**International Journal of Emerging Engineering Research and Technology**
**Volume 5, Issue 8, 2017, PP 28-31**
**ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)**

# Quantum Communication Based on Simon's Algorithm

**K. Nagata,[1] T. Nakamura,[2] H. Geurdes,[3] J. Batle,[4] S. Abdalla,[5] and A. Farouk[6]**

*[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]Geurdes Datascience, KvK 64522202, C vd Lijnstraat 164, 2593 NN, Den Haag Netherlands*
*[4]Departament de F´ısica, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Europe*
*[5]Department of Physics, Faculty of Science, King Abdulaziz University Jeddah, P.O. Box 80203, Jeddah 21589, Saudi Arabia*
*[6]Computer Sciences Department, Faculty of Computers and Information, Mansoura University, Egypt*

***Corresponding Author:** K. Nagata, Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*

***Received Date: 13-11-2017*** ***Accepted Date: 24-11-2017*** ***Published Date: 05-12-2017***

## ABSTRACT

*We study quantum communication based on Simon's algorithm. We discuss the fact that quantum communication overcomes classical communication by a factor of O(√2N/N) in Simons algorithm case.*

**PACS Numbers:** *03.67.Lx, 03.67.-a 03.67.Ac*

**Keywords:** *Quantum computation architectures and implementations, Quantum information, Quantum algorithms, protocols, and simulations*

## INTRODUCTION

Quantum communication is the art of transferring a quantum state from one place to another. Traditionally, the sender is named Alice and the receiver Bob. The basic motivation is that quantum states code quantum information - called qubits in the case of 2-dimensional Hilbert spaces and that quantum information allows one to perform tasks that could only be achieved far less efficiently, if at all, using classical information.

A quantum computer is a device for computation that makes direct use of quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from digital computers based on transistor gates. Whereas digital computers require data to be encoded into binary digits (bits), quantum computation utilizes quantum properties to represent data and perform operations on these data [1]. A theoretical model is the quantum Turing machine, also known as the universal quantum computer. Quantum computers share theoretical similarities with non-deterministic and probabilistic computers, like the ability to be in more than one state simultaneously. The field of quantum computing was first introduced by Richard Feynman in 1982 [2, 3].

The Deutsch-Jozsa algorithm is a quantum algorithm, proposed by David Deutsch and Richard Jozsa in 1992 [4] with improvements by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998 [5]. Although of little practical use, it is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm. It is also a deterministic algorithm, meaning that it always produces an answer, and that answer is always correct.

The Deutsch-Jozsa algorithm generalizes earlier (1985) work by David Deutsch, which provided a solution for the simple case. Specifically we are given a boolean function whose input is 1 bit, $f : \{0, 1\} \rightarrow \{0, 1\}$ and asked if it is constant [6].

The algorithm as Deutsch has originally proposed it is not, in fact, deterministic. The algorithm is successful with a probability of one half. 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 requires two function evaluations instead of only one.

Further improvements to the Deutsch-Jozsa algorithm are made by Cleve et al., [5] resulting in an algorithm that is both deterministic and requires only a single query of f. This algorithm is still referred to as Deutsch-Jozsa algorithm in honour of the groundbreaking techniques they employed [5].

The Deutsch-Jozsa algorithm provides inspiration for Shor's algorithm and Grover's algorithm, two of the most revolutionary quantum algorithms [7, 8].

Looking at studies of quantum computing, implementation of a quantum algorithm to solve Deutsch's problem [4—6] on a nuclear magnetic resonance quantum computer is reported firstly [9]. An implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [10]. There are several attempts to use single-photon two-qubit states for quantum computing. Oliveira et al. implements Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [11]. In addition, single-photon Bell states are prepared and measured [12]. Also the decoherence-free implementation of Deutsch's algorithm is reported by using such single-photon and by using two logical qubits [13]. A one-way based experimental implementation of Deutsch's algorithm is reported [14].

For a number of recent algorithmic developments we mention the following. In 1993, the Bernstein-Vazirani algorithm was reported [15, 16]. This can be considered as an extended Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was reported [17]. Implementation parity problem without entanglement on an ensemble quantum computer can be mentioned as an important quantum algorithm [18]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits was also discussed in the recent past [19]. The question if quantum learning is robust against noise is studied [20].

