International Journal of Theoretical Physics (2020) 59:1944–1955
https://doi.org/10.1007/s10773-020-04467-4

The Three-party Quantum Key Agreement Protocol with Quantum Fourier Transform

Wei Wang[1] · Bao-Min Zhou[1] · Long Zhang[1,2]

Received: 16 October 2019 / Accepted: 8 April 2020 / Published online: 7 May 2020

Abstract
Quantum key agreement(QKA) is an important part of quantum cryptography. In QKA, the final shared key must be negotiated equally by all participants, and any nontrivial subset of participants cannot fully determine the shared key. In this scheme, a novel three-party QKA with quantum fourier transform(QFT) is proposed. In addition, we utilize random numbers, decoy states and a hash function to make this protocol be resistant external attacks and participant attacks. Furthermore, the scheme can meet fairness i.e. each participant contributes fairly and equally to the final key.

Keywords Quantum key agreement · QFT · Three-party · Hash

1 Introduction

Cryptography is the basic theory of information security. As an important research content in cryptography key agreement(KA) is one form to distribute keys. As we all know KA has achieved many important achievements in the study of classical cryptography. In 1976, KA was firstly proposed by Diffe and Hellman [1]. In this article, a method for generating a key share for two-parties was proposed. Based on their idea, many KA protocols have been proposed [2–11]. However, the security of these KA protocols was based on the assumption of computational complexity. With the development of quantum algorithms and quantum computers [12, 13], the classical cryptography protocols are no longer safe. In this sense, quantum cryptography was proposed [14–19], including quantum key agreement(QKA).

Quantum cryptography combines quantum mechanics with classical cryptography and safety is independent of the computational complexity of mathematics. In quantum cryptography, QKA is an important way to distribute keys. The first QKA based on quantum

✉ Long Zhang
lzhang@hlju.edu.cn

[1] School of Mathematical Science, Heilongjiang University, Harbin, 150080, China

[2] Heilongjiang Provincial Key Laboratory of the Theory and Computation of Complex Systems, Harbin, China

teleportation with two participants was presented by Zhou et al. in 2004 [20]. In the same year, Hsueh and Chen put forward another QKA protocol with maximally entangled states [21]. However in 2009, Hwang et al. pointed out that one particular user can determine the final shared key when the QKA can not meet fairness [22, 23]. In 2010, Chong and Hwang proposed a QKA protocol based on BB84 with delayed measurement and unitary operations [24, 25].

There were only two participants in these QKA. With further research of QKA, the first multi-party quantum key agreement (MQKA) protocol with Bell States and Bell measurement was shown by Shi et al. in 2013 [26]. In the same year, Liu et al. pointed out that the protocol of Shi et al. was not safe, they proved that a dishonest participant can determine the final key [27]. At the same time, they showed that the protocol can resist internal attacks by participants with single photon. In the same year, Sun et al. improved the protocol of Liu et al. by adding two positive operations and improved its bit efficiency [28]. Many MQKA protocols [29–33] and their security analysis [34] were given. Most of the above protocols were based on single-particle or Bell states, the efficiency of bits is low. In 2016, Zhu et al. put forward a three-party QKA protocol based on two-photon entanglement states [35]. In the same year, Sun et al. proposed an MQKA protocol based on an entangled six-qubit state [36]. In 2018, Min et al. gave an MQKA protocol using G-like state and Bell state [37]. In the same year, Wang et al. presented a MQKA protocol based on the four-qubit symmetric W-state using block transmission techniques and dense coding methods [38]. Cai et al. proposed a highly efficient MQKA protocol with the five-qubit brown state. Each party performed a single-qubit unitary operations on his local part of brown state [39].

In this paper, we propose a three-party QKA with the quantum Fourier transform. We do not only utilize decoy state and auxiliary particle, but also use quantum Fourier transform(QFT), inverse quantum Fourier transform(QFT^{-1}) and Controlled-NOT CNOT operator to share the final key. According to our analysis, our protocol is secure against both outside eavesdropping attacks and inside participant attacks.

