boxed{F_n}$ for and arbitrary number n of partites.

For a state $|x\rangle$ we define the Fourier coefficients in a standard basis as the results of Fourier measurement.

Definition 3.1. *For any set of entangled qubit states*

$$|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in F_2^n} e^{2\pi i \mathbf{x}.\mathbf{y}/2^n} |\mathbf{y}\rangle,$$

the Fourier coefficients are considered as the ***results of Fourier measurement****.*

Remark 3.2. *For a fixed orthonormal basis consisting of 2^n vectors of n entangled qubits in GHZ states*

$$|0\ldots0\rangle_{ij\ldots n} = \frac{1}{\sqrt{2}} \left(|0\rangle_i \otimes |0\rangle_j \otimes \cdots \otimes |0\rangle_n + |1\rangle_i \otimes |1\rangle_j \otimes \cdots \otimes |1\rangle_n\right)$$

$$|0\ldots1\rangle_{ij\ldots n} = \frac{1}{\sqrt{2}} \left(|0\rangle_i \otimes |0\rangle_j \otimes \cdots \otimes |0\rangle_n - |1\rangle_i \otimes |1\rangle_j \otimes \cdots \otimes |1\rangle_n\right)$$

. . . . . .

$$|11\ldots10\rangle_{ij\ldots n} = \frac{1}{\sqrt{2}} \left(|1\rangle_i \otimes |1\rangle_j \otimes \cdots \otimes |0\rangle_n + |0\rangle_i \otimes |1\rangle_j \otimes \cdots \otimes |1\rangle_n\right)$$

$$|11\ldots11\rangle_{ij\ldots n} = \frac{1}{\sqrt{2}} \left(|1\rangle_i \otimes |0\rangle_j \otimes \cdots \otimes |0\rangle_n - |0\rangle_i \otimes |1\rangle_j \otimes \cdots \otimes |1\rangle_n\right)$$

the Fourier transform measurements give the coefficients as the values of measurements.

Let us first remind the Quantum Fourier transform code picture, Figure 3 from Ekert lectures [2]:

4. The general case

Consider the following problem: Alice wishes to convey the same key to N users (Bob, Carol,. . . , Nathan), while preventing Eve from acquiring information without being detected. This problem, called multiparty key distribution, is a special case of networked cryptographic conferencing. Here I introduce a protocol for using GHZ states for multiparty quantum key distribution that, as far as I know, has not been presented anywhere before. It can be considered as a generalization to many parties of the two-party protocol.

Theorem 4.1. *The above multiparty quantum telecommunication problem of secret sharing with quantum key distribution can be solved by a procedure with using the quantum Fourier transform measurements.*

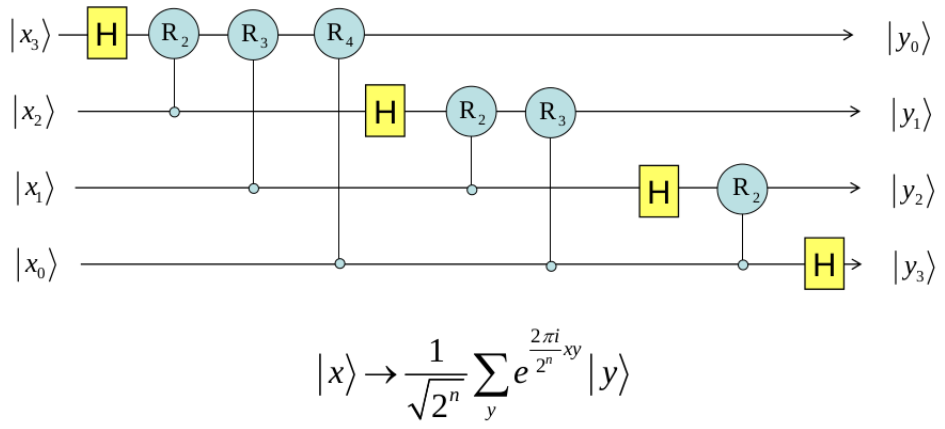

FIGURE 3. Quantum Fourier transform measurement of multiparty entangled states

Proof. The theorem is proved by the following

Procedure, the same as in the 3 persons case [1], the system state is changing as follows.

$$|\psi_i\rangle \longrightarrow |\psi_{ii}\rangle \longrightarrow |\psi_{iii}\rangle \longrightarrow |\psi_{iv}\rangle$$

Let us consider in more details.