A quantum algorithm for approximating the influences of Boolean functions and its applications is recently studied [21]. In addition, Quantum computation with coherent spin states and the close Hadamard problem [22] and the transport implementation of the Bernstein-Vazirani algorithm with ion qubits are studied [23]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [24]. We mention that the dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [25]. A method of computing many functions simultaneously by using many parallel quantum systems is reported [26].

On the other hand, we may wonder if we need all the previously mentioned studies to reach our goal. The earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than its classical counterpart. Its magnitude grows exponentially with the number of qubits. In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [27]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [28]. Subsequently, a highly speedy secure quantum cryptography based on the Deutsch-Jozsa algorithm is proposed [29]. The relation between quantum computer and quantum secret sharing is discussed [30].

In this paper, we investigate the relation between quantum communication and Simon's algorithm.

## SIMON'S ALGORITHM

In this section, we review Simon's algorithm. Suppose

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

is a function with a N-bit domain and a N-bit range. We assume the following case

$$f(x) = f(x \oplus s), \forall x.$$

$$x \oplus s = (x_1 \oplus s_1, x_2 \oplus s_2, ..., x_N \oplus s_N). \quad (2)$$

Simon's algorithm combines quantum parallelism with a property of quantum mechanics known as interference.

Let us follow the quantum states through Simon's algorithm. The input state is

$$|\psi) = |0)^{\otimes N}|0). \quad (3)$$

After the Hadamard transformation on the first N-bit state we have

$$|\psi_1) = x\{0,1\}^N |x/\sqrt{}) \, 2^N |0) \quad (4)$$

Next, the function f is evaluated (by Bob) using

$$U_f : |x, y) \rightarrow |x, y \oplus f(x)), \quad (5)$$

giving

$$|\psi_2) = x \sqrt{|x)/2^N} \, |f(x)). \quad (6)$$

We have

$$|\psi_3) = x \, |x \oplus s)/\sqrt{2^N} \, |f(x)) \quad (7)$$

by using $f(x) = f(x \oplus s)$. Thus,

$$|\psi_4) = ½ \, (|\psi_2) + |\psi_3))$$

$$= \in x \, |x) + |x \oplus s)/\sqrt{2^{N+2}} \, |f(x)). \quad (8)$$

In what follows, we derive the result of the Hadamard transformation of $|x) + |x \oplus s)$. We have the very useful equation

$$H^{\otimes N}|x) = \in z(-1)^{x \cdot z} \, |z)/\sqrt{2^N}. \quad (9)$$

And we have

$$H^{\otimes N}|x \oplus s) = \in z(-1)^{z \cdot (x \oplus s)} \, |z)/\sqrt{2N}, \quad (10)$$

Thus,

$$H^{\otimes N}(|x) + |x \oplus s))$$

$$= \in z(-1)^{x \cdot z + z \cdot (x \oplus s)} |z)/\sqrt{2^N}$$

$$= \in z \, [(-1)^{x \cdot z}(1 + (-1)^{z \cdot s})]|z)/\sqrt{2N}, \quad (11)$$

Therefore, if Alice measures $|z)$ then

$$z \cdot s = 0. \quad (12)$$

And thus, if Alice measures $|z_1),|z_2),...,|z_N)$ she gets the s.

## Quantum Communication Based on Simon's Algorithm

We study quantum communication based on Simon's algorithm.

First, Alice and Bob have promised to use a function f such as $f(x) = f(x \oplus s)$ for all x. Alice does not know s. Bob knows s. Alice's goal is to determine with certainty what s Bob has chosen. Alice prepares suitable N +1 partite uncorrelated state, performs the Hadamard transformation to the state, and sends the output state to Bob. And Bob performs Simon's algorithm and inputs the information of the s into the final state. Alice asks him what state is it O(N) times. Alice measures the final state and she knows the s. If the s is learned by Alice, Alice and Bob share N bits of information, by O(N)-communication with each other. In the classical case, Alice needs at least $O(\sqrt{2^N})$-communication with Bob to get the s.

- First Alice prepares the qubits in (4) and sends the N + 1 qubits to Bob.
- Next, Bob picks N bits "s" and Bob applies $U_f$ Eq. (5) evolving the N + 1 qubits to Eq. (6). He then sends the N qubit to Alice.
- Finally, Alice applies the Hadamard transformation to each of the first N qubits and measures it O(N) times. She learns s. Alice and Bob now share N bits of information.
- In the classical case (without this quantum computing), Alice needs at least $O(\sqrt{2^N})$-communication with Bob to get the s.

