International Journal of Theoretical Physics
https://doi.org/10.1007/s10773-020-04571-5

Continuous-Variable Quantum Computing and its Applications to Cryptography

Do Ngoc Diep[1,2] · **Koji Nagata**[3] · **Renata Wong**[4]

Received: 11 June 2020 / Accepted: 8 August 2020 / Published online: 22 August 2020

Abstract
We propose a quantum cryptography based on an algorithm for determining a function using continuous-variable entangled states. The security of our cryptography is based on the Ekert 1991 protocol, which uses an entangled state. Eavesdropping destroys the entangled state. Alice selects a secret function from the very large number of possible function types. Bob's aim is to determine the selected function (a key) without an eavesdropper learning it. In order for both Alice and Bob to be able to select the same function classically, in the worst case Bob requires a very large number of queries to Alice. In the quantum case however, Bob requires just a single query. By measuring the single entangled state, which is sent to him by Alice, Bob can obtain the function that Alice has selected. This quantum key distribution method is faster than the very large number of classical queries that would be required in the classical case.

Keywords Quantum cryptography and communication security · Quantum communication · Quantum algorithms · Quantum computation · Formalism

1 Introduction

Continuous-variable quantum information is the area of quantum information science that makes use of physical observables, such as the strength of an electromagnetic field, whose numerical values belong to continuous intervals. In 1998, Braunstein studied error correction for continuous quantum variables [1] and quantum error correction for communication with linear optics [2]. In 1999, Lloyd and Braunstein proposed quantum computation

✉ Koji Nagata
ko_mi_na@yahoo.co.jp

[1] TIMAS, Thang Long University, Nghiem Xuan Yem Road, Hoang Mai District, Hanoi, Vietnam

[2] Institute of Mathematics, VAST, 18 Hoang Quoc Viet Road, Cau Giay District, Hanoi, Vietnam

[3] Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon, 34141, Korea

[4] Department of Computer Science and Technology, Nanjing University, 163 Xianlin Road, 210093, Nanjing, Jiangsu, China

over continuous variables [3]. The same year, Ralph considered continuous-variable quantum cryptography [4]. In 2000, Hillery discussed quantum cryptography with squeezed states [5], while Reid described quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations [6]. In 2001, secure quantum key distribution using squeezed states was studied by Gottesman and Preskill [7]. A year later, continuous-variable quantum cryptography using coherent states was first proposed by Grosshans and Grangier [8]. Efficient classical simulation of continuous-variable quantum information processes has been studied by Bartlett et al. [9].

More recently, there has been developement with regards to applying quantum algorithms to quantum cryptography. In 2015, Nagata and Nakamura [10] discussed the use of the Deutsch–Jozsa algorithm for quantum key distribution, and in 2017, the authors described a method of secure quantum key distribution based on Deutsch's algorithm using an entangled state [11]. Subsequently, Nagata et al. [12] proposed an approach to high-speed secure quantum cryptography based on the Deutsch–Jozsa algorithm. A generalization of it to a d-level quantum system was explored by Nguyen and Kim [13, 14]. The relation between quantum computers and secret key sharing based on the use of quantum principles was discussed by Diep and Giang [15]. Quantum cryptography by means of quantum computer algorithms was proposed by Nagata et al. [16] in 2020.

In this short contribution, we propose a quantum cryptography based on an algorithm for determining a function using continuous-variable entangled states. As the security of our cryptography is based on Ekert's 1991 protocol [17], we use an entangled state. An eavesdropper will destroy the entangled state. Consider the very large number of possible functions. Alice selects a secret function. Bob's aim is to determine the selected function (a key) without the eavesdropper learning it. Classically, in order to select the same function, Bob would require a very large number of queries to Alice in the worst-case scenario. In the quantum case, Bob requires just a single query. By measuring the single entangled state, which is sent to him by Alice, Bob can obtain the selected function. This protocol's performance is faster than the very large number of queries required in the case of classical cryptography.

2 Quantum Cryptography Based on an Algorithm for Determining a Function Using Continuous-variable Entangled States

Suppose $f : [0, d] \to [0, e]$, $(1 \leq e \leq d)$, $e, d \in \mathbf{N}$ is a function. We specify the condition $(e \leq d)$ in order to make the function $\omega^{f(x)}$ univalent, where $\omega = e^{2\pi i/d}$. There is a very large number of functions of this form. Alice selects a function $f(x)$ secretly. Bob's aim is then to determine the secret function $f(x)$ without Eve's interference. Classically, in the worst case, Bob requires to query Alice a very large number of times in order to be able to select the same function as Alice has. Example queries would be, e.g., "What is the value of $f(0.2)$?", "What is the value of $f(1)$?", and so on. In the quantum case however, Bob needs just a single query, which is faster than the classical scenario of having to query Alice a very large number of times.

Alice can select one of the very large number of functions. Later we will introduce a continuous parameter $i \in [0, e^d]$ for the functions f_i.

