Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in d-level Quantum System

Duc Manh Nguyen & Sunghwan Kim

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 58
Number 1

Int J Theor Phys (2019) 58:71-82
DOI 10.1007/s10773-018-3910-4

Volume 58 • Number 1 • January 2019

International Journal of Theoretical Physics

10773 · ISSN 0020-7748
58(1) 1–332 (2019)

Springer

International Journal of Theoretical Physics (2019) 58:71–82
https://doi.org/10.1007/s10773-018-3910-4

Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in *d*-level Quantum System

Duc Manh Nguyen[1] · Sunghwan Kim[1]

Received: 4 June 2018 / Accepted: 1 October 2018 / Published online: 12 October 2018

Abstract

In this paper, we consider the modified generalization of the Deutsch-Jozsa algorithm in the d-level (qudits) quantum system to determine the types of the function f (*constant* or *linear*) that had been used. A comparison of the efficiency between the quantum algorithm and the classical case have been given. In addition, the quantum key distribution protocol based on the algorithm is established to show the contribution of our work to the improvement in the detecting the Eve's attack that occurs in the protocol based on the original Deutsch-Jozsa algorithm.

Keywords Quantum information theory · Quantum algorithm · Quantum cryptography · Quantum key distribution protocol

1 Introduction

The quantum mechanics, which gives approximate and at times remarkably accurate numerical predictions is successful in explaining and predicting many phenomena [1, 2]. The efficiency involved in quantum mechanics has often been demonstrated. One of the interesting applications of quantum principles is their application to information theory [3], which is a result of the effort to generalize classical information theory leading to the quantum computer. The field of quantum computing was first introduced by Richard Feynman in 1982 [4]. Digital computers based on transistor gates, that requires data to be encoded into binary digits. In contrast, quantum computer utilizes the properties of molecules to present data and subsequently

✉ Sunghwan Kim
sungkim@ulsan.ac.kr

Duc Manh Nguyen
nguyenmanhduc18@gmail.com

[1] School of Electrical Engineering, University of Ulsan, 93 Daehak-ro, Nam-gu, Ulsan 44610, Korea

quantum computer performs the operation on these data representation, wherein the superposition of quantum states and entanglement are involved [5]. A theoretical model is the quantum Turing machine, also known as a universal quantum computer, which shares theoretical similarities with non-deterministic and probabilistic computers, including the ability to be in more than one state simultaneously.

An important milestone in quantum computing occurred in 1994 when Shor published a computationally efficient quantum algorithm for factoring integers and for evaluating discrete algorithms [6]. With these algorithms, the owner of the quantum computer could crack popular, highly utilized public key cryptosystems. In addition, Grover discovered a quantum algorithm for the important problem of searching unstructured databases, yielding a substantial speed-up over classical search algorithms. To protect the data privacy, the need for highly accurate and scalable simulation technologies then became important to access the practical feasibility and foresee difficulties in the practical implementation of theoretical achievements [7]. The performance of quantum algorithms promised significant improvements, and many quantum algorithms have thus been proposed. The simplest quantum algorithm, as originally proposed by Deutsch is concerned with the function from the set {0,1} to the set {0,1} to solve a slightly contrived problem [8]. In 1992, Deutsch and Jozsa produced a deterministic algorithm which was generalized to a function which takes n bits for its input. Unlike Deutsch's algorithm, this algorithm required two function evaluations instead of only one. Further improvements to the Deutsch-Jozsa algorithm were made by Cleve et al. [9], resulting in an algorithm that is both deterministic and requires only a single query of function f. This algorithm is referred to as the Deutsch-Jozsa algorithm in honour of the ground-breaking techniques employed and demonstrates that quantum computation is faster than the classical counterpart with a magnitude that grows exponentially with the number of qubits. It also provided inspiration for Shor's and Grover's algorithms, two of the most revolutionary quantum algorithms. Hence, a great deal of research has been carried out to improve and apply the Deutsch-Jozsa algorithm, such as for the initialization-free generalized Deutsch-Jozsa [10] and energy-based computing [11]. In 2015, it was shown that the Deutsch-Jozsa algorithm can be used for quantum key distribution [12, 13]. Subsequently, secure quantum key distribution based on a special Deutsch-Jozsa algorithm using an entangled state [14] and using a special function [15] was proposed.

Originally, the purpose of the Deutsch-Jozsa algorithm is to determine the type of function f that had been used (*balanced* or *constant*) via quantum system by using only one query. The main aim of this paper is to propose a modified generalization of the Deutsch-Jozsa algorithm in a d-level (qudits) system to determine the type of function f (*constant* or *linear*) used. The proposed algorithm also required only one query in comparison with the classical case. In addition, the quantum key distribution protocol based on the algorithm is discussed to show the contributions of our work to improving the detection of Eve's attack, which cannot be distinguished by the protocol based on the original Deutsch-Jozsa algorithm.