We have shown quantum communication overcomes classical communication by a factor of $O(\sqrt{2}N/N)$ in Simon's algorithm case.

## Conclusions

In conclusion, we have discussed quantum communication based on mimon's algorithm. Alice and Bob have promised to use a function f such as $f(x) = f(x \oplus s)$ for all x. Alice does not have known s. Bob has known s. Alice's goal has been to determine with certainty what s Bob has chosen. If the s has been learned by Alice, Alice and Bob have shared N bits of information, by O(N)- communication with each other. In the classical case, Alice has needed at least $O(\sqrt{2}N)$-communication with Bob to get the s. This has shown quantum communication overcomes classical communication by a factor of $O(\sqrt{2^N}/N)$ in Simon's algorithm case.

## References


[1] "Quantum Computing with Molecules" article in Scientific American by Neil Gershenfeld and Isaac L. Chuang.

[2] Quantum computation. David Deutsch, Physics World, 1/6/92.

[3] Quantum computer - Wikipedia, the free encyclopedia

[4] D. Deutsch and R. Jozsa, Proc. Roy. Soc. London Ser. A 439, 553 (1992).

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

[6] D. Deutsch, Proc. Roy. Soc. London Ser. A 400, 97 (1985).

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

[8] L. K. Grover, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 212 (1996).

[9] J. A. Jones and M. Mosca, J. Chem. Phys. 109, 1648 (1998).

[10] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. H¨affner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) 421, 48 (2003).

[11] A. N. de Oliveira, S. P. Walborn, and C. H. Monken, J. Opt. B: Quantum Semiclass. Opt. 7, 288-292 (2005).

[12] Y.-H. Kim, Phys. Rev. A 67, 040301(R) (2003).

[13] M. Mohseni, J. S. Lundeen, K. J. Resch, and A. M. Steinberg, Phys. Rev. Lett. 91, 187903 (2003).

[14] M. S. Tame, R. Prevedel, M. Paternostro, P. B¨ohi, M. S. Kim, and A. Zeilinger, Phys. Rev. Lett. 98, 140501 (2007).

[15] 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.

[16] E. Bernstein and U. Vazirani, SIAM J. Comput. 26-5, pp. 1411-1473 (1997).

[17] D. R. Simon, Foundations of Computer Science, (1994) Proceedings, 35th Annual Symposium on: 116-123, retrieved 2011-06-06.

[18] J. Du, M. Shi, X. Zhou, Y. Fan, B. J. Ye, R. Han, and J. Wu, Phys. Rev. A 64, 042306 (2001).

[19] E. Brainis, L.-P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. 90, 157902 (2003).

[20] A. W. Cross, G. Smith, and J. A. Smolin, Phys. Rev. A 92, 012327 (2015).

[21] H. Li and L. Yang, Quantum Inf. Process. 14, 1787 (2015).

[22] M. R. A. Adcock, P. Hoyer, and B. C. Sanders, Quantum Inf. Process. 15, 1361 (2016).

[23] 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).

[24] [24] D. N. Diep, D. H. Giang, and N. Van Minh, Int J Theor Phys (2017) 56: 1948. https://doi.org/10.1007/s10773- 017-3340-8.

[25] W. Jin, Quantum Inf. Process. 15, 65 (2016).

[26] K. Nagata, G. Resconi, T. Nakamura, J. Batle, S. Abdalla, A. Farouk, and H. Geurdes, Asian J. Math. Phys. 1 (1) (2017), 1-4.

[27] K. Nagata and T. Nakamura, Open Access Library Journal, 2: e1798 (2015). http://dx.doi.org/10.4236/oalib.1101798.

[28] K. Nagata and T. Nakamura, Int J Theor Phys (2017) 56: 2086. https://doi.org/10.1007/s10773-017-3352-4

[29] K. Nagata, T. Nakamura, and A. Farouk, Int J Theor Phys (2017) 56: 2887. https://doi.org/10.1007/s10773- 017-3456-x

[30] D. N. Diep and D. H. Giang, Int J Theor Phys (2017) 56: 2797. https://doi.org/10.1007/s10773-017-3444-1

**Citation:** *K. Nagata, T. Nakamura, H. Geurdes, J. Batle, S. Abdalla and A. Farouk, "Quantum Communication Based on Simon's Algorithm", International Journal of Emerging Engineering Research and Technology, vol. 5, no. 8, pp. 28-31, 2017.*