Quantum cryptography based on the Deutsch-Jozsa algorithm

Koji Nagata,[1] Tadao Nakamura,[2] and Ahmed Farouk[3, 4, 5]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
[2] *Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
[3] *Computer Sciences Department, Faculty of Computers and Information, Mansoura University*
[4] *University of Science and Technology, Zewail City of Science and Technology, Giza, Egypt*
[5] *Scientific Research Group, Egypt*

(Dated: July 2, 2017)

Recently, secure quantum key distribution based on Deutsch's algorithm using the Bell state is reported [35]. Our aim is of extending the result to a multipartite system. In this paper, we propose a highly speedy key distribution protocol. We present secure quantum key distribution based on a special Deutsch-Jozsa algorithm using Greenberger-Horne-Zeilinger states. Originally, Bob has promised to use a function f which is of one of the two kinds; either the value of $f(x)$ is constant for all x, or the value of $f(x)$ is balanced, that is, it is equal to 1 for exactly half of all the possible x, and 0 for the other half. Here, Bob uses a special function when it is not constant. We may say the value of $f(x)$ is special. Our quantum key distribution overcomes a classical counterpart by a factor $O(2^N)$.

PACS numbers: 03.67.Lx, 03.67.Ac, 03.67.Dd
Keywords: Quantum computation architectures and implementations, Quantum algorithms, protocols, and simulations, Quantum cryptography

I. INTRODUCTION

The quantum theory (cf. [1–6]) gives approximate and at times remarkably accurate numerical predictions. Much experimental data approximately fits to the quantum predictions for the past some 100 years. We may not doubt the correctness of the quantum theory. The quantum theory, in these days, keeps saying modern science with respect to information theory, where the science is called the quantum information theory [6]. Therefore, the quantum theory gives us another very useful theory in order to create new information science and to explain the handling of raw experimental data in our physical world.

As for foundations of the quantum theory, Leggett-type non-local variables theory [7] is experimentally investigated [8–10]. The experiments report that the quantum theory does not accept Leggett-type non-local variables interpretation. However, there are debates for the conclusions of the experiments. See Refs. [11–13].

Meanwhile, as for applications of the quantum theory, implementation of a quantum algorithm to solve Deutsch's problem [14–16] on a nuclear magnetic resonance quantum computer is reported firstly [17]. An implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [18]. There are several attempts to use single-photon two-qubit states for quantum computing. Oliveira *et al.* implement Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [19]. Single-photon Bell states are prepared and measured [20]. Also the decoherence-free implementation of Deutsch's algorithm is reported by using such single-photon and by using two logical qubits [21]. More recently, a one-way based experimental implementation of Deutsch's algorithm is reported [22]. In 1993, the Bernstein-Vazirani algorithm was reported [23, 24]. It can be considered as an extended Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was reported [25]. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer is reported [26]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits is discussed [27]. Quantum learning robust against noise is studied [28]. A quantum algorithm for approximating the influences of Boolean functions and its applications is recently reported [29]. Quantum computation with coherent spin states and the close Hadamard problem is also discussed [30]. Transport implementation of the Bernstein-Vazirani algorithm with ion qubits is more recently reported [31]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [32]. Finally, we mention that the dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [33].

On the other hand, the earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than classical counterpart with a magnitude that grows exponentially with the number of qubits. In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [34]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [35].

In this paper, we present secure quantum key distribution based on a special Deutsch-Jozsa algorithm by using Greenberger-Horne-Zeilinger (GHZ) state [36, 37]. Originally, Bob has promised to use a function f which is of one of the two kinds; either the value of $f(x)$ is constant for all x, or the value of $f(x)$ is balanced, that is, it is equal to 1 for exactly half of all the possible x, and 0 for the other half. Here, Bob uses a special function when it is not constant. We may say the value of $f(x)$ is special. Our quantum key distribution overcomes a classical counterpart by a factor $O(2^N)$. The security of the protocol is based on it in Ekert 91 protocol [38]. That is, Eve must destroy the GHZ state.

The paper is organized as follows:

In Sec. II, we review Deutsch's algorithm along with Ref. [6].

In Sec. III, we review the Deutsch-Jozsa algorithm along with Ref. [6].

In Sec. IV, we study the special Deutsch-Jozsa algorithm.