Step 1. Initialization of 3n qubits. Alice has $n+2$ qubits: $1, 2, 3, A_1, \ldots, A_{n-1}$: qubits 1 and 2 are entangled in Bell state, qubits $3, A_1, \ldots, A_{n-1}$ are entangled in GHZ state. $n-1$ persons: Bob, Carol, ..., Nathan, each has 2 entangled qubits $i+3, C_i, i = 1 \ldots, n-1$ namely in null state. Alice produces a Bell state measurement on qubit 1 and 2 and a Fourier measurement $\boxed{F_n}$ on n qubits $3, A_1, \ldots, A_{n-1}$. Each of participants makes a Bell state Fourier measurement $\boxed{F_2}$ of entangled $i+3, C_i, i = 1 \ldots n-1$. At the end of this step 1, the system is in the state

$$|\psi_i\rangle = |0 \ldots 0\rangle_{3A_1 \ldots A_{n-1}} \otimes |00\rangle_{12} \otimes |00\rangle_{4C_1} \otimes \cdots \otimes |00\rangle_{n+2,C_{n-1}}$$

Step 2. Entangled Bell-state measurements. Alice sends each qubit A_i of her GHZ state out to each i^{th} participant of the other $n-1$ users.

The system is in the state

$$|\psi_{ii}\rangle = |AP\rangle_{3A_1\dots A_{n-1}} \otimes |BP\rangle_{1C_1} \otimes |CP\rangle_{2C_2} \otimes \cdots \otimes |NP\rangle_{n+2,C_{n-1}}$$

Step 3. Secret Bell-state measurement. Next, Alice and each user performs a Bell-state Fourier measurement $\boxed{F_2}$ on the received qubit and one of their qubits. After these measurements the state of the system becomes

$$|\psi_{iii}\rangle = |AP\rangle_{3A_1\dots A_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,A_1} \otimes \cdots \otimes |NS\rangle_{n+2,A_{n-1}},$$

where $|AP\rangle$ is n-qubit GHZ state of the standard basis 3.2.

Step 4. Secret sharing. The $n-1$ users sends a qubit (the one they have not used) to Alice, and she performs a Fourier measurement $\boxed{F_n}$ to discriminate between the 2^n GHZ states, and publicly announces the result $|AP\rangle_{3C_1\dots C_{n-1}}$. After these measurements the state of the system becomes

$$|\psi_{iv}\rangle = |AP\rangle_{1C_1\dots C_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,A_1} \otimes \cdots \otimes |NS\rangle_{n+2,A_{n-1}},$$

The result AP, and the result of their own secret measurement allow each legitimate user to infer the first bit of Alices secret result AS. To find out the second bit of AS, all users (except Alice) must cooperate. The proof therefore is achieved. □

Remark 4.2. *The same is true for qudits in place of qubits. In that situation we do use the phase Fourier coefficients in place of* $\pm$.

5. Security

It was shown [1] that the protocools guarantees the security in the following sense: The secret that Alice admits has two qubits 2 and 3. by the public entangled Bell-state measurement of qubit 1 and 2, 4 and C_1, 5 and C_2 etc. and the entangled GHZ state of 1 and C_1 and C_{n-1}, every participant knows the first bit of the secret of Alice.

In order to find out the second bit of Alice's secret all $n-1$ particpand do cooperate together and following the public result of GHZ state measurement of qubits $3, A_1, \dots, A_{n-1}$ every body knows also the second bit of the qubit 3 of Alice. The Alice's secret is therefore discovered by each participant.

A eavesdropper Eve can not do change the situation: Eve need to have the same as each participant - any attempt ot find out one of the secret result of participant will change the Alice's public GHZ measurement result AP and peoples know about attempting of Eve.

Detecting Eve's presence requires the comparison of fewer bits. The probability of the result of AP to be n times false is

$$\frac{1}{2^n}\left(1+2+\cdots+2^{n-1}\right)=\frac{2^n-1}{2^n}.$$

In all these cases peoples observe the brochen results of AP and remove the telecommunication, while Eve cannot discover the secret AS.

6. Illustration with holographic softwares

In this section we review the work of A. Jaffe, Z. Liu, and A. Wozniakowski [4] involving the softwares of sharing problem. The pictures are taken from their work.