The rest of this paper is organized as follows. In Section 2, we give preliminaries of this protocol. The three-party QKA protocol is presented in Section 3. In Section 4, we give the security analysis. At last, a short discussion and conclusion are given in Sections 5 and 6, espectively.

2 Preliminaries

Some essential preliminaries are provided in this section.

2.1 The Requirements of QKA

A secure QKA protocol should meet the following three requirements:

(1) Correctness: Each participant in the protocol can get the identical shared key.
(2) Security: Both an external eavesdropper and participants cannot get any useful information about the final shared key without being detected.
(3) Fairness: All involved participants are entirely peer entities and can equally influence the final shared key.

2.2 Operations used in the Protocol

Firstly, we introduce the QFT. The QFT as the quantum version of the standard discrete Fourier operator is a linear operator on qubits. For $x, j \in \{0, 1, \cdots, N-1\}$, the QFT and the inverse QFT are defined as follows [40]:

$$QFT : |x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{x}{N} j} |j\rangle \tag{1}$$

and the corresponding QFT^{-1} is

$$QFT^{-1} : |j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \frac{j}{N} x} |x\rangle. \tag{2}$$

Obviously, it can be seen that

$$QFT^{-1}(QFT|x\rangle) = QFT^{-1}(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{x}{N} j} |j\rangle) = |x\rangle \tag{3}$$

The two sets $V_1 = \{|x\rangle\}_{x=0}^{N-1}$ and $V_2 = \{F|x\rangle\}_{x=0}^{N-1}$, are two common conjugate bases [41].

Then, the CNOT operator is introduced. The CNOT operator is that the first qubit is the control qubit, and the second qubit is the target qubit, with the form of

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4}$$

The CNOT operator: $|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$. If the control qubit sets to $|0\rangle$, the target qubit will be left alone. If the control qubit sets to $|1\rangle$, the target qubit will be flipped.

Finally, we define a phase operation as

$$U = \sum_{k=0}^{N-1} e^{2\pi i \frac{k}{N}} |k\rangle\langle k| \tag{5}$$

and

$$\begin{aligned} U|x\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{k}{N}} |k\rangle\langle k|(\sum_{j=0}^{N-1} e^{2\pi i \frac{x}{N} j} |j\rangle) \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{j}{N}(1+x)} |j\rangle \end{aligned} \tag{6}$$

According to the theoretical tools above, the three-party protocol based on QFT and random numbers is presented in the following section.

3 The Proposed Three-party QKA Protocol

Without loss of generality, three participants assume that Alice, Bob and Charlie in this QKA protocol. They want to share a key $K_A \oplus K_B \oplus K_C$ without revealing their respective

secret by agreement, here $\oplus$ denotes the bitwise Exclusive OR. Furthermore, each participant cannot know the keys of any other participants without being discovered before the final key is determined. Three participants in this protocol contribute to the final shared key fairly and equally. The three-party QKA protocol will be proposed in this section. The proposed three-party QKA protocol can be described as follows:

Step 1 Alice, Bob and Charlie respectively generate a n-bit string K_A, K_B, K_C as their private key,

$$K_A = \{a_1, a_2, \cdots, a_n\} \tag{7}$$

$$K_B = \{b_1, b_2, \cdots, b_n\} \tag{8}$$

$$K_C = \{c_1, c_2, \cdots, c_n\} \tag{9}$$

meanwhile, they generate a sequence of random numbers

$$R_A = \{r_{a1}, r_{a2}, \cdots, r_{an}\} \tag{10}$$

$$R_B = \{r_{b1}, r_{b2}, \cdots, r_{bn}\} \tag{11}$$

$$R_C = \{r_{c1}, r_{c2}, \cdots, r_{cn}\} \tag{12}$$

respectively, here $j_A = (K_A + R_A) mod N$, $j_B = (K_B + R_B) mod N$ and $j_C = (K_C + R_C) mod N$, $a_i, b_i, c_i \in \{0, 1\}$, $r_{ai}, r_{bi}, r_{ci} \in \{0, 1, \cdots N-1\}$, $i = 1, 2, \cdots, n$.

