Academia Journal of Scientific Research 7(11): 000-000, November 2019
DOI: 10.15413/ajsr.2019.0713
ISSN 2315-7712

Academia Publishing

CrossMark click for updates

Research Paper

Quantum algorithm of evaluating a function and its applications to cryptography

Accepted 15th November, 2019

Koji Nagata[1]*, Do Ngoc Diep[2,3] and Tadao Nakamura[4]

[1]Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea.
[2]TIMAS, Thang Long University, Nghiem Xuan Yem Road, Hoang Mai district, Hanoi, Vietnam.
[3]Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam.
[4]Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan.

*Corresponding author. E-mail: ko–mi–na@yahoo.co.jp.

ABSTRACT

We propose quantum cryptography based on an algorithm of determining a function. The security of our cryptography is based on the Ekert (1991) protocol, that is, we use an entangled state. Eve must destroy the entangled state. Consider a function. Alice knows all the mappings concerning the function. Bob knows none of them. His aim is to obtain all of them without Eve's attack. In classical case, Bob needs some queries. In quantum case, Bob needs just a query. By measuring the single entangled state, which is sent by Alice, Bob can obtain all the mappings concerning the function, simultaneously. This is faster than classical cryptography.

Key words: Quantum cryptography and communication security, quantum communication, quantum algorithms, quantum computation, formalism.

PACS numbers: 03.67.Dd, 03.67.Hk 03.67.Ac, 03.67.Lx, 03.65.Ca

INTRODUCTION

Among a number of algorithmic developments, we can mention the following. The Bernstein—Vazirani algorithm (1993, 1997), which was first published in 1993, can be considered an extension of the Deutsch—Jozsa algorithm (Deutsch, 1985; Deutsch and Jozsa, 1992; Cleve et al., 1998). In 1994, several algorithms were proposed by Simon (1994) and Shor (1994). Grover (1996) presented strong arguments for exploring the computational possibilities offered by quantum mechanics.

In this contribution, we propose quantum cryptography based on an algorithm of determining a function. The security of our cryptography is based on the Ekert (1991) protocol, that is, we use an entangled state. Eve must destroy the entangled state. Eve means an eaves-dropper. Eve can change a secret function to another one whenever by entangled states. Bob and Alice can observe that Eve dropped in. Subsequently, we will refer to this situation simply as "Eve's attack". Consider a function. Alice knows all the mappings concerning the function. Bob knows none of them. His aim is of obtaining all of them without Eve's attack. In classical case, Bob needs some queries. In quantum case, Bob needs just a query. By measuring the single entangled state, which is sent by Alice, Bob can obtain all the mappings concerning the function, simultaneously. This is faster than classical cryptography.

QUANTUM CRYPTOGRAPHY DERIVED FROM AN ALGORITHM OF DETERMINING A FUNCTION USING QUBIT SYSTEMS

Quantum superposition is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate the mappings of a function $f(x)$ for many different (x) simultaneously. Suppose

$$f : \{0,1\} \rightarrow \{0,1\} \qquad (1)$$

is a function. Alice knows it. Bob's aim is to determine all the mappings:

$$f(0) = ?, f(1) = ?, \qquad (2)$$

That is, $f(x)$ itself without Eve's attack. Eve means an eavesdropper. Eve can change a secret function to another one whenever by entangled states, Bob and Alice can observe that Eve dropped in. Subsequently, we will refer to this situation simply as "Eve's attack". In classical case, Bob requires 2 queries. In quantum case, Bob requires just a query. This is faster than classical cryptography, which would require at least 2 queries.

Alice can select one of the 4 functions because of the combinations of the mappings. Later we introduce a parameter $i = 0, 1, 2, 3$ for the functions.