First let us remind that the measurement can also be produced with the code as shown in Figure 4

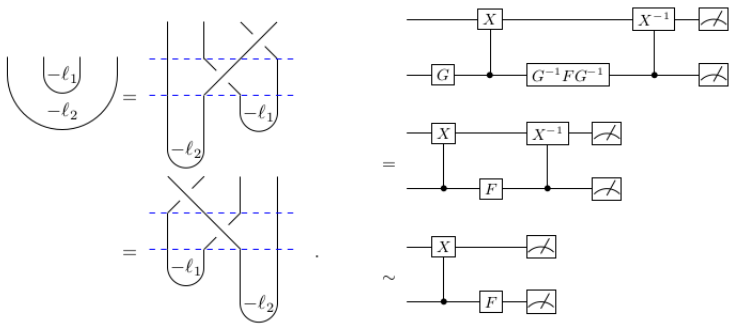

Figure 4. Measurement and corresponding code

This kind of scheme can then be applied to 1-qubit-teleport problem in Figure 5

The secret sharing problem between Alice, Bob and Carol can be illustrated as the holographic software and code in Figure 6. The scheme for Alice-Bob-Carol sharing is easily generalized as BVK code for n-partitie-sharing problem as shown in Figure 7

7. Conclusion

We proposed to use the Fourier transform measurements for entangled GHZ-state of qubits. The result is independent of indicating the positions and directions, as used in [3]. The result is certainly true also for qudits in place of qubits. The codes can be illustrated by the holographic software and corresponding codes.

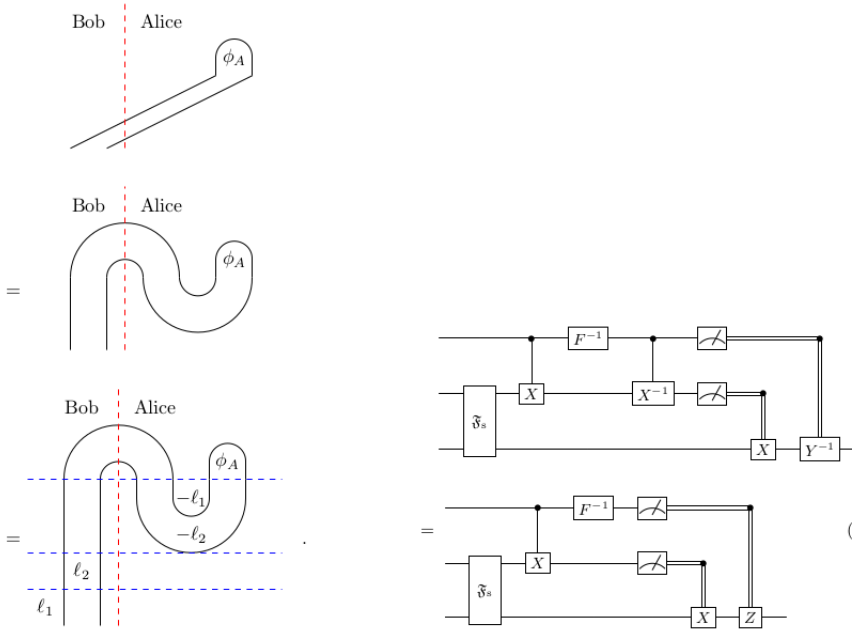

FIGURE 5. 1-qubit-teleport problem and corresponding code

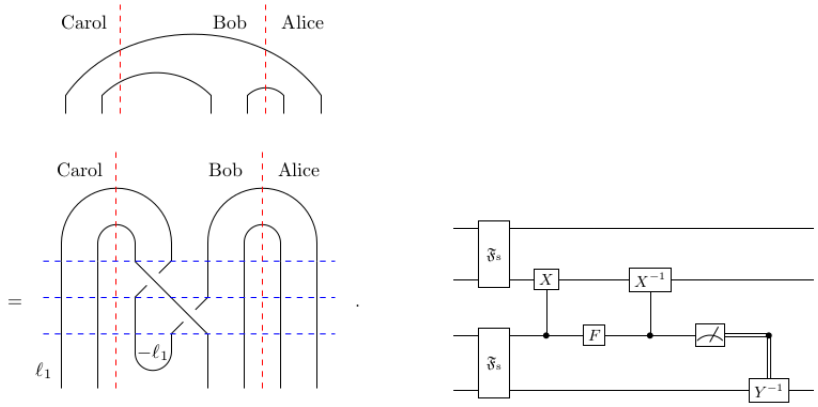

FIGURE 6. Secret sharing problem between Alice, Bob and Carol illustrated as the holographic software and corresponding code

REFERENCES

[1] A. CABELLO, *Multiparty key distribution and secret sharing based on entanglement swapping*, arXiv:quant-ph/0009025v1, 2000.