The organization of this paper is as follows. In the next section, we review the basic theory of quantum information in qubits and its generalization in the qudits system, and we review the Deutsch-Jozsa algorithm and its generalization in the qudits system. In section III, we propose the modified generalization Deutsch-Jozsa algorithm in the qudits system. It is demonstrated that the proposed quantum key distribution protocol based on the Deutsch-Jozsa algorithm overcomes the weakness of the previous protocol based on the original Deutsch-Jozsa algorithm. Finally, the conclusions are presented in section IV.

2 Basic Quantum Information

2.1 Quantum Bits and Quantum Gates

A bit is a unit of information describing a two-dimensional (2D) classical system. The term "bit' in computing has several meanings, such as electricity traveling through a circuit (high) or not travelling through a circuit (low), a way to denote "true" or "false", or a switch turned on or off. We usually write such opposing states as 0 and 1, or F and T, … A quantum bit or a qubit is a unit of information describing a 2D quantum system. The two-basis state $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and a qubit shall be represented by a 2-by-1 matrix with a complex number, as the superposition of two basis states: $|a\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0|0\rangle + c_1|1\rangle$. As the norm condition for qubits, the following condition must be satisfied: $|c_0|^2 + |c_1|^2 = 1$. Due to the superposition concept, the state can be considered to have both values |0) and |1) at the same time, with the probability of state based on |0) and |1); hence, the amount of information that can be represented is infinite. A quantum memory is a physical system composed of n qubits; i.e. multiples of the tensor product of some qubits. Generally, the n-qubits state is denoted as:

$$|\varphi\rangle = \sum_{i=0}^{n} a_i|i\rangle = \sum_{i_k=\{0,1\},i=\overline{i_1 i_2 \ldots i_{n(2)}}} a_i|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle = \sum_{i_k=\{0,1\},i=\overline{i_1 i_2 \ldots i_{n(2)}}} a_i|i_1 i_2 \ldots i_n\rangle$$

A particularly effective way to understand a quantum system is to examine the behavior of the various transformations on state at any one time. A quantum system requires unitary transformations that can be represented as matrices called unitary matrices. Pauli operators have been used as the basis for all unitary matrices as the properties of commutative or anti-commutative. Hence, all the important matrices, such as controlled-NOT, phase-change, phase-shift and controlled-U are written as a combination of Pauli operators. It is well known that {AND, NOT} forms the set of the universal logical gate; hence, every logical circuit can be simulated using only the AND gate and the NOT gate. A quantum world also has universal quantum gates; one set of universal quantum gates is {Hadamard, controlled-NOT and phase-shift gate}. The Hadamard matrix plays a significant role in the quantum world and is used to change the single state into the superposition state, which has been the encoding and decoding step in many quantum algorithms. To place n qubit into the superposition, we use the tensor product of n Hadamard matrices, which we denote as $\mathbf{H}^{\otimes n}$. We define the inner product function as,

$$'' \circ '' : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

as follows: given two binary strings of length n, $x = x_0x_1 \ldots x_{n-1}$ and $y = y_0y_1 \ldots y_{n-1}$, we have:

$$x \circ y = (x_0 \cdot y_0) \oplus (x_1 \cdot y_1) \oplus \ldots \oplus (x_{n-1} \cdot y_{n-1})$$

where " · "· denotes the AND operation. We obtain the general formula for matrix $\mathbf{H}^{\otimes n}$ as,

$$\mathbf{H}^{\otimes n}[\mathbf{i}, \mathbf{j}] = \frac{1}{\sqrt{2^n}} (-1)^{\mathbf{i} \circ \mathbf{j}},$$

where **i** and **j** are the row and column numbers in the binary strings, respectively. The most significant role of the Hadamard matrix is that it transfers the arbitrary state into the superposition state, whereby the basic state $|y\rangle$ is changed by Hadamard transformation, as follows

$$\mathbf{H}^{\otimes n}|y\rangle = \frac{1}{\sqrt{2^n}}\sum\nolimits_{x\in\{0,1\}^n}(-1)^{x\circ y}|x\rangle$$

2.2 Quantum Qudits System

The generalized form of the quantum system will be one in which all the quantum states and quantum gates are replaced by their corresponding higher dimensional versions. The d-dimensional quantum state, instead of being the superposition of the basis states $|0\rangle$ and $|1\rangle$, will be the superposition of the basis states $|0\rangle$, $|1\rangle$, …, $|d-1\rangle$. Its phase will be the form $\omega^k = e^{i\frac{2\pi k}{d}}$, where ω is the d-th root of unity instead of the usual ±1. During measurement, the generalized state behaves the same way as the normal state does. It collapses into any of its basis states with the probability given by the absolute square of its coefficient. If a quantum state can be able to assume more than two levels, more information condensed into a single state.