Let us discuss our quantum cryptography. We introduce the transformation O_f defined by the map:

$$O_f|x\rangle|j\rangle = |x\rangle|(f(x)+j) \bmod 2\rangle. \tag{3}$$

From the map O_f, we insert an imaginary number i and we can define the following formulas:

$$O_f|0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} = +|0\rangle(|f(0)\rangle - i|f(0)+1\rangle)/\sqrt{2}$$
$$= \begin{cases} |0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} & \text{if } f(0)=0, \\ -i|0\rangle(|0\rangle + i|1\rangle)/\sqrt{2} & \text{if } f(0)=1. \end{cases} \tag{4}$$

$$O_f|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} = +|1\rangle(|f(1)\rangle - |f(1)+1\rangle)/\sqrt{2}$$
$$= \begin{cases} |1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if } f(1)=0, \\ -|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if } f(1)=1. \end{cases} \tag{5}$$

Notice

$$(O_f)^2|x\rangle|j\rangle = |x\rangle|(2f(x)+j) \bmod 2\rangle = |x\rangle|j\rangle. \tag{6}$$

Therefore, the map O_f is a cyclic transformation. Here, we defined the normalized input state $(\langle\psi_0|\psi_0\rangle = 1)$ as follows:

$$|\psi_0\rangle = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right],$$
$$|\alpha|^2 + |\beta|^2 = 1, \alpha \neq 0, \beta \neq 0. \tag{7}$$

Let us introduce a parameter i. Later, we see all the information for f_i is imbedded into a single output entangled state. This means Bob gets all the information for f_i when he knows the single output entangled state. This is the key of our quantum cryptography.

Alice applies $O_{f_i}, (i = 0, 1, 2, 3)$ to $|\psi_0\rangle$, $O_{f_i}|\psi_0\rangle : |\psi_1\rangle_i$ the output entangled state is one of 4 cases:

$$|\psi_1\rangle_0 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$
$$\text{then } f_0(0)=0, f_0(1)=0, \tag{8}$$

$$|\psi_1\rangle_1 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] - \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$
$$\text{then } f_1(0)=0, f_1(1)=1, \tag{9}$$

$$|\psi_1\rangle_2 = -i\alpha|0\rangle\left[\frac{|0\rangle + i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$
$$\text{then } f_2(0)=1, f_2(1)=0, \tag{10}$$

$$|\psi_1\rangle_3 = -i\alpha|0\rangle\left[\frac{|0\rangle + i|1\rangle}{\sqrt{2}}\right] - \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$
$$\text{then } f_3(0)=1, f_3(1)=1, \tag{11}$$

where these equations have a property that the relation between each equation and the condition after "then" is regarded as a "if and only if" condition since we herein process all of the operations only under the cyclic transformation. So, the conditions after "then" are regarded as the results.

So, by measuring an entangled state $|\psi_1\rangle_i$, is sent by Alice, Bob may determine all the 2 mappings of $f_i(x)$ for all x(= 0, 1), simultaneously. This is very interesting indeed: our quantum cryptography gives us the ability to transmit a perfect property of $f_i(x)$, namely, $f_i(x)$ itself without Eve's attack. This is faster than classical cryptography, which would require at least 2 queries.

Our cryptography is as follows:

- Alice randomly selects a function f_1.
- She applies O_{fi} to $|\psi_0\rangle$ in giving an entangled state $|\psi_1\rangle_i$;
- She sends the entangled state $|\psi_1\rangle_i$;
- Bob compares (by measurement) the result state $|\psi_1\rangle_i$ with the input state and obtain all the two mappings concerning the function $\mathbf{f_i}$.
- Bob realizes what function Alice selects.
- Alice and Bob compare their functions (subset of the results).
- If Eve's attack exists, Alice and Bob select the different function.
- If Eve's attack does not exist, Alice and Bob select the same function.

Alice and Bob perform the protocol described above as many times to obtain enough secret keys (functions).