In Sec. V, we study the special Deutsch-Jozsa algorithm by using another input state. In the case, we cannot perform the special Deutsch-Jozsa algorithm.

In Sec. VI, we study the special Deutsch-Jozsa algorithm by using the GHZ state.

In Sec. VII, we discuss the fact that the special Deutsch-Jozsa algorithm can be used for quantum key distribution by using the GHZ state.

Section VIII concludes the paper.

II. A REVIEW OF DEUTSCH'S ALGORITHM

In this section, we review Deutsch's algorithm along with Ref. [6].

Quantum parallelism is a fundamental feature of many quantum algorithms. It allows quantum computers to

evaluate the values of a function $f(x)$ for many different x simultaneously. Suppose

$$f : \{0,1\} \to \{0,1\}, \tag{1}$$

is a function with a one-bit domain and range. A convenient way of computing the function on a quantum computer is to consider a two-qubit quantum computer which starts in the state

$$|x, y\rangle. \tag{2}$$

With an appropriate sequence of logic gates it is possible to transform this state into

$$|x, y \oplus f(x)\rangle, \tag{3}$$

where $\oplus$ indicates addition modulo 2. We give the transformation defined by the map

$$|x, y\rangle \to |x, y \oplus f(x)\rangle, \tag{4}$$

a name, U_f.

Deutsch's algorithm combines quantum parallelism with a property of quantum mechanics known as interference. Let us use the Hadamard gate to prepare the first qubit

$$|0\rangle, \tag{5}$$

as the superposition

$$(|0\rangle + |1\rangle)/\sqrt{2}, \tag{6}$$

but let us prepare the second qubit as the superposition

$$(|0\rangle - |1\rangle)/\sqrt{2}, \tag{7}$$

using the Hadamard gate applied to the state

$$|1\rangle. \tag{8}$$

The Hadamard gate is as $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ or equivalently

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 1| + |1\rangle\langle 0| + |0\rangle\langle 0| - |1\rangle\langle 1|). \tag{9}$$

Let us follow the states along to see what happens in this circuit. The input state

$$|\psi_0\rangle = |01\rangle, \tag{10}$$

is sent through two Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{11}$$

A little thought shows that if we apply U_f to the state

$$|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}, \tag{12}$$

then we obtain the state

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}. \tag{13}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } \; f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } \; f(0) \neq f(1). \end{cases} \tag{14}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle|1\rangle & \text{if } \; f(0) = f(1) \\ \pm|1\rangle|1\rangle & \text{if } \; f(0) \neq f(1). \end{cases} \tag{15}$$

So by measuring the first qubit we may determine $f(0) \oplus f(1)$. This is very interesting indeed: the quantum circuit gives us the ability to determine a global property of $f(x)$, namely $f(0) \oplus f(1)$, using only one evaluation of $f(x)$! This is faster than is possible with a classical apparatus, which would require at least two evaluations.

III. A REVIEW OF THE DEUTSCH-JOZSA ALGORITHM

The earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than classical counterpart with a magnitude that grows exponentially with the number of qubits.

Let us follow the argumentation presented in [6]. —— The application, known as *Deutsch's problem*, may be described as the following game. Alice, in Amsterdam, selects a number x from 0 to $2^N - 1$, and mails it in a letter to Bob, in Boston. Bob calculates the value of some function

$$f : \{0, \ldots, 2^N - 1\} \to \{0, 1\}, \tag{16}$$

and replies with the result, which is either 0 or 1. Now, Bob has promised to use a function f which is of one of the two kinds; either the value of $f(x)$ is constant for all x, or the value of $f(x)$ is balanced, that is, it is equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's goal is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible. How fast can she succeed?

In the classical case, Alice may only send Bob one value of x in each letter. At worst, Alice will need to query Bob at least

$$2^N/2 + 1, \tag{17}$$

times, since she may receive $2^N/2$ 0s before finally getting a 1, telling her that Bob's function is balanced. The best deterministic classical algorithm she can use therefore requires $2^N/2 + 1$ queries. Note that in each letter, Alice sends Bob N bits of information. Furthermore, in this example, physical distance is being used to artificially elevate the cost of calculating $f(x)$, but this is not needed in the general problem, where $f(x)$ may be inherently difficult to calculate.