The next logical step in our process is to design higher dimensional quantum gates capable of manipulating these states. Out of the many generalizations possible, in this paper, we look at what is perhaps the simplest and most straightforward [16]. The motivation behind defining gates in this way is that they allow the creation of a higher dimensional analogue for the quantum circuit without significant modification to the original circuit. The Hadamard gate **H** thus becomes the d-dimensional discrete Fourier transform matrix defined by

$$|j\rangle \xrightarrow{Fourier} \sum_{s=0}^{d-1}\omega^{j\cdot s}|s\rangle \xrightarrow{Fourier} |j\rangle$$

The tensor product of the d-dimensional discrete Fourier transform matrix can then be given by,

$$\mathfrak{J}^{\otimes n} = \frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{x},\mathbf{y}\in\{0,1,\dots,d-1\}^n}\omega^{\mathbf{x}\circ\mathbf{y}}|\mathbf{y}\rangle\langle\mathbf{x}| \tag{1}$$

From the Fourier operator in (1), the Fourier transforms apply to the basic d-dimensional states as follows,

$$\mathfrak{J}|d-1\rangle = \frac{1}{\sqrt{d}}\sum\nolimits_{y\in\{0,1,\dots,d-1\}}\omega^{(d-1)\cdot y}|y\rangle = \frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d-1\rangle\right], \tag{2}$$

$$\mathfrak{J}^{\otimes n}|00\ldots0\rangle = \frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{x},\mathbf{y}\in\{0,1,\dots,d-1\}^n}\omega^{\mathbf{x}\circ\mathbf{y}}|\mathbf{y}\rangle\langle\mathbf{x}||00\ldots0\rangle = \frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}\in\{0,1,\dots,d-1\}^n}|\mathbf{y}\rangle, \tag{3}$$

$$\mathfrak{J}^{\otimes n}|\mathbf{s}\rangle = \frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{x},\mathbf{y}\in\{0,1,\dots,d-1\}^n}\omega^{\mathbf{x}\circ\mathbf{y}}|\mathbf{y}\rangle\langle\mathbf{x}||\mathbf{s}\rangle = \frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}\in\{0,1,\dots,d-1\}^n}\omega^{\mathbf{s}\circ\mathbf{y}}|\mathbf{y}\rangle \tag{4}$$

2.3 Reviews of Deutsch-Jozsa Algorithm

Let us consider the function f: $\{0, 1\}^n \rightarrow \{0, 1\}$ which accepts the string of n 0's and 1's, and outputs a zero or one. The domain might be thought of any natural number from 0 to 2^{n-1}. The function f is considered as *balanced* if exactly half of the inputs go to zero (and the other half go to 1). We consider the function f to be *constant* if all the inputs go to zero or all the inputs go to one.

The Deutsch-Jozsa algorithm solves the following problem: suppose we are given the function f which we can evaluate but cannot see the way it is defined. Here, we are assured that the function is either *balanced* or *constant*; let us determine whether the function is *balanced* or *constant*. Classically, this algorithm can be solved by evaluating the function on different inputs. In the best case, when we know the exactly two different inputs give two different outputs, we can have assured that the function is *balanced*. In contrast, to ensure that the function is *constant*, the function must be evaluated the function on more than half of the possible inputs. Therefore, the worst-case scenario requires $2^{n-1}+1$ function evaluation.

If we use the qubits system, instead of only classical bits, we could then solve the problem in only one correspondence, using the quantum system to exchange information, as shown in the Fig. 1, and in the following steps:

Step 1. The inputs state is

$$|\varphi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle.$$

Step 2. After the Hadamard transformation on the query register and the Hadamard gate on the answer register, we have

$$|\varphi_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{y=\{0,1\}^n} |\mathbf{y}\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]\right)$$

Step 3. We apply the function f by using the $\mathbf{U}_f$: $|x, y\rangle \rightarrow^{U_f} |x, y \oplus f(x)\rangle$, giving

$$|\varphi_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{y=\{0,1\}^n} (-1)^{f(y)} |y\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]\right)$$