Concrete example

We present a concrete example to understand our quantum

cryptography fully and naturally. Let us consider the case where Alice randomly selects a function *f1*. Bob wants to know all the following mappings

$$f(0) = ?, f(1) = ?, \quad (12)$$

without Eve's attack. In classical case, Bob requires 2 evaluations. In quantum case, Bob requires just a query.
Alice prepares the following input entangled state:

$$|\psi_0\rangle = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \quad (13)$$

Next, Alice applies *Of*1 to $|\psi_0\rangle$, $O_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$. She has the following output entangled state:

$$|\psi_1\rangle_1 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] - \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \quad (14)$$

Bob asks what quantum output entangled state Alice has. Then Bob obtains all the mappings of f1(x), simultaneously:

$$f_1(0) = 0, f_1(1) = 1. \quad (15)$$

Bob realizes that Alice selects $f_1(x)$. Alice and Bob compare their functions (subset of the results). If Eve's attack exists, Alice and Bob select the different function. If Eve's attack does not exist, Alice and Bob select the same function. Alice and Bob perform the protocol described above as many times to obtain enough secret keys (functions).
Also, this is faster than classical cryptography, which would require at least 2 evaluations. Likewise, Alice can select the 4 combinations of the mappings. That is, our argumentations are true for each parameter i.

QUANTUM CRYPTOGRAPHY DERIVED FROM AN ALGORITHM OF DETERMINING A FUNCTION USING QUTRIT SYSTEMS

Quantum superposition is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate the mappings of a function $f(x)$ for many different (x) simultaneously. Suppose:

$$f : \{0,1,2\} \to \{0,1\} \quad (16)$$

is a function. Alice knows it. Bob's aim is to determine all the mappings

$$f(0) = ?, f(1) = ?, f(2) = ?, \quad (17)$$

that is, f(x) itself without Eve's attack. In classical case, Bob requires 3 queries. In quantum case, Bob requires just a query. This is faster than classical cryptography, which would require at least 3 queries.
Alice can select one of the 8 functions because of the combinations of the mappings. Later we introduce a parameter i = 0, 1, 2,..., 7 for the functions.
Let us discuss our quantum cryptography using qutrit systems. We newly introduce the transformation Of defined by the map:

$$O_f|x\rangle|j\rangle = |x\rangle|(f(x) + j) \bmod 3\rangle. \quad (18)$$

From the map O_f, we insert an imaginary number i and we can define the following formulas:

$$O_f|0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} = +|0\rangle(|f(0)\rangle - i|f(0)+1\rangle)/\sqrt{2}$$
$$= \begin{cases} |0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} & \text{if } f(0) = 0, \\ |0\rangle(|1\rangle - i|2\rangle)/\sqrt{2} & \text{if } f(0) = 1. \end{cases} \quad (19)$$

$$O_f|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} = +|1\rangle(|f(1)\rangle - |f(1)+1\rangle)/\sqrt{2}$$
$$= \begin{cases} |1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if } f(1) = 0, \\ |1\rangle(|1\rangle - |2\rangle)/\sqrt{2} & \text{if } f(1) = 1. \end{cases} \quad (20)$$

We define a quantum state in a three-dimensional space $|\phi\rangle$ as follows:

$$|\phi\rangle = \frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle), \quad (21)$$

where $\omega = e^{2\pi i/3}$. We have the following formula by the phase kick-back formation:

$$O_f|2\rangle|\phi\rangle = \omega^{f(2)}|2\rangle|\phi\rangle. \quad (22)$$

In fact, from the map O_f, we can define the following formulas:

$$O_f|2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle)$$
$$= |2\rangle\frac{1}{\sqrt{3}}(\omega^3|f(2)\rangle + \omega^2|f(2)+1\rangle + \omega|f(2)+2\rangle)$$
$$= \begin{cases} |2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle) & \text{if } f(2) = 0, \\ \omega|2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle) & \text{if } f(2) = 1. \end{cases} \quad (23)$$

Notice

$$(O_f)^3|x\rangle|j\rangle = |x\rangle|(3f(x)+j) \bmod 3\rangle = |x\rangle|j\rangle. \quad (24)$$

Therefore, the map O_f is a cyclic transformation. Here, we define the normalized input state $(\langle\psi_0|\psi_0\rangle = 1)$ as follows:

$$|\psi_0\rangle = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle,$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1, \alpha \neq 0, \beta \neq 0, \gamma \neq 0. \quad (25)$$

Let us introduce a parameter i. Later, we see all the information for $\mathbf{f_i}$ is imbedded into a single output entangled state. This means Bob gets all the information for $\mathbf{f_i}$ when he knows the single output entangled state. This is the key of our quantum cryptography.