If Bob and Alice were able to exchange qubits, instead of just classical bits, and if Bob agreed to calculate $f(x)$ using a unitary transformation U_f, then Alice could achieve her goal in just one correspondence with Bob, using the following algorithm.

Alice has an N qubit register to store her query in, and a single qubit register which she will give to Bob, to store the answer in. She begins by preparing both her query and answer registers in a superposition state. Bob will evaluate $f(x)$ using quantum parallelism and leave the result in the answer register. Alice then interferes states in the superposition using a Hadamard transformation (a unitary transformation),

$$H = (\sigma_x + \sigma_z)/\sqrt{2}, \tag{18}$$

on the query register, and finishes by performing a suitable measurement to determine whether f was constant or balanced.

Let us follow the quantum states through this algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \tag{19}$$

Here the query register describes the state of N qubits all prepared in the

$$|0\rangle, \tag{20}$$

state. After the Hadamard transformation on the query register and the Hadamard gate on the answer register we have

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{21}$$

The query register is now a superposition of all values, and the answer register is in an evenly weighted superposition of $|0\rangle$ and $|1\rangle$. Next, the function f is evaluated (by Bob) using

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle, \tag{22}$$

giving

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{23}$$

Here

$$y \oplus f(x), \tag{24}$$

is the bitwise XOR (exclusive OR) of y and $f(x)$. Alice now has a set of qubits in which the result of Bob's function evaluation is stored in the amplitude of the qubit superposition state. She now interferes terms in the superposition using a Hadamard transformation on the query register. To determine the result of the Hadamard transformation it helps to first calculate the effect of the Hadamard transformation on a state

$$|x\rangle. \tag{25}$$

By checking the cases $x = 0$ and $x = 1$ separately we see that for a single qubit

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}. \tag{26}$$

Thus

$$H^{\otimes N}|x_1, \ldots, x_N\rangle = \frac{\sum_{z_1,\ldots,z_N}(-1)^{x_1 z_1 + \cdots + x_N z_N}|z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \tag{27}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \tag{28}$$

where

$$x \cdot z, \tag{29}$$

is the bitwise inner product of x and z, modulo 2. Using this equation and (23) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{30}$$

Alice now observes the query register. Note that the absolute value of the amplitude for the state

$$|0\rangle^{\otimes N}, \tag{31}$$

is

$$\sum_x (-1)^{f(x)}/2^N. \tag{32}$$

Let's look at the two possible cases — f constant and f balanced — to discern what happens. In the case where f is constant the absolute value of the amplitude for

$$|0\rangle^{\otimes N}, \tag{33}$$

is $+1$. Because

$$|\psi_3\rangle, \tag{34}$$

is of unit length it follows that all the other amplitudes must be zero, and an observation will yield

$$0, \tag{35}$$

for all N qubits in the query register. Thus, global measurement outcome is

$$0. \tag{36}$$

If f is balanced then the positive and negative contributions to the absolute value of the amplitude for

$$|0\rangle^{\otimes N}, \tag{37}$$

cancel, leaving an amplitude of zero, and a measurement must yield a result other than

$$0, \tag{38}$$

that is,

$$+1, \tag{39}$$

on at least one qubit in the query register. Summarizing, if Alice measures all 0s and global measurement outcome is 0 the function is constant; otherwise the function is balanced.

IV. A SPECIAL DEUTSCH-JOZSA ALGORITHM

In this section, we study a special Deutsch-Jozsa algorithm.

Originally, Bob has promised to use a function f which is of one of the two kinds; either the value of $f(x)$ is constant for all x, or the value of $f(x)$ is balanced, that is, it is equal to 1 for exactly half of all the possible x, and 0 for the other half. Here, Bob uses a special function when it is not constant. We may say the value of $f(x)$ is special.

We have the following when the value of $f(x)$ is special.

$$\sum_{x\in\{0,1\}^N} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} = \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}. \tag{40}$$

That is, the function has the following character:

$$f(x) = \begin{cases} 0 & \text{if } \ 1 \text{ is even in } x \\ \\ +1 & \text{if } \ 1 \text{ is odd in } x. \end{cases} \tag{41}$$

Alice's goal is to determine with certainty whether Bob has chosen a constant or a special function, corresponding with him as little as possible.