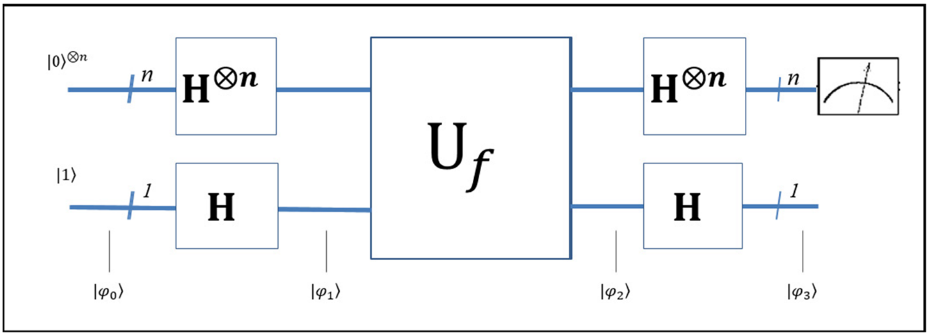

Fig. 1 Quantum system for the Deutsch-Jozsa algorithm

Step 4. Finally, we apply the Hadamard to the top qubits that are already in a superposition of different states.

$$|\varphi_3\rangle = \left(\frac{1}{\sqrt{2^n}}\sum\nolimits_{y=\{0,1\}^n}(-1)^{f(y)}|0\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]\right)$$

The top qubits become

$$\frac{1}{2^n}\sum\nolimits_{\mathbf{y}=\{0,1\}^n}(-1)^{f(y)}|0\rangle = \begin{cases} -1|0\rangle & \text{if } f(x) \text{ is } \textit{constant} \text{ at } 1, \\ +1|0\rangle & \text{if } f(x) \text{ is } \textit{constant} \text{ at } 0. \\ 0|0\rangle & \text{Since when } f(x) \text{ is } \textit{balance}, \text{ half of the } x's \text{ will cancel the other half.} \end{cases}$$

Then, when measuring the top qubits, we get only $|\mathbf{0}\rangle$ if the function is *constant*. If other states, or a non- deterministic state, are found after being measured, then the function is *balanced*.

We consider the generalization of the Deutsch-Jozsa algorithm in the d-level system. The aim of the generalization of the Deutsch-Jozsa algorithm is to determine whether the function f: is *constant* or *balanced*, as f: $\{0, 1, ..., d-1\}^n \to \{0, 1, ..., d-1\}$. Function f is called a *constant* if $f(\mathbf{x}) = f(\mathbf{y})$ for all $\mathbf{x}$, $\mathbf{y} \in \{0, 1, ..., d-1\}^n$ and is *balanced* when an equal number of d^n domain values, namely d^{n-1} is mapped to each of the d elements $\{0, 1, ..., d-1\}$. If we use the qubits system, instead of only classical bits, we could then solve the problem in only one correspondence, using the quantum system to exchange information, as shown in the Fig. 1 and in following steps,

Step 1. The input state in qudits system is as follows,

$$|\psi_0\rangle = |0\rangle^{\otimes n}\otimes|d-1\rangle$$

Step 2. Instead of applying Hadamard operators, in the qudits system, we use Fourier operators to obtain the superposition as follows,

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}|\mathbf{y}\rangle\right)\otimes\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d-1\rangle\right]\right)$$

Step 3. Next, we apply the function f by using the $\mathbf{U}_f$ operator, giving

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right)\otimes\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d-1\rangle\right]\right)$$

Step 4. Finally, we apply the Fourier transformation to the top qudits that are already in a superposition of different states.

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{d^n}}\mathcal{F}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right)\right)\otimes\left(\mathcal{F}\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d-1\rangle\right]\right)\right)$$

If function *f* is *constant*, for example, *f*(**x**)=**a** for all **x**, then the top qudits become

$$\begin{aligned}\frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right) &= \frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{a}|\mathbf{y}\rangle\right)\\ &= \frac{\omega^a}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{0\circ\mathbf{y}}|\mathbf{y}\rangle\right) = \frac{\omega^a}{\sqrt{d^n}}|\mathbf{0}\rangle\end{aligned}$$

Then, the final state, $|\psi_3\rangle = \frac{\omega^a}{\sqrt{d^n}}|\mathbf{0}\rangle\otimes|d-1\rangle$.

