A Quantum Trapdoor One-Way Function that Relies on the Hardness of the Graph Automorphism Problem

Akinori Kawachi[1 2 *] Takeshi Koshiba[1 3 †] Harumichi Nishimura[4 ‡]
Tomoyuki Yamakami[4 §]

[1] *ERATO Quantum Computation and Information Project, JST.*
Matsuo-BLDG 2F, 406 Iseya-cho, Kawaramachi-Marutamachi, Kamigyo-ku, Kyoto 602-0873, Japan.
[2] *Graduate School of Informatics, Kyoto University*
Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan.
[3] *Secure Computing Lab., Fujitsu Laboratories Ltd.*
4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki 211-8588, Japan.
[4] *School of Information Technology and Engineering, University of Ottawa*
800 King Edward Avenue Ottawa, Ontario Canada, K1N 6N5

Abstract. We propose a quantum trapdoor one-way function, which maps classical bits, 0 and 1, into two quantum states respectively, assuming the intractability of the graph automorphism problem. More precisely, our function satisfies the following properties: (1) we can easily compute the function by generating one of the two quantum states corresponding to an input bit; (2) if we know a trapdoor, we can easily invert the function; (3) if there exists an efficient quantum adversary which can invert the function without any trapdoor, we can efficiently solve the graph automorphism problem. Based on our function, we propose a provably secure quantum public-key cryptosystem.

Keywords: trapdoor one-way function, public-key cryptosystem, provable security

1 Introduction

A function is in general regarded as *one-way* if it is efficiently computable but cannot be inverted efficiently. Such a function is known to be one of the most important primitives in modern cryptography since many cryptographic schemes, such as, pseudorandom generators, bit commitment protocols, and digital signatures can be constructed from any one-way function. The security of these schemes relies on the one-wayness of the underlying functions. The famous RSA function as well as the discrete logarithmic function are believed to be one-way and have been used largely in practice. Nonetheless, a quantum mechanical computer, as Shor [7] demonstrated, has an ability to invert those functions easily. This leads us to seek a new type of one-way function, which is one-way even by the use of a quantum computer [1, 2, 6].

Furthermore, the *trapdoor property* of a function plays another important role in cryptography. This property requires that certain secret information, called a *trapdoor*, enables us to invert the function efficiently. Trapdoor one-way functions are used as a basis of public-key cryptosystems. The RSA function, for instance, serves as a candidate for a trapdoor one-way function (against classical computation).

Recently, Okamoto, Tanaka, and Uchiyama [6] proposed a quantum trapdoor one-way function, based on a certain subset of the subset-sum problem, and its corresponding quantum public-key cryptosystem. Their cryptosystem is considered to be secure against certain types of attacks by any quantum adversary. However, it is not yet known whether the one-wayness of their function relies on any computationally hard problem.

This paper proposes, for the first time, a new candidate for a quantum trapdoor one-way function, whose one-wayness relies on the hardness of the following well-known NP-problem, called the Graph Automorphism Problem (GA): Given an undirected graph G, decide whether G has a non-trivial automorphism or not. We show that if a quantum computer can efficiently invert our trapdoor one-way function then GA can be solved efficiently on a quantum computer. Since GA is not yet known to be efficiently computable on a quantum computer, our function is likely to be one-way. In addition, it is known that GA can be quantumly reducible to the hidden subgroup problem for the symmetric group. Although quantum Fourier transformation (QFT) seems essential in quantum computation, recent study [3, 4] shows that QFT alone cannot efficiently solve the hidden subgroup problem for the symmetric group. We also show that the complexity of finding a trapdoor is at least as hard as searching for the unique non-trivial automorphism for any given graph.

From our quantum trapdoor one-way function, we build a provably secure quantum public-key cryptosystem. Our cryptosystem exploits the computational indistinguishability of certain two quantum states built from classical trapdoors. The security of our cryptosystem relies on the hardness of GA since the inversion of our trapdoor one-way function is reducible to GA.

2 Quantum Trapdoor One-Way Function

Let n be a *hardness parameter* (or *security parameter* in the cryptographic sense), which specifies the hardness of inverting our function, and let m be a *precision parameter*, which specifies the precision of the inversion and is

*kawachi@kuis.kyoto-u.ac.jp
†koshiba@qci.jst.go.jp
‡anishi@site.uottawa.ca
§yamakami@site.uottawa.ca

a polynomial in n (e.g., $m = n$).