Step 2 Alice(Bob and Charlie) prepares a n-qubits state $|j_A\rangle(|j_B\rangle$ and $|j_C\rangle)$. Furthermore, $|A_k\rangle$, $|B_k\rangle$, $|C_k\rangle$ is kth qubit of $|j_A\rangle$, $|j_B\rangle$ and $|j_C\rangle$, respectively, where $k \in 1, 2, \cdots, n$. That is, the jth particle of the sequence $|j_A\rangle(|j_B\rangle$ and $|j_C\rangle)$is $|x\rangle$ if the jth bit in $j_A(j_B$ and $j_C)$ is x.

$$|j_A\rangle = |A_1\rangle|A_2\rangle \cdots |A_n\rangle \tag{13}$$

$$|j_B\rangle = |B_1\rangle|B_2\rangle \cdots |B_n\rangle \tag{14}$$

$$|j_C\rangle = |C_1\rangle|C_2\rangle \cdots |C_n\rangle \tag{15}$$

Alice(Bob and Charlie) applies QFT to the $|A_k\rangle(|B_k\rangle$ and $|C_k\rangle)$ and gets the result $|j_{A^1}\rangle(|j_{B^1}\rangle$ and $|j_{C^1}\rangle)$. That is,

$$|j_{A^1}\rangle = |A_1^1\rangle|A_2^1\rangle \cdots |A_n^1\rangle \tag{16}$$

$$|j_{B^1}\rangle = |B_1^1\rangle|B_2^1\rangle \cdots |B_n^1\rangle \tag{17}$$

$$|j_{C^1}\rangle = |C_1^1\rangle|C_2^1\rangle \cdots |C_n^1\rangle \tag{18}$$

Here,

$$|A_k^1\rangle = F|A_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{A_k}{N} j} |j\rangle \tag{19}$$

$$|B_k^1\rangle = F|B_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{B_k}{N} j} |j\rangle \tag{20}$$

$$|C_k^1\rangle = F|C_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{C_k}{N} j} |j\rangle \tag{21}$$

Step 3 Alice(Bob and Charlie) prepares n-qubits $|0\rangle$ and performs CNOT operator on $|A_k^1\rangle|0\rangle(|B_k^1\rangle|0\rangle$ and $|C_k^1\rangle|0\rangle)$, where $|A_k^1\rangle(|B_k^1\rangle$ and $|C_k^1\rangle)$ is the control qubit and each $|0\rangle$ is the target qubit. Here we can get the result state $|j_{A^2}\rangle(|j_{B^2}\rangle$ and $|j_{C^2}\rangle)$, where

$$|j_{A^2}\rangle = |A_1^2\rangle|A_2^2\rangle \cdots |A_n^2\rangle \tag{22}$$

$$|j_{B^2}\rangle = |B_1^2\rangle|B_2^2\rangle\cdots|B_n^2\rangle \tag{23}$$

$$|j_{C^2}\rangle = |C_1^2\rangle|C_2^2\rangle\cdots|C_n^2\rangle \tag{24}$$

here

$$|A_k^2\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{A_k}{N}j}|j\rangle|j\rangle_t \tag{25}$$

$$|B_k^2\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{B_k}{N}j}|j\rangle|j\rangle_t \tag{26}$$

$$|C_k^2\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{C_k}{N}j}|j\rangle|j\rangle_t \tag{27}$$

here, the subscript t denotes that the qubits used for transmission.

Step 4 Alice(Bob and Charlie) randomly selects n decoy particles in the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ inserts them into $|j\rangle_t$ to obtain the sequence $|j^*\rangle_t$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Meanwhile, Alice(Bob and Charlie) records the initial states and corresponding positions of every checking particles, and then sends the sequence $|j^*\rangle_t$ to Bob(Charlie and Alice). After confirming that Bob(Charlie and Alice) has received the sequence $|j^*\rangle_t$, the three users can calculate the error probability by comparing the measurement results with the initial states of decoy particles. If the error ratio exceeds the predetermined threshold value, she/he declares that the communication is invalid; otherwise, the process continues to the next step.