If function *f* is *balanced*, the top qudits become

$$\begin{aligned}\frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right) &= \frac{1}{\sqrt{d^n}}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}\right)\left(\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}|\mathbf{y}\rangle\right)\right)\\ &= \frac{d^{n-1}}{\sqrt{d^n}}\left(\sum_{j=0}^{d-1}\omega^j\right)\left(\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{0\circ\mathbf{y}}|\mathbf{y}\rangle\right)\right) = \frac{\omega^a}{\sqrt{d^n}}\mathbf{0}|\mathbf{0}\rangle\end{aligned}$$

Then, when measuring the top qubits, we obtain only |**0**⟩ if the function is *constant*. If other states or a non- deterministic state is found after being measured, then the function is *balanced*.

3 Modified Generalized of Deutsch-Jozsa Algorithm

3.1 Modified Generalization of Deutsch-Jozsa Algorithm in Quantum Qudits System

Let us consider the function *f*: $\{0, 1, ..., d-1\}^n \rightarrow \{0, 1, ..., d-1\}$

$$f(\mathbf{x}) = \begin{cases}\mathbf{a} & f \text{ is called } \textit{constant}\\ \mathbf{b}\circ\mathbf{x} & f \text{ is called } \textit{linear}\end{cases}$$

where **a** and **b** are vectors of length n over $\{0, 1, ..., d-1\}$, vector **b** differs to vector **0** (all numbers are 0), operator " ∘ " denotes the inner product with modulo d, sharing between Alice in Amsterdam and Bob in Boston, and the values of **a** and **b** are hidden for Bob, and are known only by Alice. Bob selects the vector **x** from $\{0, 1, ..., d-1\}^n$, and mails it in the letter to Alice. Alice in Amsterdam promises to select the function *f* whether it is a *constant* or *linear* function, then calculates the value and returns it to Bob. Bob's goal is to determine the function chosen by Alice. We now need to determine the speed at which he can succeed?

In the classical algorithm, for the best case, Bob needs to query n times the values from $\{0, 1, ..., d-1\}^n$, which we denote as $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n$. Bob then receives the returned messages from Alice, $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_n$, respectively. Then, Bob needs to solve the following equation to obtain the value of **b** and can then find the function *f* chosen by Alice.

$$\begin{cases}\mathbf{b}\circ\mathbf{x}_1 = \mathbf{y}_1\\ \mathbf{b}\circ\mathbf{x}_2 = \mathbf{y}_2\\ \qquad\vdots\\ \mathbf{b}\circ\mathbf{x}_n = \mathbf{y}_n\end{cases}$$

For the worst case, Bob needs to query d^{n-1}+1 time to determine whether the function *f* is *constant* or linear. For example, the worst case occurred when **b**=00…01. After d^{n-1} queries, Bob first obtained the same values, but the last time, Bob obtained a different value. If Alice and Bob establish the quantum system, instead of merely exchanging the classical bit, they will only need one correspondence as follows,

Step 1. We prepare the input state as,

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |d{-}1\rangle$$

Step 2. Next, we use Fourier operators to obtain the superposition for the top states as follows,

$$|\psi_1\rangle = \mathcal{J}^{\otimes n}\left(|0\rangle^{\otimes n}\right) \otimes \mathcal{J}\left(|d{-}1\rangle\right).$$

As the result of equation (2) and (3), we have:

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{d^n}} \sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} |\mathbf{y}\rangle\right) \otimes \left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d{-}1\rangle\right]\right)$$

Step 3. Then, we apply the type of function f by using the $\mathbf{U}_f$ operator $|x, j\rangle \rightarrow^{\mathbf{U}_f} |x, (j \oplus f(x)) \bmod d\rangle$, giving:

$$\begin{aligned}
&|\psi_2\rangle = \mathbf{U}_f\left(\left(\frac{1}{\sqrt{d^n}} \sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} |\mathbf{y}\rangle\right) \otimes \left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d{-}1\rangle\right]\right)\right)\\
&= \frac{1}{\sqrt{d^n}} \sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \left(|\mathbf{y}\rangle \otimes \left(\left(\frac{1}{\sqrt{d}}\left[\omega^d|0+f(y)\rangle + \omega^{d-1}|1+f(y)\rangle + \ldots + \omega^1|d{-}1+f(y)\rangle\right]\right)\right)\right)\\
&= \frac{1}{\sqrt{d^n}} \sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \left(|\mathbf{y}\rangle \otimes \left(\left(\frac{1}{\sqrt{d}} \omega^{f(y)}\left[\omega^{d-f(y)}|0+f(y)\rangle + \omega^{d-1-f(y)}|1+f(y)\rangle + \ldots + \omega^{1-f(y)}|d{-}1+f(y)\rangle\right]\right)\right)\right).\\
&= \left(\frac{1}{\sqrt{d^n}} \sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \omega^{f(y)} |\mathbf{y}\rangle\right) \otimes \left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d{-}1\rangle\right]\right)
\end{aligned}$$