Let us discuss our quantum cryptography using continuous-variable entangled states. To that end, we introduce the transformation U_f defined by the mapping $U_f|x\rangle|j\rangle = |x\rangle|(f(x) + j) \bmod d\rangle$. We define a quantum state $|\phi_d\rangle$ in an infinite-dimensional space as

follows: $|\phi_d\rangle = \int_{j\in[0,+d)} dj \frac{\omega^{d-j}|j\rangle}{\sqrt{d}}$, where $\omega = e^{2\pi i/d}$. By the phase kick-back formation [18] (See Appendix) we have the following formula: $U_f|x\rangle|\phi_d\rangle = \omega^{f(x)}|x\rangle|\phi_d\rangle$. Notice that $(U_f)^d|x\rangle|j\rangle = |x\rangle|(df(x)+j) \bmod d\rangle = |x\rangle|j\rangle$. Therefore, the mapping U_f is a cyclic transformation. Here, we define the normalized input state ($\langle\psi_0|\psi_0\rangle = 1$) as follows: $|\psi_0\rangle = \int_0^d dn\alpha(n)|n\rangle|\phi_n\rangle$, $\int_0^d dn|\alpha(n)|^2 = 1, \alpha(n) \neq 0$.

Now, let us introduce the continuous parameter i. Later, we will see that all the information for f_i is embedded in a single output entangled state. Therefore, knowing the single output entangled state, Bob will be able to obtain all the information for f_i. This is the key of our quantum cryptography.

By applying U_{f_i}, ($i \in [0, e^d]$), to $|\psi_0\rangle$ Alice obtains the following output entangled state: $U_{f_i}|\psi_0\rangle = |\psi_1\rangle_i = \int_0^d dn\omega^{f_i(n)}\alpha(n)|n\rangle|\phi_n\rangle$ iff $f_i(n) \in [0, e], \forall n \in [0, d]$.

So, by measuring the entangled state $|\psi_1\rangle_i$, which he received from Alice, Bob will be able to determine the secret function that Alice selected. Interestingly, our quantum cryptography gives us the ability to transmit a perfect property of $f_i(x)$, namely, the $f_i(x)$ itself, without Eve's interference. This is faster than endlessly querying Alice, which would have been the case classically.

Our cryptography is as follows:

- Alice selects a function $f_i, i \in [0, e^d]$, at random.
- Alice applies U_{f_i} to $|\psi_0\rangle$, which results in an entangled state $|\psi_1\rangle_i$.
- Alice sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the state $|\psi_1\rangle_i$ with the input state and obtains all the maps for the values of the function f_i.
- Bob determines what function Alice has selected.
- Alice and Bob compare their respective functions (subset of the results).
- If Eve has interfered, Alice and Bob determine that they each have a different function.
- If Eve hasn't interfered, Alice and Bob determine that they share the same function.

Alice and Bob carry out the protocol described above many times to share enough secret keys (functions). Again, this protocol is faster than the very large querying executed in the corresponding classical cryptography.

In what follows, we consider a concrete example.

2.1 Concrete Example

We present a concrete example to facilitate a full and natural understanding of our quantum cryptography. Let us consider the case where Alice randomly selects a secret function $f_0(x) = x$ and we assume that $d = e$. Bob wants to learn the secret function without Eve's interference. Classically, in the worst case, Bob would need to query Alice a very large number of times. In the quantum case however, Bob requires just a single query.

Alice prepares the following input entangled state: $|\psi_0\rangle = \int_0^d dn\alpha(n)|n\rangle|\phi_n\rangle$. Then, she applies U_{f_0} to $|\psi_0\rangle$ and obtains the following output entangled state: $U_{f_0}|\psi_0\rangle = |\psi_1\rangle_0 = \int_0^d dn\omega^{f_0(n)}\alpha(n)|n\rangle|\phi_n\rangle$ iff $f_0(n) = n \in [0, d]$. Upon Bob's inquiry as to what quantum output state she has obtained, Alice sends the entangled state $|\psi_1\rangle_0$ to Bob over a quantum channel. Then Bob obtains simultaneously all the maps with the values $f_0(x) = x, \forall x \in [0, d]$. Based on that, Bob determines that Alice has selected $f_0(x) = x$.

Alice and Bob execute the protocol described above a number of times to obtain enough secret keys (functions) changing the secret function. After that, Alice and Bob compare

their functions (subset of the results). If Eve's interference is established, Alice and Bob will determine that they have different functions. If Eve hasn't interfered, Alice and Bob will determine that they share the same function.

Again, this protocol is faster than the corresponding classical cryptography, which would require, in the worst case, a very large number of queries. Likewise, Alice can select among the very large number of combinations of maps. Hence, our argument is true for every parameter i.