Step 5 By deleting the decoy states from $|j^*\rangle_t$, Bob(Charlie and Alice) can get the sequence $|j\rangle_t$. Bob(Charlie and Alice) applies the operator U^{B_k}(U^{C_k} and U^{A_k}) on the $|A_k^2\rangle$($|B_k^2\rangle$ and $|C_k^2\rangle$), the result state is $|j_{A^3}\rangle$($|j_{B^3}\rangle$ and $|j_{C^3}\rangle$), where, $|A_k^3\rangle$($|B_k^3\rangle$ and $|C_k^3\rangle$) is k-th state of $|j_{A^3}\rangle$($|j_{B^3}\rangle$ and $|j_{C^3}\rangle$),

$$|A_k^3\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{A_k+B_k}{N}j}|j\rangle|j\rangle_t \tag{28}$$

$$|B_k^3\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{B_k+C_k}{N}j}|j\rangle|j\rangle_t \tag{29}$$

$$|C_k^3\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{A_k+C_k}{N}j}|j\rangle|j\rangle_t \tag{30}$$

Step 6 Bob(Charlie and Alice) first randomly inserts n decoy particles into the ancillary $|j\rangle_t$, then sends them to Charlie(Alice and Bob). Each participant performs eavesdropping check as Step 4. They perform the similar process as Step 5 and the following result can be got:

$$|A_k^4\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i(\frac{A_k+B_k+C_k}{N})j}|j\rangle|j\rangle_t \tag{31}$$

$$|B_k^4\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\frac{A_k+B_k+C_k}{N})j} |j\rangle |j\rangle_t \tag{32}$$

$$|C_k^4\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\frac{A_k+B_k+C_k}{N})j} |j\rangle |j\rangle_t. \tag{33}$$

Step 7 Charlie(Alice and Bob) randomly inserts n decoy particles into the ancillary $|j\rangle_t$, each participant performs eavesdropping check as step 5. Charlie(Alice and Bob) sends ancillary $|j\rangle_t$ back to Alice(Bob and Charlie), each of them again applies $CNOT$ on her/his n qubits $|j\rangle_t$ to get the following result,

$$|A_k^5\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\frac{A_k+B_k+C_k}{N})j} |j\rangle |0\rangle_t \tag{34}$$

$$|B_k^5\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\frac{A_k+B_k+C_k}{N})j} |j\rangle |0\rangle_t \tag{35}$$

$$|C_k^5\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i (\frac{A_k+B_k+C_k}{N})j} |j\rangle |0\rangle_t \tag{36}$$

where the first n qubits are the control qubit and the corresponding n qubits of the second are the target qubit.

Step 8 After that, Alice(Bob and Charlie) measures the second n qubits of $|0\rangle_t$ in the computational basis. If the measured result is $|0\rangle$, she/he will perform the next step; otherwise she/he thinks that there are one or two dishonest participants, then this protocol will be terminated.

Step 9 At last, they applies QFT^{-1} on n qubits and measures them, they rightly get the $(j_A + j_B + j_C) mod N$.

Step 10 Alice, Bob and Charlie compute the hash value $H((j_A + j_B + j_C) mod N)$ using a pre-shared hash function H. If the hash function values are equal, Alice, Bob and Charlie will simultaneously publish random numbers R_A, R_B, R_C through the authenticated classical channel, respectively; otherwise, there is at least one dishonest participant and ends the reconstruction phase. Finally, Alice, Bob and Charlie can share the key $K_A \oplus K_B \oplus K_C$. The illustration of the presented protocol can be shown in Figs. 1 and 2.