Alice applies O_{fi} , $(i = 0, 1, ..., 7)$ to $|\psi_0\rangle$, $O_{f_i}|\psi_0\rangle = |\psi_1\rangle_i$,

$$|\psi_1\rangle_0 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_0(0) = 0, f_0(1) = 0, f_0(2) = 0, \quad (26)$$

$$|\psi_1\rangle_1 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_1(0) = 0, f_1(1) = 0, f_1(2) = 1, \quad (27)$$

$$|\psi_1\rangle_2 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_2(0) = 0, f_2(1) = 1, f_2(2) = 0, \quad (28)$$

$$|\psi_1\rangle_3 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_3(0) = 0, f_3(1) = 1, f_3(2) = 1, \quad (29)$$

$$|\psi_1\rangle_4 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_4(0) = 1, f_4(1) = 0, f_4(2) = 0, \quad (30)$$

$$|\psi_1\rangle_5 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_5(0) = 1, f_5(1) = 0, f_5(2) = 1, \quad (31)$$

$$|\psi_1\rangle_6 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_6(0) = 1, f_6(1) = 1, f_6(2) = 0, \quad (32)$$

$$|\psi_1\rangle_7 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{then} \quad f_7(0) = 1, f_7(1) = 1, f_7(2) = 1, \quad (33)$$

where these equations have a property that the relation between each equation and the condition after "then" is regarded as a "if and only if" condition since we herein process all of the operations only under the cyclic transformation. So, the conditions after "then" are regarded as the results.

So, by measuring an entangled state $|\psi_1\rangle_i$, which is sent by Alice, Bob may determine all the 3 mappings of $f_i(x)$ for all x(= 0, 1, 2), simultaneously. This is very interesting indeed: our quantum cryptography gives us the ability to transmit a perfect property of $f_i(x)$, namely, $f_i(x)$ itself without Eve's attack. This is faster than classical cryptography, which would require at least 3 queries.

Our cryptography is as follows:

- Alice randomly selects a function f_i.
- She applies O_f to $|\psi_0\rangle$ in giving an entangled state $|\psi_1\rangle_i$.
- She sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the result state $|\psi_1\rangle_i$ with the input state and obtains all the three mappings concerning the function fi.
- Bob realizes what function Alice selects.
- Alice and Bob compare their functions (subset of the results).
- If Eve's attack exists, Alice and Bob select the different function.
- If Eve's attack does not exist, Alice and Bob select the same function.

Alice and Bob perform the protocol described above many times of obtaining enough secret keys (functions).

Concrete example

We present a concrete example to understand our quantum cryptography fully and naturally. Let us consider the case where Alice randomly selects a function f_1.

Bob wants to know all the following mappings

$$f(0) = ?, f(1) = ?, f(2) = ?, \quad (34)$$

without Eve's attack. In classical case, Bob requires 3 evaluations. In quantum case, Bob requires just a query. Alice prepares the following input entangled state:

$$|\psi_0\rangle = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle. \quad (35)$$

Next, Alice applies Of_i to $|\psi_0\rangle$, $O_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$. She has the following output entangled state:

$$|\psi_1\rangle_1 = \alpha|0\rangle\left|\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right| + \beta|1\rangle\left|\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right| + \omega\gamma|2\rangle|\phi\rangle. \quad (36)$$

Bob asks what quantum output entangled state Alice has. Then Bob obtains all the mappings of $f_i(x)$., simultaneously:

$$f_1(0) = 0, f_1(1) = 0, f_1(2) = 1. \quad (37)$$

Bob realizes that Alice selects $f_i(x)$. Alice and Bob compare their functions (subset of the results). If Eve's at- tack exists, Alice and Bob select the different function. If Eve's attack does not exist, Alice and Bob select the same function. Alice and Bob perform the protocol described above as many times to obtain enough secret keys (functions).