Our proposed trapdoor one-way function maps 0 and 1 respectively into the following two quantum states:

$$\iota_m = \bigotimes_m I/n! \quad \text{and} \quad \varrho_m = \bigotimes_m \rho_\pi,$$

where

$$\rho_\pi = \frac{1}{2n!} \sum_{\sigma \in S_n} (|\sigma\rangle + |\sigma\pi\rangle)(\langle\sigma| + \langle\sigma\pi|),$$

with a trapdoor $\pi \in S_n - \{id\}$.

Corresponding to our function, we can construct two quantum algorithms: one that efficiently computes our function (Theorem 1) and the other that efficiently inverts our function with a trapdoor (Theorem 2).

Theorem 1 *Given $\pi \in S_n - \{id\}$, we can generate the quantum state ρ_π with probability $1-(1/2)^n$ in time polynomial in n.*

Theorem 2 *Given $\pi \in S_n - \{id\}$, there exists a quantum polynomial-time algorithm which can invert ϱ_m to 1 and ι_m to 0 with success probability at least $1 - e^{-m/128}$.*

Next, we consider the hardness of inverting our function. We can show that the distinction between ϱ_m and ι_m is at least as hard as a special case of GA, called UniqueGA: Given an undirected graph G that has only one non-trivial automorphism or none, decide whether G has the non-trivial automorphism or not.

Lemma 3 *If there exists a polynomial-time quantum algorithm which can distinguish ϱ_m from ι_m with non-negligible probability* on average *when we choose $\pi \in S_n - \{id\}$ uniformly at random, there exists a polynomial-time quantum algorithm which can solve UniqueGA with non-negligible probability.*

Köbler et al. [5] gave a proof of the proposition which implies that UniqueGA is as hard as GA. (The UniqueGA is a promise problem and it was called (1GA,GA) in [5].)

Proposition 4 *(Köbler, Schöning, and Torán [5]) GA is polynomial-time Turing reducible to UniqueGA.*

Thus, we can show the hardness of the one-wayness of our function by combining the above lemma and proposition.

We can also show the hardness of finding π from ρ_π by reducing it to a search variant of GA, called UniqueGA-search: Given an undirected graph G that has only one non-trivial automorphism, find the non-trivial automorphism. Note that GA can be solved using the oracle that efficiently solves UniqueGA-search.

Lemma 5 *If there exists a polynomial-time quantum algorithm which can find π from polynomially many ρ_π's when we choose π from the uniform distribution over $S_n - \{id\}$ with non-negligible probability, there exists a polynomial-time quantum algorithm which can solve UniqueGA-search with non-negligible probability.*

From Lemmas 3 and 5, and Proposition 4, we can prove that the inversion of our function is at least as hard as solving GA.

Theorem 6 *If there exists a polynomial-time quantum algorithm which can invert ϱ_m to 1 and ι_m to 0 with non-negligible probability in the average case when we choose $\pi \in S_n - \{id\}$ uniformly at random, there exists a polynomial-time quantum algorithm which can solve GA with non-negligible probability.*

3 Quantum Public-Key Cryptosystem

When Alice wants to send a classical message to Bob, she can send it securely under a public-key cryptosystem based on our quantum trapdoor one-way function. First, Bob chooses a non-trivial permutation π as a secret key from $S_n - \{id\}$ uniformly at random. Then, Bob can efficiently generate the mixed state ρ_π as a public key (Theorem 1). He generates sufficiently-many public keys for Alice's encryption. Obtaining the public keys from Bob, Alice can encrypt 0 into the mixed state ι_m and 1 into ϱ_m respectively, and then she sends the encrypted message to Bob. After receiving Alice's message, Bob can efficiently decrypt it using the secret key π (Theorem 2). We can guarantee the security of this cryptosystem from the difficulty in inverting our function (Theorem 6).

References

[1] M. Adcock and R. Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *Proc. 19th Symposium on Theoretical Aspects of Computer Science, LNCS 2285*, pages 323–334, 2002.

[2] D. Gottesman and I. Chuang. Quantum digital signatures. quant-ph/0105032, 2001.

[3] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proc. 33rd ACM Symposium on Theory of Computing*, pages 68–74, 2001.

[4] S. Hallgren, A. Russell, and A. Ta-shma. The hidden subgroup problem and quantum computation using group representations. In *Proc. 32nd ACM Symposium on Theory of Computing*, pages 627–635, 2000.

[5] J. Köbler, U. Schöning, and J. Torán. *The graph isomorphism problem: its structural complexity.* Birkhäuser Boston Inc., 1993.

[6] T. Okamoto, K. Tanaka, and S. Uchiyama. Quantum public-key cryptosystems. In *Proc. CRYPTO2000*, pages 147–165, 2000.

[7] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.