3 Conclusions

We have proposed a quantum cryptography based on an algorithm for determining a function using continuous-variable entangled states. The security of our cryptography is based on the Ekert protocol of 1991 [17], that is, we use an entangled state. The presence of an eavesdropper will destroy the entangled state. Alice selected a secret function from the very large number of different functions. Bob's aim was to determine the selected function (a key) without an eavesdropper learning it. In order for Alice and Bob to select the same function classically, Bob would have to request a very large amount of information about the function values from Alice in the worst case. In the quantum case however, Bob required just a single query. By measuring the single entangled state, which was sent to him by Alice, Bob was able to obtain the selected function. Our cryptography was faster than the corresponding classical cryptography, which requires a very large number of queries.

Acknowledgments We thank Professor Shahrokh Heidari, Professor Germano Resconi, Professor Santanu Kumar Patro, Professor Tadao Nakamura, Professor Jaewook Ahn, and Professor Han Geurdes for valuable comments.

Compliance with Ethical Standards

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

Appendix: The Phase Kick-Back Formation

We have the following formula by the phase kick-back formation [18]:

$$U_f|x\rangle|\phi_d\rangle = \omega^{f(x)}|x\rangle|\phi_d\rangle. \tag{1}$$

In what follows, we discuss the rationale behind the above relation (1). Consider the action of the U_f gate on the state $|x\rangle|\phi_d\rangle$. Each summand in $|\phi_d\rangle$ is of the form $\omega^{d-j}|j\rangle$. We observe that

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{d-j}|x\rangle|(j + f(x)) \bmod d\rangle. \tag{2}$$

A variable k is introduced such that $f(x) + j = k$, from which it follows that $d - j = d + f(x) - k$. Thus, (2) becomes

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{f(x)}\omega^{d-k}|x\rangle|k \bmod d\rangle. \tag{3}$$

If $k < d$ we have that $|k \bmod d\rangle = |k\rangle$ and thus the summands in $|\phi_d\rangle$ for which $k < d$ are transformed as follows:

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{f(x)}\omega^{d-k}|x\rangle|k\rangle. \tag{4}$$

On the other hand, as both $f(x)$ and j are bounded from above by d, k is strictly less than $2d$. Thus, when $d \leq k < 2d$, we have $|k \bmod d\rangle = |k - d\rangle$. Let $k - d = m$. We have

$$\begin{aligned} &\omega^{f(x)}\omega^{d-k}|x\rangle|k \bmod d\rangle = \omega^{f(x)}\omega^{-m}|x\rangle|m\rangle \\ &= \omega^{f(x)}\omega^{d-m}|x\rangle|m\rangle. \end{aligned} \tag{5}$$

Hence, the summands in $|\phi_d\rangle$ for which $k \geq d$ are transformed as follows:

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{f(x)}\omega^{d-m}|x\rangle|m\rangle. \tag{6}$$

Finally, regarding (4) and (6), we have

$$U_f|x\rangle|\phi_d\rangle = \omega^{f(x)}|x\rangle|\phi_d\rangle. \tag{7}$$

Therefore, the relation (1) holds.

References

1. Braunstein, S.L.: Phys. Rev. Lett. **80**, 4084 (1998)
2. Braunstein, S.L.: Nature (London) **394**, 47 (1998)
3. Lloyd, S., Braunstein, S.L.: Phys. Rev. Lett. **82**, 1784 (1999)
4. Ralph, T.C.: Phys. Rev. A **61**, 010303(R) (1999)
5. Hillery, M.: Phys. Rev. A **61**, 022309 (2000)
6. Reid, M.D.: Phys. Rev. A **62**, 062308 (2000)
7. Gottesman, D., Preskill, J.: Phys. Rev. A **63**, 022309 (2001)
8. Grosshans, F., Grangier, P.: Phys. Rev. Lett. **88**, 057902 (2002)
9. Bartlett, S.D., Sanders, B.C., Braunstein, S.L., Nemoto, K.: Phys. Rev. Lett. **88**, 097904 (2002)
10. Nagata, K., Nakamura, T.: Open Access Library J. **2**, e1798 (2015)
11. Nagata, K., Nakamura, T.: Int. J. Theor. Phys. **56**, 2086 (2017)
12. Nagata, K., Nakamura, T., Farouk, A.: Int. J. Theor. Phys. **56**, 2887 (2017)
13. Nguyen, D.M., Kim, S.: Int. J. Theor. Phys. **58**, 71 (2019)
14. Nguyen, D.M., Kim, S.: Int. J. Theor. Phys. **58**, 2043 (2019)
15. Diep, D.N., Giang, D.H.: Int. J. Theor. Phys. **56**, 2797 (2017)
16. Nagata, K., Diep, D.N., Nakamura, T.: Asian J. Math. Phys. **4**(1), 7 (2020)
17. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
18. Nagata, K., Geurdes, H., Patro, S.K., Heidari, S., Farouk, A., Nakamura, T.: Int. J. Theor. Phys. **58**, 3694 (2019)