Again, this is faster than classical cryptography, which would require at least 3 evaluations. Similarly, Alice can select the 8 combinations of the mappings. That is, our argumentations are true for each a parameter i.

QUANTUM CRYPTOGRAPHY DERIVED FROM AN ALGORITHM OF DETERMINING A FUNCTION USING QUDIT SYSTEMS

Quantum superposition is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate the mappings of a function $f(x)$ for many different x simultaneously. Suppose

$$f : \{0, 1, 2, ..., d-1\} \to \{0, 1\} \quad (38)$$

is a function. Alice knows it. Bob's aim is to determine all the mappings

$$f(0) = ?, f(1) = ?, f(2) = ?, ..., f(d-1) = ?, \quad (39)$$

that is, $f(x)$ itself without Eve's attack. In classical case, Bob requires d queries. In quantum case, Bob requires just a query. This is faster than classical cryptography, which would require at least d queries.

Alice can select one of the 2^d functions because of the combinations of the mappings. Later we introduce a parameter $i = 0, 1, 2, ..., 2^d - 1$ for the functions.

Let us discuss our quantum cryptography using qudit systems. We introduce the transformation O_f defined by the map

$$O_f|x\rangle|j\rangle = |x\rangle|(f(x) + j) \bmod d\rangle. \quad (40)$$

We define a quantum state in a d-dimensional space $|\phi_d\rangle$ as follows:

$$|\phi_d\rangle = \frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + ... + \omega|d-1\rangle), \quad (41)$$

where $\omega = e^{2\pi i/d}$. We have the following formula by the phase kick-back formation:

$$O_f|x\rangle|\phi_d\rangle = \omega^{f(x)}|x\rangle|\phi_d\rangle. \quad (42)$$

Notice

$$(O_f)^d|x\rangle|j\rangle = |x\rangle|(df(x) + j) \bmod d\rangle = |x\rangle|j\rangle. \quad (43)$$

Therefore, the map O_f is a cyclic transformation. Here, we define the normalized input state $(\langle\psi_0|\psi_0\rangle = 1)$ as follows:

$$|\psi_0\rangle = \sum_{n=1}^{d} \alpha_n|n-1\rangle|\phi_n\rangle,$$

$$\sum_{n=1}^{d} |\alpha_n|^2 = 1, \alpha_1 \neq 0, \alpha_2 \neq 0, ..., \alpha_d \neq 0. \quad (44)$$

Let us introduce a parameter i. Later, we see all the information for $\mathbf{f_i}$ is imbedded into a single output entangled state. This means Bob gets all the information for $\mathbf{f_i}$ when he knows the single output entangled state. This is the key of our quantum cryptography.

Alice applies $O_{f_i}, (i = 0, 1, ..., 2^d - 1)$ to $|\psi_0\rangle$, $O_{f_i}|\psi_0\rangle = |\psi_1\rangle_i$; the output entangled state is one of 2^d cases:

$$|\psi_1\rangle_i = \sum_{n=1}^{d} \omega^{f_i(n-1)}\alpha_n|n-1\rangle|\phi_n\rangle$$
$$\text{then } f_i(n-1) = 0 \text{ or } 1, \quad (45)$$

where this equation has a property that the relation between the equation and the condition after "then" is regarded as a "if and only if" condition since we herein process all of the operations only under the cyclic transformation. So, the conditions after "then" are regarded as the results.

