Quantum Cryptography Based on An Algorithm of Determining All The Mappings of A Function

Koji Nagata*, Do Ngoc Diep#, Tadao Nakamura@

*Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea

#TIMAS, Thang Long University,Nghiem Xuan Yem road, Hoang Mai district, Hanoi, Vietnam, Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, CauGiay district, Hanoi, Vietnam

@Department of Information and Computer Science, Keio University,3-14-1 Hiyoshi,Kohoku-ku,Yokohama 223-8522,Japan

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 anentangled 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 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 thesingle entangled state, which is sent by Alice, Bob can obtainall the mappings concerning the function, simultaneously.This is faster than classical cryptography.

Keywords: *Quantum cryptography and communication security,Quantum communication, Quantum algorithms, Quantum computation, Formalism*

I. Introduction

Among a number of algorithmic developments, we can mention the following.The Bernstein-Vazirani algorithm [1,2], which was published in 1993, can be considered an extension of the Deutsch-Jozsa algorithm [3,4,5]. In 1994, algorithms were proposed by Simon [6] and by Shor [7]. In 1996, Grover [8]presented strong arguments for exploring thecomputational 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 [9], that is, we use anentangled state.Eve must destroy the entangled state.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. For short, later 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 thesingle entangled state, which is sent by Alice, Bob can obtainall the mappings concerning the function, simultaneously.This is faster than classical cryptography.

II. 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) many different x simultaneously.Suppose

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

is a function.Alice knows it.Bob's aim is of determining all the mappings

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

that is, f(x) itself without 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

$O_f|x>|j>=|x>|(f(x)+j) mod\ 2>.$ (3)

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

$$O_f|0>\frac{|0>-i|1>}{\sqrt{2}}=|0>\frac{|f(0)>-i|f(0)+1>}{\sqrt{2}}=$$

$$\begin{cases}|0>\frac{|0>-i|1>}{\sqrt{2}} & if\ f(0)=0,\\ -i|0>\frac{|0>+i|1>}{\sqrt{2}} & if\ f(0)=1.\end{cases} \quad (4)$$

$$O_f|1>\frac{|0>-|1>}{\sqrt{2}}=|1>\frac{|f(1)>-|f(1)+1>}{\sqrt{2}}=$$

$$\begin{cases}|1>\frac{|0>-|1>}{\sqrt{2}} & if\ f(1)=0,\\ -|1>\frac{|0>-|1>}{\sqrt{2}} & if\ f(1)=1.\end{cases} \quad (5)$$

Notice

$(O_f)^2|x>|j>=|x>|(2f(x)+j) mod\ 2>=|x>|j>.$ (6)

Therefore, the map O_f is a cyclic transformation. Here, we define the normalized input state ($<\Psi_0|\Psi_0>=1$) as follows:

$$|\Psi_0>=\alpha|0>\frac{|0>-i|1>}{\sqrt{2}}+\beta|1>\frac{|0>-|1>}{\sqrt{2}},$$

$|\alpha|^2+|\beta|^2=1, \alpha\neq 0, \beta\neq 0.$ (7)

Let us introduce a parameter i. Later, we seeall 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 $|\Psi_0>$, $O_{f_i}|\Psi_0>=|\Psi_1>_i$,the output entangled state is one of the 4 cases:

$|\Psi_1>_0=\alpha|0>\frac{|0>-i|1>}{\sqrt{2}}+\beta|1>\frac{|0>-|1>}{\sqrt{2}}$ then $f_0(0)=0, f_0(1)=0,$ (8)

$|\Psi_1>_1=\alpha|0>\frac{|0>-i|1>}{\sqrt{2}}-\beta|1>\frac{|0>-|1>}{\sqrt{2}}$ then $f_1(0)=0, f_1(1)=1,$ (9)

$|\Psi_1>_2=-i\alpha|0>\frac{|0>+i|1>}{\sqrt{2}}+\beta|1>\frac{|0>-|1>}{\sqrt{2}}$ then $f_2(0)=1, f_2(1)=0,$ (10)

$|\Psi_1>_3=-i\alpha|0>\frac{|0>+i|1>}{\sqrt{2}}-\beta|1>\frac{|0>-|1>}{\sqrt{2}}$ then $f_3(0)=1, f_3(1)=1,$ (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 operationsonly under the cyclic transformation. So, the conditions after "then" are regarded as the results.

So, by measuring an entangled state $|\Psi_1>_i$, which 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 cryptographygives us the ability to transmit a perfect property of $f_i(x)$, namely, $f_i(x)$ itselfwithout 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_i.
- She applies O_{f_i} to $|\Psi_0>$ in giving an entangled state $|\Psi_1>_i$.
- She sends the entangled state $|\Psi_1>_i$ to Bob.
- Bob compares (by measurement) the result state $|\Psi_1>_i$ with the input state and obtain all the two 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 obtainingenough secret keys (functions).

A. 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

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

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:

$$|\Psi_0>=\alpha|0>\frac{|0>-i|1>}{\sqrt{2}}+\beta|1>\frac{|0>-|1>}{\sqrt{2}}. \qquad (13)$$

Next, Alice applies O_{f_1} to$|\Psi_0>$, $O_{f_1}|\Psi_0>=|\Psi_1>_1$. She has the following output entangled state:

$$|\Psi_1>_1=\alpha|0>\frac{|0>-i|1>}{\sqrt{2}}-\beta|1>\frac{|0>-|1>}{\sqrt{2}} \qquad (14)$$

Bob asks what quantum output entangled state Alice has.

Then Bob obtains all the mappings of $f_{1}(x)$, simultaneously:

$$f_1(0)=0, f_1(1)=1, \qquad (15)$$

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 many times of obtainingenough secret keys (functions).

Again, 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 a 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 thesingle entangled state, which is sent by Alice, Bob can have obtainedall the mappings concerning the function, simultaneously.This has been faster than classical cryptography.

Acknowledgments

We thank Professor ShahrokhHeidari andProfessor GermanoResconifor valuable comments.

Note

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] E. Bernstein and U. Vazirani,Proceedings of 25th Annual ACM Symposium on Theory of Computing (STOC '93), p. 11 (1993), https://doi.org/10.1145/167088.167097.

[2] E. Bernstein and U. Vazirani,SIAM J. Comput.**26**, 1411 (1997).

[3] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97(1985).

[4] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A **439**, 553(1992).

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A **454**, 339(1998).

[6] D. R. Simon, Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p.116 (1994).

[7] P. W. Shor,Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p. 124(1994).

[8] L. K. Grover,Proceedings of 28th Annual ACM Symposium on Theory of Computing,p. 212(1996).

[9] K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).