Step 4. Finally, we apply the Fourier transformation to the top qubits that are already in a superposition of different states

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{d^n}} \mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \omega^{f(y)} |\mathbf{y}\rangle\right)\right) \otimes \left(\mathcal{J}\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d{-}1\rangle\right]\right)\right)$$

If Alice used the *constant* function *f*, for example, *f*(**x**)=**a** for all **x**. Then, the top qudits become

$$\begin{aligned}
\frac{1}{\sqrt{d^n}} \mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \omega^{f(\mathbf{y})} |\mathbf{y}\rangle\right) &= \frac{1}{\sqrt{d^n}} \mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \omega^{\mathbf{a}} |\mathbf{y}\rangle\right)\\
&= \frac{\omega^{\mathbf{a}}}{\sqrt{d^n}} \mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n} \omega^{0\circ\mathbf{y}} |\mathbf{y}\rangle\right) = \frac{\omega^a}{\sqrt{d^n}} |\mathbf{0}\rangle
\end{aligned}$$

As the equation (2), the bottom qudit becomes:

$$\mathcal{J}\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \ldots + \omega^1|d{-}1\rangle\right]\right) = |d{-}1\rangle$$

Therefore, the final state is $|\psi_3\rangle = \frac{\omega^{\mathbf{a}}}{\sqrt{d^n}} |\mathbf{0}\rangle \otimes |d{-}1\rangle$.

If Alice used the *linear* function *f*, $f(\mathbf{x}) = \mathbf{b} \circ \mathbf{x}$, we have:

$$\frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\dots,d-1\}^n}\omega^{f(\mathbf{y})}|\mathbf{y}\rangle\right) = \frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\dots,d-1\}^n}\omega^{\mathbf{b}\circ\mathbf{y}}|\mathbf{y}\rangle\right)$$
$$= \frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\dots,d-1\}^n}\omega^{\mathbf{b}\circ\mathbf{y}}|\mathbf{y}\rangle\right) = \frac{1}{\sqrt{d^n}}|\mathbf{0}\rangle$$

As the equation (2), the bottom qudit becomes:

$$\mathcal{J}\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \dots + \omega^1|d-1\rangle\right]\right) = |d-1\rangle$$

Then, the final state is $|\psi_3\rangle = \frac{1}{\sqrt{d^n}}|\mathbf{b}\rangle\otimes|d-1\rangle$.

Then, when measuring the top qubits, we obtain state |**0**) if the function type that needs to be exchanged is *constant*. If the final state is |**b**), it differs to state |**0**), the function type needing to be exchanged is *linear*. Via the quantum system, Bob and Alice need only one query to exchange the information. If Alice and Bob exchange in classical bits, for the best case, Bob needs to query *n* times, while for the worst case, Bob needs to query d^{n-1}times. In contrast, If Alice and Bob established the quantum system as shown in Fig. 1, they could exchange the information with only one query. Hence, our quantum key distribution protocol overcomes a classical counterpart by a factor of **O**(d^n).

3.2 Key Distribution Protocol Based on Modified Generalization Deutsch-Jozsa Algorithm

The modified generalization of the Deutsch-Jozsa algorithm can also be used for a quantum key distribution protocol between two parties, Alice and Bob, and the steps of the algorithm follows those shown in Fig. 2. Alice and Bob promised to use a function *f* which has two types: the values of *f* are either constant or linear. This information is hidden from Eve. Alice and Bob's goals are to determine with certainty whether Alice has chosen a constant or a linear function without revealing information about the function to Eve.

– First, Bob prepares the qubits in a separate state, the ancilla qudits: $|0\rangle^{\otimes n}\otimes|d-1\rangle$. He applies the Fourier transform to obtain the superposition entanglement state:

$$\left(\frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}=\{0,1,\dots,d-1\}^n}|\mathbf{y}\rangle\right)\otimes\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \dots + \omega^1|d-1\rangle\right]\right)$$

Bob then transfers the superposition entanglement state to Alice through the quantum channel.

– Next, Alice picks up the function *f* that is constant or linear and encrypts the key by using the $\mathbf{U}_f$ function, and the *n*+1 qudits system evolves:

$$\left(\frac{1}{\sqrt{d^n}}\sum\nolimits_{\mathbf{y}=\{0,1,\dots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right)\otimes\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle + \omega^{d-1}|1\rangle + \dots + \omega^1|d-1\rangle\right]\right)$$

Then, Alice returns the state to Bob through the quantum channel.