4 Security Analysis

In this section, we will give the correctness and security analysis of the proposed three-party QKA protocol. First, we show that if all parties execute the protocol honestly, they will get the final shared key correctly. Then, we show that it is immune to attacks from internal eavesdropping. Finally, the proposed protocol is secure against external eavesdropping.

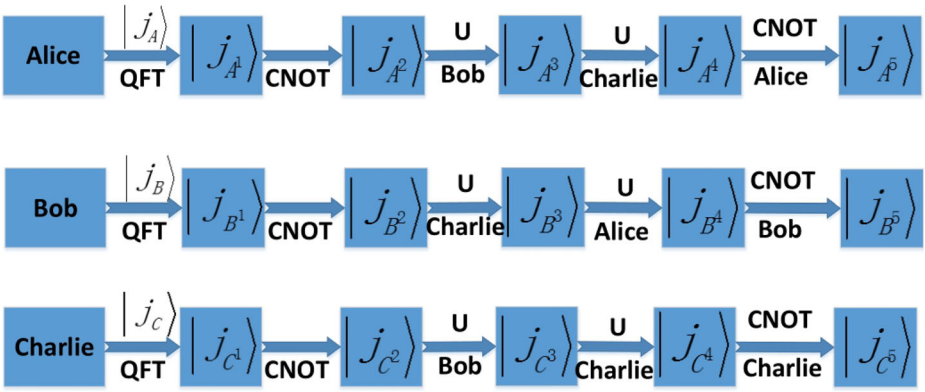

Fig. 1 The illustration of the protocol

4.1 Correctness

The correctness of the proposed protocol means that three participants can correctly share the identical key. We will give proof and analysis of the correctness of the protocol.

The correctness proof of protocol

$$1.\ U^{B_k}|A_k^2\rangle = \sum_{x=0}^{N-1} e^{2\pi i \frac{x}{N} B_k}|x\rangle\langle x|(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{A_k}{N} j}|j\rangle|j\rangle_t)$$

$$= \frac{1}{\sqrt{N}}\sum_{x,j=0}^{N-1} e^{2\pi i \frac{xB_k + A_k j}{N}}|j\rangle|j\rangle_t$$

$$= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{A_k + B_k}{N} j}|j\rangle|j\rangle_t$$

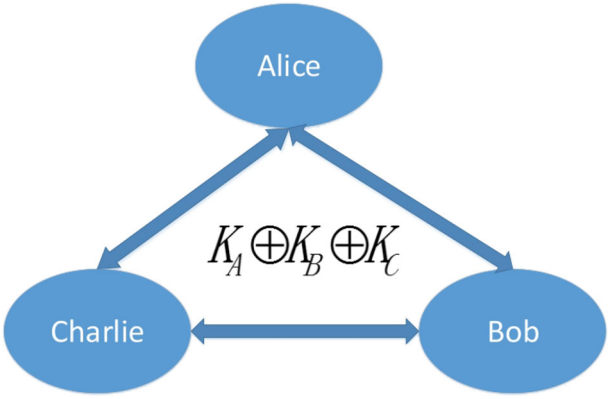

Fig. 2 The final shared key by agreement with the three participants

where, $|A_k^2\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{A_k}{N} j} |j\rangle |j\rangle_t$, $U^{B_k} = \sum_{x=0}^{N-1} e^{2\pi i \frac{x}{N} B_k} |x\rangle\langle x|$.

$$
\begin{aligned}
&2.\ QFT^{-1}(\tfrac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{j_k}{N} j} |j\rangle) \\
&= \tfrac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{j_k}{N} j} QFT^{-1} |j\rangle \\
&= \tfrac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{j_k}{N} j} (\tfrac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \frac{j}{N} x} |x\rangle) \\
&= \tfrac{1}{N} \sum_{j,x=0}^{N-1} e^{2\pi i (\frac{j_k - x}{N}) j} |x\rangle \\
&= |j_k mod N\rangle + \tfrac{1}{N} \sum_{x=0, x\neq j_k}^{N-1} (\sum_{j=0}^{N-1} e^{2\pi i (\frac{j_k - x}{N}) j} |x\rangle) \\
&= |j_k mod N\rangle + \tfrac{1}{N} \sum_{x=0, x\neq j_k}^{N-1} 0 \cdot |x\rangle \\
&= |j_k mod N\rangle
\end{aligned}
$$

where, $j_k = A_k + B_k + C_k$.