The input state

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle, \tag{42}$$

is sent through $N+1$ Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]^{\otimes N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{43}$$

We apply U_f of obtaining the following state

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{44}$$

Applying U_f (unitary operation) to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]^{\otimes N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } \ f(x) = \text{constant} \\ \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } \ f(x) = \text{special}. \end{cases} \tag{45}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle^{\otimes N}|1\rangle & \text{if } \ f(x) = \text{constant} \\ \\ \pm|1\rangle^{\otimes N}|1\rangle & \text{if } \ f(x) = \text{special}. \end{cases} \tag{46}$$

In the case we perform the special Deutsch-Jozsa algorithm.

V. FAILING THE SPECIAL DEUTSCH-JOZSA ALGORITHM

In this section, we study the special Deutsch-Jozsa algorithm by using another input state. In the case, we cannot perform the algorithm as shown below.

The input state

$$|\psi_0\rangle = |1\rangle^{\otimes N}|0\rangle, \tag{47}$$

is sent through $N+1$ Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N} \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]. \tag{48}$$

We apply U_f to the following state

$$\frac{\overbrace{|a\rangle - |b\rangle + |c\rangle - \cdots + |d\rangle}^{2^N}}{\sqrt{2^N}}|x\rangle. \tag{49}$$

If $x = 1$

$$\frac{|a\rangle|1\rangle - |b\rangle|1\rangle + |c\rangle|1\rangle - \cdots + |d\rangle|1\rangle}{\sqrt{2^N}}, \tag{50}$$

we have

$$\frac{|a\rangle|\overline{f(a)}\rangle - |b\rangle|\overline{f(b)}\rangle + |c\rangle|\overline{f(c)}\rangle - \cdots + |d\rangle|\overline{f(d)}\rangle}{\sqrt{2^N}}, \tag{51}$$

and if $x = 0$

$$\frac{|a\rangle|0\rangle - |b\rangle|0\rangle + |c\rangle|0\rangle - \cdots + |d\rangle|0\rangle}{\sqrt{2^N}}, \tag{52}$$

we have

$$\frac{|a\rangle|f(a)\rangle - |b\rangle|f(b)\rangle + |c\rangle|f(c)\rangle - \cdots + |d\rangle|f(d)\rangle}{\sqrt{2^N}}. \tag{53}$$

Thus,

$$\frac{|a\rangle(|f(a)\rangle + |\overline{f(a)}\rangle) - |b\rangle(|f(b)\rangle + |\overline{f(b)}\rangle) + |c\rangle(|f(c)\rangle + |\overline{f(c)}\rangle) - \cdots + |d\rangle(|f(d)\rangle + |\overline{f(d)}\rangle)}{\sqrt{2^N}}. \tag{54}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] & \text{if} \quad f(x) = \text{constant} \\ \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] & \text{if} \quad f(x) = \text{special.} \end{cases} \tag{55}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|1\rangle^{\otimes N}|0\rangle & \text{if} \quad f(x) = \text{constant} \\ \\ \pm|1\rangle^{\otimes N}|0\rangle & \text{if} \quad f(x) = \text{special.} \end{cases} \tag{56}$$

In the case we fail of performing the special Deutsch-Jozsa algorithm.

VI. THE SPECIAL DEUTSCH-JOZSA ALGORITHM USING THE GHZ STATE

In this section, we study the special Deutsch-Jozsa algorithm by using the GHZ state.
The input state

$$|\psi_0\rangle = \frac{|1\rangle^{\otimes N}|0\rangle + |0\rangle^{\otimes N}|1\rangle}{\sqrt{2}}, \tag{57}$$

is sent through $N + 1$ Hadamard gates to give

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] + \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]). \tag{58}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \pm\frac{1}{\sqrt{2}}(\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]), \tag{59}$$

if $f(x) =$ constant, or

$$|\psi_2\rangle = \pm\frac{1}{\sqrt{2}}(\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]^{\otimes N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]), \tag{60}$$

if $f(x) =$ special. The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm\dfrac{|1\rangle^{\otimes N}|0\rangle \pm |0\rangle^{\otimes N}|1\rangle}{\sqrt{2}} & \text{if } f(x) = \text{constant (GHZ)} \\ \pm\dfrac{|1\rangle^{\otimes N}|0\rangle \pm |1\rangle^{\otimes N}|1\rangle}{\sqrt{2}} & \text{if } f(0) = \text{special (separable).} \end{cases} \tag{61}$$