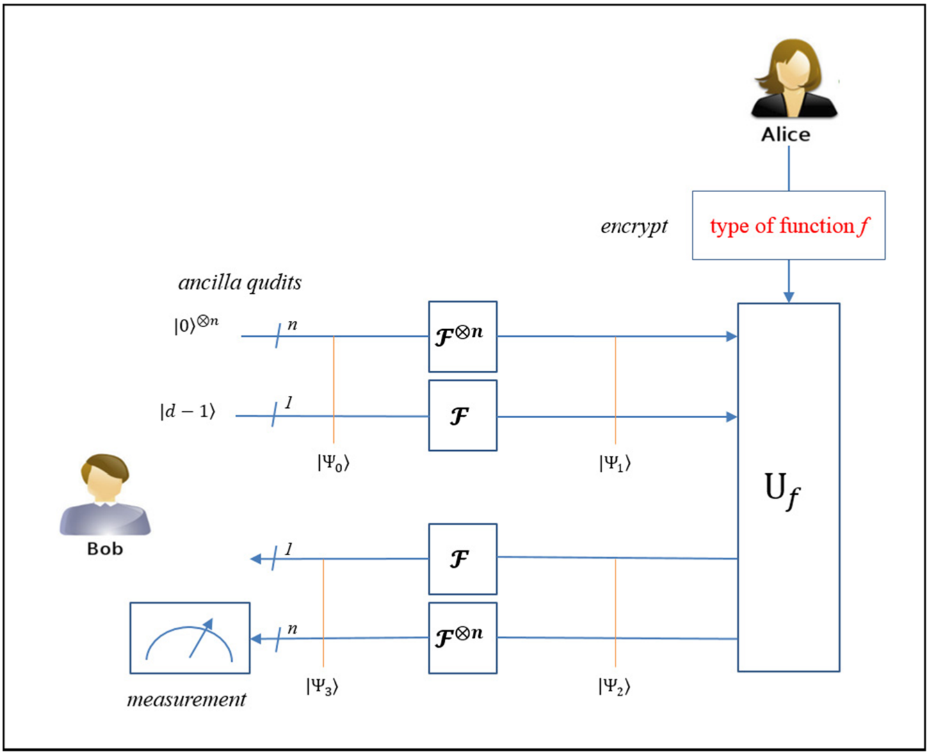

Fig. 2 Quantum key distribution protocol between Alice and Bob based on Deutsch-Jozsa algorithm

- Finally, Bob applies the Fourier transform to decrypt the key that was embedded into the channel as follows,

$$\left(\frac{1}{\sqrt{d^n}}\mathcal{J}^{\otimes n}\left(\sum\nolimits_{\mathbf{y}=\{0,1,\ldots,d-1\}^n}\omega^{f(y)}|\mathbf{y}\rangle\right)\right)\otimes\left(\mathcal{J}\left(\frac{1}{\sqrt{d}}\left[\omega^d|0\rangle+\omega^{d-1}|1\rangle+\ldots+\omega^1|d-1\rangle\right]\right)\right)$$

The final states after being decrypted differ for each case of function f that has been used. Bob prepares the measurement by the computation basis of the n qudits system: $\{\,|00\ldots0\rangle, |00\ldots1\rangle, |00\ldots2\rangle, \ldots, |00\ldots(d-1)\rangle, \ldots, |(d-1)(d-1)\ldots(d-1)\rangle\}$. Bob will learn the type of function f after his measurement. Now, Alice and Bob share a random bit of information (the type of function f).

Table 1 Comparison between protocol based on original Deutsch-Jozsa and proposal algorithm

		No Eve's attack: the final state	Eve's attack: the final state
Protocol based on original Deutsch-Jozsa	f is *balanced* function	Non-deterministic	Non-deterministic
	f is *constant* function	$\|\mathbf{0}\rangle\otimes\ \|\ d-1\rangle$	Non-deterministic
Protocol based on proposed Deutsch-Jozsa	f is *linear* function	$\|\mathbf{b}\rangle\otimes\ \|\ d-1\rangle$	Non-deterministic
	f is *constant* function	$\|\mathbf{0}\rangle\otimes\ \|\ d-1\rangle$	Non-deterministic

In the case where Eve attacks the system, the quantum cryptography is based on quantum mechanism such as the uncertainty principle, no-cloning theorem and measurement destroying the system. Therefore, Eve also prepares the computation basis of the n-qudits system: $\{|00...0\rangle, |00...1\rangle, |00...2\rangle, ..., |00...(d-1)\rangle,..., |(d-1)(d-1)...(d-1)\rangle\}$ to perform her measurement. The measurement will thereafter destroy the system. Then, the system will be disturbed, and it collapses, becoming non- deterministic.