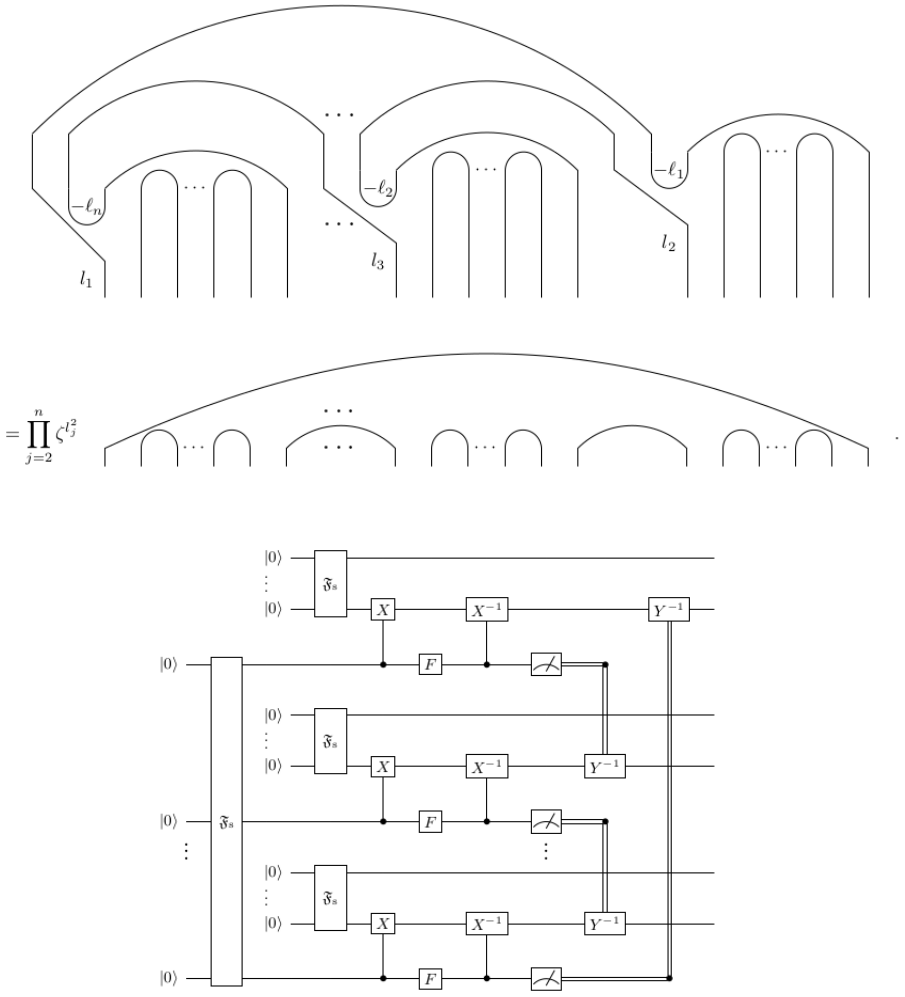

FIGURE 7. n-partitie-sharing problem and corresponding BVK code

[2] A. EKERT, P. HAYDEN AND H. INAMORI, *Basis Concepts In Quantum Computation*, Centre for Quantum Computation, University of Oxford, (2000).

[3] GUO-JYUN ZENG, KUAN-HUNG CHEN, ZHE-HUA CHANG, YU-SHAN YANG, AND YAO-HSIN CHOU, *Multiparty Quantum Key Agreement based on Quantum Secret Direct Communication with GHZ states*, arXiv:1602.00832v1[quant-ph], 2016.

[4] A. JAFFE, Z. LIU, AND A. WOZNIAKOWSKI, *Holographic Software for Quantum Networks*, https://www.researchgate.net/publication/301818865

[1] Institute of Mathematics, Vietnam National Academy of Science and Technology, Hoang Quoc Viet road, Cau Giay district, 10307 Hanoi, Vietnam

E-mail address: dndiep@math.ac.vn

[2] Thang Long University, Nghiem Xuan Yem, Hoang Mai district, Hanoi, Vietnam