So by measuring the qubits (by means of the GHZ measurement) we may determine $f(x)$ is constant or special. The GHZ measurement is explained as follows: Alice and Bob prepare the following GHZ basis

$$\begin{aligned} |\Psi_+\rangle &= \frac{|1\rangle^{\otimes N}|0\rangle + |0\rangle^{\otimes N}|1\rangle}{\sqrt{2}}, \\ |\Psi_-\rangle &= \frac{|1\rangle^{\otimes N}|0\rangle - |0\rangle^{\otimes N}|1\rangle}{\sqrt{2}}, \\ |\Phi_+\rangle &= \frac{|1\rangle^{\otimes N}|1\rangle + |0\rangle^{\otimes N}|0\rangle}{\sqrt{2}}, \\ |\Phi_-\rangle &= \frac{|1\rangle^{\otimes N}|1\rangle - |0\rangle^{\otimes N}|0\rangle}{\sqrt{2}}. \end{aligned} \tag{62}$$

If the state $|\psi_3\rangle$ is the GHZ state, we have

$$|\langle\psi_3|\Psi_+\rangle|^2 = 1 \;\text{ or }\; |\langle\psi_3|\Psi_-\rangle|^2 = 1 \;\text{ or }\; |\langle\psi_3|\Phi_+\rangle|^2 = 1 \;\text{ or }\; |\langle\psi_3|\Phi_-\rangle|^2 = 1. \tag{63}$$

Therefore the measurement outcome should be 1 if the function is constant. If the state $|\psi_3\rangle$ is a separable state, we have

$$|\langle\psi_3|\Psi_+\rangle|^2 = 1/2 \;\text{ or }\; |\langle\psi_3|\Psi_-\rangle|^2 = 1/2 \;\text{ or }\; |\langle\psi_3|\Phi_+\rangle|^2 = 1/2 \;\text{ or }\; |\langle\psi_3|\Phi_-\rangle|^2 = 1/2. \tag{64}$$

Therefore the measurement outcome should not be 1 if the function is special.

VII. QUANTUM KEY DISTRIBUTION BASED ON THE SPECIAL DEUTSCH-JOZSA ALGORITHM

We discuss the fact that the special Deutsch-Jozsa algorithm can be used for quantum key distribution by using the GHZ state.

Alice and Bob have promised to use a function f which is of one of the two kinds; either the value of f is constant or special. To Eve, it is secret. Alice's and Bob's goal is to determine with certainty whether they have chosen a constant or a special function without information of the function to Eve. If the function is constant the output qubits are fullly entangled (the GHZ state), otherwise a separable state. Alice and Bob perform the GHZ measurement mentioned above. Alice and Bob share one secret bit if they determine the function f by getting a suitable measurement outcome. Eve destroys fully entangled state into separable state. The security of our protocol is based on it in Ekert 91 protocol [38].

- First, Alice prepares the entangled qubits, applies the Hadamard transformation to the state, and sends the output state described in the GHZ state to Bob.
- Next, Bob randomly picks a function "f" that is either special or constant and Bob applies U_f. He then sends the N qubits to Alice.
- Finally, Alice and Bob perform the GHZ measurement. She learns whether f was special or constant. If the final qubits are fully entangled, then the function is constant. If the final qubits are not the GHZ state, then the function is special - Alice and Bob now share a secret bit of information (the "type" of $f(x)$).
- The result of the GHZ measurement is 1 if the function is constant.

- Alice and Bob compare a subset of all the results of the GHZ measurements when the function is constant; all of them should be 1.
- Eve must destroy the GHZ state (Ekert 91).
- Eve is detected in the following case; The result of the GHZ measurement is not 1 and the function is constant.

In conclusion, we have shown that the special Deutsch-Jozsa algorithm can be used for secure quantum key distribution. The security is based on it in Ekert 91 protocol. Our quantum key distribution overcomes a classical counterpart by a facter $O(2^N)$.

VIII. CONCLUSIONS

In conclusion, we have presented quantum key distribution based on a special Deutsch-Jozsa algorithm by using Greenberger-Horne-Zeilinger states. Originally, Bob has had promised to use a function f which is of one of the two kinds; either the value of $f(x)$ is constant for all x, or the value of $f(x)$ is balanced, that is, it is equal to 1 for exactly half of all the possible x, and 0 for the other half. Here, Bob has used a special function when it is not constant. We may have said the value of $f(x)$ is special. Our quantum key distribution has overcome a classical counterpart by a factor $O(2^N)$.