Furthermore,

$$
\sum_{j=0}^{N-1} e^{2\pi i \frac{j_k}{N} j} = \begin{cases} 0 & if j_k \neq 0 mod N \\ N & if j_k = 0 mod N \end{cases}
$$

We analyze the correctness of shared key with Alice, Bob and Charlie. After getting the state$|j_{A^5}\rangle$, according to the proof of the correctness, Alice can obtain $(j_B + j_C) mod N$ by QFT^{-1}. Alice's key is $(j_A + j_B + j_C) mod N$. After receiving the $|j_{B^5}\rangle$, Bob can get $(j_A + j_C) mod N$, his key is $(j_A + j_B + j_C) mod N$. For Charlie, he can determine $(j_A + j_B) mod N$ by $|j_{C^5}\rangle$, his key is $(j_A + j_B + j_C) mod N$. After step 10, Alice, Bob and Charlie can obtain $(R_A + R_B + R_C) mod N$. Therefore, three participants can correctly share the key final key $K_A \oplus K_B \oplus K_C$.

4.2 Internal Attack

Internal attack means that the participant determines the final key by cooperation or by himself. As known to all, internal attack is more dangerous than outside attack. Therefore, we will primarily focus on the security analysis of this protocol from internal attack. Internal attacks include joint attacks and entanglement measurement attacks, etc.

4.2.1 Joint Attack

Joint attack means that participants collaborate to obtain the final shared key information without being detected. In this protocol, we apply the random numbers and auxiliary particle to resist participant attack.

First, suppose the dishonest participants want to replace their keys with other particles, but they cannot change the final key as they expected. That's because this protocol uses auxiliary state $|0\rangle$. Each participant measures the second n qubits of $|0\rangle_t$ in step 8. If the measured result is $|0\rangle$, she/he will perform the next step; otherwise she/he will realize that there are one or two dishonest participants and end this protocol.

Then, suppose Bob and Charlie are dishonest participants and want to cooperate to determine Alice's key. After step 9, Bob and Charlie can cooperate to obtain the $j_A = (K_A + R_A) mod N$, because they cannot know Alice's random numbers R_A in advance, they cannot successfully cooperate to determine Alice's key K_A. Therefore this protocol can resistant to joint attacks.

4.2.2 Entangle-Measure Attack

The entanglement attack means that dishonest participant prepares the auxiliary particle. The dishonest participant first generates an entanglement relationship with the intercepted quantum state, then retransmits it to the other participants. At last, he obtains the final key by measuring the auxiliary particle. Without loss of generality, we suppose Alice is dishonest participant who wants to get the final key alone. In order to achieve it, she will prepare the auxiliary particle $|E\rangle$. In this scene, Alice perform a cooperate operation U_E on received state as follows:

$$U_E|0\rangle|E\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \tag{37}$$

$$U_E|1\rangle|E\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \tag{38}$$

$$U_E|+\rangle|E\rangle = \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle) \tag{39}$$

$$= \frac{1}{2}(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle) \tag{40}$$

$$U_E|-\rangle|E\rangle = \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle) \tag{41}$$

$$= \frac{1}{2}(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle) \tag{42}$$

where $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$, $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ represent decoy state. If Alice wants to introduce no error, the equation above must satisfy

$$a = d = 1, b = c = 0, |e_{00}\rangle = |e_{11}\rangle \tag{43}$$

It means that if and only if Alice particles are $|0\rangle$ or $|1\rangle$, she will not be detected. If Alice prepares $|0\rangle$ or $|1\rangle$, she will not get useful information about the final key. Alice can not get the final key without being detected. Therefore, the proposed protocol meets the security and fairness requirement.