We have shown that the generalization of the Deutsch-Jozsa algorithm can be used for securing a quantum key distribution as shown in Fig. 2. In comparison to the protocol based on the original Deutsch-Jozsa algorithm, we list all the cases of function f and the values of the final states in Table 1. As can be seen in the table, when we use the protocol based on the original quantum D-J algorithm (function f is balanced or constant), we consider the output at $|\psi_3\rangle$. If the function f is balanced, the coefficient is zero for all measurements, this means that the final state is non-deterministic. Then, Alice considers whether the line was attacked by Eve since the measurement of Eve also destroyed the system. Therefore, the conclusion that the function is balanced was not correct. In contrast, if the function f is linear, the final state is deterministic to one of the basis states. Then, the measurement gives us a certain value of probability in a basis state. Hence, if Eve attacked the system, the system would be disturbed, and Alice and Bob would be notified.

Finally, it would be interesting to determine whether the higher computational power of qudits could be exploited to improve other existing quantum algorithm, or even to design the new quantum algorithms. We expect that this will eventually be the case, and that the use of qudits can serve as a valuable tool in the development of efficient quantum algorithms. In the work in [17], the authors derive a set of one and two-qudit gates that are sufficient for universal multivalued computing (a generalization of Boolean algebra) that plays a significant role in classical and quantum theories of computation. The work shows how such gates (a generalization of binary logic gate) can be implemented by using d-level ions in the linear ion trap model.

4 Conclusions

In conclusion, we presented a modified Deutsch-Jozsa algorithm in a d-level quantum system to determine the type of function f (*linear* or *constant*) used via one query of function f. The efficiency of using a quantum algorithm in comparison to the classical case is demonstrated. In addition, the quantum key distribution protocol based on our work was established to explain the detection of Eve's attack that occurs in the protocol based on the original Deutsch-Jozsa algorithm.

Acknowledgments This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF-2016R1D1A1B03934653).

References

1. Von Neumann, J.: Mathematical Foundations of Quantum Mechanics. Princeton University Press, Princeton. In: New Jersey ((1955))
2. Feynman, R.P., Leighton, R.B., Sands, M.: Lectures on Physics. Volume III. Quantum mechanics. In: Addison-Wesley Publishing Company ((1965))
3. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, UK (2000)

4. Feynman, R.P.: Simulating Physics with Computers. Int. J. Theor. Phys. **21**, 6 (1982)
5. Yanofsky, N.S., Mannucci, M.A.: Quantum Computing for Computer Scientists. Cambridge University Press, Cambridge, UK (2008)
6. Shor, P.W.: Algorithms for quantum computation discrete logarithms and factoring. IEEE Computer Society Press. 124–134 ((1994))
7. Grover, L.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**, 325 (1997)
8. Deutsch, D., Jozsa, R.: Rapid solutions of problems by quantum computation. Proceedings of the Royal Society of London A. (1992)
9. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. Proceedings of the Royal Society of London A. **454**, 339–354 (1998)
10. Chi, D.P., Kim, J., Lee, S.: Initialization-free generalized Deutsch–Jozsa algorithm. J. Phys. A: Math. Gene. **34**, 5251–5258 (2001)
11. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A., Diep, D.N.: Creating Very True Quantum Algorithms for Quantum Energy Based Computing. Int. J. Theor. Phys. **57**, 973–980 (2018)
12. Nagata, K., Nakamura, T.: Can von Neumann's Theory Meet the Deutsch-Jozsa Algorithm? Int. J. Theor. Phys. **49**, 162–170 (2010)
13. Nagata, K., Nakamura, T.: The Deutsch-Jozsa Algorithm Can Be Used for Quantum Key Distribution. Open Access Library Journal. **2**, e1798 (2015)
14. Nagata, K., Nakamura, T. and Farouk, A.:Quantum Cryptography Based on the Deutsch-Jozsa Algorithm. Int. J. Theor. Phys. **56**, 2887-2897 (2017)
15. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A.: Secure Quantum Key Distribution Based on a Special Deutsch-Jozsa Algorithm. Asian J. Math. Phys. **2**, 6–13 (2018)
16. Daniel, G.: Fault-tolerant quantum computation with higher-dimensional systems. In: Quantum Computing and Quantum Communications, pp. 302–313, Springer Berlin Heidelberg (1999)
17. Muthukrishnan, A., Stroud, C.R.: Multivalued logic gates for quantum computation. Phys. Rev. A. **62** ((2000))