[1] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, New Jersey, 1955).
[2] R. P. Feynman, R. B. Leighton, and M. Sands, *Lectures on Physics, Volume III, Quantum mechanics* (Addison-Wesley Publishing Company, 1965).
[3] M. Redhead, *Incompleteness, Nonlocality, and Realism* (Clarendon Press, Oxford, 1989), 2nd ed.
[4] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Netherlands, 1993).
[5] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley Publishing Company, 1995), Revised ed.
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[7] A. J. Leggett, Found. Phys. **33**, 1469 (2003).
[8] S. Gröblacher, T. Paterek, R. Kaltenbaek, Č. Brukner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, Nature (London) **446**, 871 (2007).
[9] T. Paterek, A. Fedrizzi, S. Gröblacher, T. Jennewein, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. Lett. **99**, 210406 (2007).
[10] C. Branciard, A. Ling, N. Gisin, C. Kurtsiefer, A. Lamas-Linares, and V. Scarani, Phys. Rev. Lett. **99**, 210407 (2007).
[11] A. Suarez, Found. Phys. **38**, 583 (2008).
[12] M. Żukowski, Found. Phys. **38**, 1070 (2008).
[13] A. Suarez, Found. Phys. **39**, 156 (2009).
[14] D. Deutsch, *Proc. Roy. Soc. London Ser. A* **400**, 97 (1985).
[15] D. Deutsch and R. Jozsa, *Proc. Roy. Soc. London Ser. A* **439**, 553 (1992).
[16] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. Roy. Soc. London Ser. A* **454**, 339 (1998).
[17] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).
[18] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) **421**, 48 (2003).
[19] A. N. de Oliveira, S. P. Walborn, and C. H. Monken, J. Opt. B: Quantum Semiclass. Opt. **7**, 288-292 (2005).
[20] Y.-H. Kim, Phys. Rev. A **67**, 040301(R) (2003).
[21] M. Mohseni, J. S. Lundeen, K. J. Resch, and A. M. Steinberg, Phys. Rev. Lett. **91**, 187903 (2003).
[22] M. S. Tame, R. Prevedel, M. Paternostro, P. Böhi, M. S. Kim, and A. Zeilinger, Phys. Rev. Lett. **98**, 140501 (2007).
[23] E. Bernstein and U. Vazirani, Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11-20 (1993), doi:10.1145/167088.167097.
[24] E. Bernstein and U. Vazirani, SIAM J. Comput. 26-5, pp. 1411-1473 (1997).
[25] D. R. Simon, Foundations of Computer Science, (1994) Proceedings., 35th Annual Symposium on: 116-123, retrieved 2011-06-06.
[26] J. Du, M. Shi, X. Zhou, Y. Fan, B. J. Ye, R. Han, and J. Wu, Phys. Rev. A **64**, 042306 (2001).
[27] E. Brainis, L.-P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. **90**, 157902 (2003).
[28] A. W. Cross, G. Smith, and J. A. Smolin, Phys. Rev. A **92**, 012327 (2015).
[29] H. Li and L. Yang, Quantum Inf. Process. **14**, 1787 (2015).
[30] M. R. A. Adcock, P. Hoyer, and B. C. Sanders, Quantum Inf. Process. **15**, 1361 (2016).
[31] S. D. Fallek, C. D. Herold, B. J. McMahon, K. M. Maller, K. R. Brown, and J. M. Amini. New J. Phys. **18**, 083030 (2016).

[32] D. N. Diep, D. H. Giang, and N. Van Minh, Int J Theor Phys (2017) 56: 1948. doi:10.1007/s10773-017-3340-8.
[33] W. Jin, Quantum Inf. Process. **15**, 65 (2016).
[34] K. Nagata and T. Nakamura, Open Access Library Journal, 2: e1798 (2015), http://dx.doi.org/10.4236/oalib.1101798.
[35] K. Nagata and T. Nakamura, Int J Theor Phys (2017) 56: 2086. doi:10.1007/s10773-017-3352-4.
[36] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, The Netherlands, 1989), pp. 69-72.
[37] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[38] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).