4.3 Outside Attack

Outside attack means that the eavesdropper intercepts the key, measures retransmissions, or tampers with a resend key.

4.3.1 Intercept-Resend Attack

During transmission, suppose there is an eavesdropper Eve. Eve intercepts the particles and replaces the previous particles with new ones. He wants to perform the intercept-resend attack on the ancillary $|j\rangle_t$. However, he cannot know the positions of the decoy logical particles and the corresponding measurement bases before the eavesdropping check. Moreover, all the decoy particles are chosen from the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ randomly, the probability that Eve cannot be detected is $1/4^{\tau}$, where τ represents the number of decoy particles.

He cannot get useful information about the final key without being detected. Therefore, this protocol can resist intercept-resend attack.

5 Discussion

In this paper, we present a three-party QKA protocol based on the QFT. In the proposed protocol, random numbers and hash functions make the protocol be resistant participant attacks. The role of decoys is to resist external attacks. We use the QFT to add classical key information to the phase. For some simple forms of quantum states, we can also replace the QFT with I and X operations to encrypt the information of key. Through these methods, we can design a secure QKA protocol. In theory, it can be generalized as a model for multiparty QKA.

6 Conclusions

In all, the three-party QKA protocol based on the QFT is proposed. In addition, we utilize random numbers, decoy states and a hash function to make this protocol be resistant external attacks and participant attacks. From our analysis, each participant contributes equally and can not get the final key alone without being detected by other participants. It can be seen that this protocol meets the requirements of QKA fairness.

Acknowledgements This work is supported by National Natural Science Foundation of China under Grant No. 61802118, Open Foundation of State key Laboratory of Networking and Switching Technology (BUPT) under Grant No. SKLNST-2018-1-07, University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province under Grant No. UNPYSCT-2018015 , Hei Long Jiang Postdoctoral Foundation under Grant No.LBH-Z17048 and Natural Science Foundation of Heilongjiang Province under Grant No.LH2019F031.

References

1. Diffie, W., Hellman, M.: New directions in crypography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
2. Ingemarsson, I., Tang, D.T., Wong, C.K.: A conference key distribution system. IEEE Trans. Inf. Theory **28**, 714–719 (1982)
3. Steiner, M., Tsudik, G., Waidner, M.: Key agreement in dynamiac peer groups. IEEE Trans. Parallel Distrib. Syst. **11**, 769–780 (2000)
4. Burmester, M., Desmedt, Y.: A secure and efficient conference key distribution system. Advances in Cryptology-EUROCRYPT 1994. Lecture Notes in Computer Science **950**, 275–286 (1994)
5. Xiao, D., Liao, X., Deng, S.: A novel key agreement protocol based on chaotic maps. Inf. Sci. **177**(4), 1136–1142 (2007)
6. Han, S.: Security of a key agreement protocol based on chaotic maps. Chaos Soliton. Fract. **38**(3), 764–768 (2008)
7. Xiang, T., Wong, K., Liao, X.: On the security of a novel key agreement protocol based on chaotic maps. Chaos Soliton. Fract. **40**(2), 672–675 (2009)
8. He, D., Chen, Y., Chen, J.: Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn. **69**, 1149–1157 (2012)
9. Tan, Z.: A chaotic maps-based authenticated key agreement protocol with strong anonymity. Nonlinear Dyn. **72**, 311–32 (2013)