So, by measuring an entangled state $|\psi_1\rangle_i$ which is sent by Alice, Bob may determine all the d mappings of $f_i(x)$ for all x(= 0, 1, 2, ..., d − 1), simultaneously. This is very interesting indeed: our quantum cryptography gives us the ability to transmit a perfect property of $f_i(x)$, namely, $f_i(x)$ itself without Eve's attack. This is faster than classical cryptography, which would require at least d queries.
Our cryptography is as follows:

- Alice randomly selects a function f_1.
- She applies Of_1 to $|\psi_0\rangle$ in giving an entangled state $|\psi_1\rangle_i$.
- She sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the result state $|\psi_1\rangle_i$ with the input state and obtain all the d mappings concerning the function f_i.
- Bob realizes what function Alice selects.
- Alice and Bob compare their functions (subset of the results).
- If Eve's attack exists, Alice and Bob select the different function.
- If Eve's attack does not exist, Alice and Bob select the same function.

Alice and Bob perform the protocol described above many times of obtaining enough secret keys (functions).

Concrete example

We present a concrete example to understand our quantum cryptography fully and naturally. Let us consider the case where Alice randomly selects a function f_1.
Bob wants to know all the following mappings

$$f(0) = ?, f(1) = ?, f(2) = ?, ..., f(d-1) = ?, \quad (46)$$

without Eve's attack. In classical case, Bob requires devaluations. In quantum case, Bob requires just a query.
Alice prepares the following input entangled state:

$$|\psi_0\rangle = \sum_{n=1}^{d} \alpha_n |n-1\rangle |\phi_n\rangle \quad (47)$$

Next, Alice applies O_{f_1} to $|\psi_0\rangle$, $O_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$ She has the following output entangled state:

$$|\psi_1\rangle_1 = \sum_{n=1}^{d} \omega^{f_1(n-1)} \alpha_n |n-1\rangle |\phi_n\rangle$$

$$\text{then } f_1(d-1) = 1, f_1(n) = 0, n = 0, 1, 2, ..., d-2. \quad (48)$$

Bob asks what quantum output entangled state Alice has. Then Bob obtains all the mappings of $f_1(x)$, simultaneously:

$$f_1(0) = 0, f_1(1) = 0, f_1(2) = 0, ..., f_1(d-1) = 1 \quad (49)$$

Bob realizes that Alice selects $f_1(x)$. Alice and Bob compare their functions (subset of the results). If Eve's attack exists, Alice and Bob select the different function. If Eve's attack does not exist, Alice and Bob select the same function. Alice and Bob perform the protocol described above as many times to obtain enough secret keys (functions).
Again, this is faster than classical cryptography, which would require at least d evaluations. Similarly, Alice can select the 2^d combinations of the mappings. That is, our argumentations are true for each a fixed parameter i.

CONCLUSIONS

In conclusion, we have proposed quantum cryptography based on an algorithm of determining a function. The security of our cryptography has been based on Ekert 91 protocol, that is, we use an entangled state. Eve must have destroyed the entangled state. Consider a function. Alice has known all the mappings concerning the function. Bob has known none of them. His aim has been of obtaining all of them without Eve's attack. In classical case, Bob needs some queries. In quantum case, Bob needs just a query. By measuring the single entangled state, which is sent by Alice, Bob can obtain all the mappings concerning the function, simultaneously. This has been faster than classical cryptography.

ACKNOWLEDGMENTS

We thank Professor Shahrokh Heidari and Professor Germano Resconi for their valuable comments.

REFERENCES

Bernstein E, Vazirani U (1993). Proceedings of 25th Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11. https://doi.org/10.1145/167088.167097.
Bernstein E, Vazirani U (1997). SIAM J. Comput. 26: 1411.
Cleve R, Ekert A, Macchiavello C, Mosca M (1998). Proc. R. Soc. Lond. A 454: 339.
Deutsch D (1985). Proc. R. Soc. Lond. A 400, 97.
Deutsch D, Jozsa R (1992). Proc. R. Soc. Lond. A 439, 553.
Ekert AK (1991). Phys. Rev. Lett. 67: 661.
Grover LK (1996). Proceedings of 28th Annual ACM Sympo- sium on Theory of Computing, pp. 212.

Shor PW (1994). Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, pp. 124.
Simon DR (1994). Proceedings of 35th IEEE Annual Sympo- sium on Foundations of Computer Science, pp. 116.