10. Xie, Q., Zhao, J.M., Yu, X.Y.: Chaotic maps-based three-party password authenticated key scheme. Nonlinear Dyn. **74**, 1021–1027 (2013)
11. Wang, X., Zhao, J.: An improved key agreement protocol based on chaos. Communications in Nonlinear Science and Numerical Simulation **15**, 4052–4057 (2010)
12. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on Foundation of Computer Science, Los Alamitos, pp. 124–134 (1994)
13. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, pp. 212–219 (1996)
14. Zhang, K.J., Zhang, W.W., Li, D.: Improving the security of arbitrated quantum signatureagainst the forgery attack. Quantum Inf. Process. **12**, 2655–2669 (2013)
15. Zhang, K.J., Qin, S.J., Sun, Y., Song, T.T., Su, Q.: Reexamination of arbitrated quantum signature: the impossible and the possible. Quantum Inf. Process. **12**, 3127–3141 (2013)
16. Zhang, K.J., Zhang, X., Jia, H.Y., Long, Z.: A new n-party quantum secret sharing model based on multiparty entangled states. Quantum Inf. Process. **18**, 81 (2019)
17. Yang, Y.H., Yuan, J.T., Wang, C.H., Geng, S.J., Zuo, H.J.: Locally indistinguishable generalized Bell states with one-way local operations and classical communication. Phys. Rev. A **98**, 042333 (2018)
18. Yang, Y.H., Wang, C.H., Yuan, J.T., Wu, X., Zuo, H.J.: Local distinguishability of generalized Bell states. Quantum Inf. Process. **17**, 29 (2018)
19. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014)
20. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149 (2004)
21. Hsueh, C.C., Chen, C.Y.: Quantum key agreement protocol with maximally entangled states. In: Proceedings of the 14th Information Security Conference, pp. 236–242. National Taiwan University of Science and Technology, Taipei (2004)
22. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on Quantum key agreement protocol with maximally entangled state. Int. J. Theor. Phys. **50**, 1793–1802 (2011)
23. Tsai, C.W., Chong, S.K., Hwang, T.: Comment on quantum key agreement protocol with maximally entangled states. In: Proceedings of the 20th Cryptology and Information Security Conference, pp. 210–213. National Chiao Tung University, Hsinchu (2010)
24. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
25. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**, 2097 (2004)
26. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurement. Quantum Inf. Process **12**, 921–932 (2013)
27. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multi-party quantum key agreement with single particles. Quantum Inf. Process **12**, 1797–1805 (2013)
28. Sun, Z., Zhang, C., Wang, B., Li, Q., Long, D.: Improvements on multi-party quantum key agreement with single particles. Quantum Inf. Process **12**, 3411–3420 (2013)
29. Sun, Z.W., Yu, J.P.: Wang, P.:Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process **15**, 373–384 (2016)
30. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
31. Gu, J., Hwang, T.: Improvement of Novel multi-party quantum key agreement protocol with GHZ states. Int. J. Theor. Phys. **56**, 3108–3116 (2017)
32. Cai, B.B., Guo, G.D., Lin, S.: Multi-party quantum key agreement with teleporation. Mod. Phys. Lett. B **31**, 1750102 (2017)
33. Wang, P., Sun, Z.W., Sun, X.Q.: Multi-party quantum key agreement protocol secure against collusion attacks. Quantum Inf. Process **16**, 170 (2017)
34. Huang, W., Wen, Q.Y., Liu, B., Su, Q., Gao, F.: Cryptanalysis of a multi-party quantum key agreement protocol single particles. Quantum Inf. Process **13**, 1651–1657 (2014)
35. Zhu, Z.C., Hu, A.Q., Fu, A.M.: Participant attack on three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. **55**, 1–7 (2016)
36. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
37. Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with g-like states and bell states. Int. J. Theor. Phys. **57**, 1811–1822 (2018)
38. Wang, S.S., Xu, G.B., Liang, X.Q., et al.: Multiparty quantum key agreement with four-qubit symmetric W state. Int. J. Theor. Phys. **57**(12), 3716–3726 (2018)

39. Cai, T., Jiang, M., Cao, G.: Multiparty quantum key agreement with five-qubit brown states. Quantum Inf. Process. **17**(5), 103 (2018)
40. Diao, Z.J., Huang, C.F., Wang, K.: Quantum counting: algorithm and error distribution. Acta Appl Math. **118**, 147–159 (2012)
41. Wang, Q.L., Yu, C.H., Gao, F., Qi, H.Y., Wen, Q.Y.: Self-tallying quantum anonymous voting. Phys. Rev. A **94**, 022333 (2016)