The Existence of Quantum One-Way Functions

Ping Wang[1], Yikang Lei[1], Zishen Shen[2] and Fangguo Zhang[3]

[1] College of Electronics and Information Engineering,
Shenzhen University, Shenzhen 518060, China
wangping@szu.edu.cn, leiyikang2022@email.szu.edu.cn
[2] Pasadena City College, California 91106, USA
zshen19@go.pasadena.edu
[3] School of Computer Science and Engineering,
Sun Yat-sen University, Guangzhou 510006, China
isszhfg@mail.sysu.edu.cn

Abstract. One-way functions are essential tools for cryptography. However, the existence of one-way functions is still an open conjecture. By constructing a function with classical bits as input and quantum states as output, we prove for the first time the existence of quantum one-way functions. It provides theoretical guarantees for the security of many quantum cryptographic protocols.

Keywords: one-way function, quantum one-way function, classical to quantum

1 Introduction

One-way function f is that f can be computed by a polynomial-time algorithm, but f^{-1} can not be computed by any polynomial-time algorithm.

Definition 1 (One-Way Function (OWF)). *A function $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function, if f can be computed by a polynomial-time algorithm, and for any polynomial-time algorithm A, any positive integers c and any sufficiently large $|x|$,*

$$Pr[f(A(f(x))) = f(x)] < |x|^{-c}, \tag{1}$$

where x is chosen from the discrete uniform distribution on $\{0,1\}^{|x|}$.

The existence of one-way functions would prove P $\neq$ NP [11,13], thus addressing a fundamental problem in computer science. However, a proof of P $\neq$ NP does not imply the existence of one-way functions, as the difficulty in one-way functions must be the average-case, not the worst-case for complexity theory [10]. Candidates for one-way functions in information theory include problems such as large integer factorization, discrete logarithm problems, and

cryptographic hash functions. One-way functions are fundamental tools for cryptography, pseudorandom generators [14], digital signature schemes [20,24,28], bit commitment protocols [16,17], and other security applications.

The existence of one-way functions is still unknown. However, if one considers using quantum states as the output of a function, it may not be feasible to derive the input bit without knowing the exact information (one copy) of the output quantum states based on the principles of quantum mechanics: quantum no-cloning theorem [22,27] and quantum superposition principle [9,18]. Therefore, a quantum one-way function with classical input and quantum output may exist. We have the following definition of classical to quantum one-way function.

Definition 2 (Classical to Quantum One-Way Function (CQOWF)). *A classical to quantum function $f : \{0,1\}^* \to H$ ($Hilbert\ space$) is a one-way function, if f can be computed by a polynomial-time algorithm, and for any polynomial-time classical or quantum algorithm A, any positive integers c and any sufficiently large $|x|$,*

$$Pr[f(A(f(x))) = f(x)] < |x|^{-c}, \tag{2}$$

where x is chosen from the discrete uniform distribution on $\{0,1\}^{|x|}$.

Functions that require quantum operations or involve quantum states are called quantum functions. The concept of quantum OWF was first introduced in [4,12]. Nikolopoulos [21] proposed a quantum trapdoor function that achieves classical to quantum mapping using single-qubit rotations. This function maps any n bit string to a qubit. Although the design can be used to construct quantum public-key cryptography, it is clear that it fails to meet the criterion of a quantum one-way function: let the outputs corresponding to any two inputs x_1 and x_2 be $|\varphi_1\rangle$ and $|\varphi_2\rangle$, and comparing $|\varphi_1\rangle$ and $|\varphi_2\rangle$ by swap-test, it is impossible to obtain an error probability less than n^{-c}.

Inspired by the BB84 quantum key distribution protocol [2], we introduce a new classical to quantum one-way function, which maps classical information to quantum states, and show that the proposed function satisfies the properties of the quantum one-way function, thereby proving the existence of quantum one-way functions.

2 Proposed CQOWF

2.1 The definition

We consider the following function f with classical bits as input and quantum states as output:

$$f : \{0,1\}^{2n} \to H^{\otimes n},$$
$$f(x) = f(x' \parallel x'') = |\varphi\rangle,$$
$$x', x'' \in \{0,1\}^n; |\varphi\rangle = \otimes_{i=1}^{n} |\varphi_i\rangle,$$

where $x = x' \parallel x''$ (" $\parallel$ " denotes the concatenation of bit strings). Taking x' as the bit string to be encoded and x'' as the encoding basis (where 0 represents the standard basis and 1 represents the Hadamard basis), we get the output as follows:

$$|\varphi_i\rangle = \begin{cases} |0\rangle, & x'_i = 0 \text{ and } x''_i = 0; \\ |1\rangle, & x'_i = 1 \text{ and } x''_i = 0; \\ |+\rangle, & x'_i = 0 \text{ and } x''_i = 1; \\ |-\rangle, & x'_i = 1 \text{ and } x''_i = 1. \end{cases}$$

2.2 Proof of the function satisfying the CQOWF properties

For the proposed classical to quantum one-way function: $f : x \to |\varphi\rangle$, the process of generating $|\varphi\rangle$ from the input x is the process of encoding classical bits into qubits. That is, encoding x' into quantum states based on x''. Therefore, f can be computed efficiently with a polynomial-time complexity of $O(n)$.

Therefore, the key to satisfying the one-wayness of a function is the property of hard to invert. It means that the success probability for any probabilistic polynomial-time quantum algorithm to compute f^{-1} is negligible:

$$Pr[f(A(|\varphi\rangle)) = |\varphi\rangle] < n^{-c},$$

for any positive integers c and any sufficiently large n. In the proposed classical to quantum one-way function, different inputs correspond to different combinations of x' and x'', resulting in distinct output quantum states. This guarantees that the function is a one-to-one mapping.

The one-wayness of the proposed classical to quantum one-way function lies in the fact that it is not possible to obtain full information about the output based on (one copy of) the output quantum states, therefore, it is not possible to obtain the input bits. Regarding $f : x \to |\varphi\rangle$, deriving the input bits implies successful decoding of $|\varphi\rangle$. Decoding $|\varphi\rangle$ means accurately identifying each qubit in $|\varphi\rangle$. More precisely, if one wants to decode each qubit in $|\varphi\rangle$ without x, then for each qubit, the probability of selecting the correct encoding basis to measure it is $1/2$, and the probability P_x of obtaining the correct result for a single qubit is $P_x = 1/2 \times 1 + 1/2 \times 1/2 = 3/4$. Therefore, the probability of correctly decoding the corresponding output (i.e., getting the input bits) is $(3/4)^n$, which exponentially decreases as n increases. According to the principles of quantum mechanics, measurement leads to quantum collapse, resulting in irreversible effects on the quantum state, making it infeasible to directly derive the input through measurement.

However, an adversary with infinite computational resources can exhaust the inputs and compare the corresponding outputs (forming the set Q, where $|Q| = 2^n$) with $|\varphi\rangle$. Thus, the exhaustive attack to reverse $|\varphi\rangle$ can be viewed as a quantum state discrimination problem based on the set Q. Note that $|Q| = 2^n$ contains not only completely orthogonal quantum states but also some non-orthogonal ones. The orthogonal quantum states can be correctly distinguished with a probability of 1 through projection measurement. However, for an unknown state $|\varphi\rangle$, the probability of selecting the same state as $|\varphi\rangle$ or its orthogonal state from Q is $1/2^{n-1}$. Hence, the probability of successfully getting x by

projecting two orthogonal states is $P_r(succeed) = 1 \times 1/2^{n-1} = 1/2^{n-1}$. On the other hand, the unambiguous discrimination of non-orthogonal quantum states through Ivanović-Dieks-Peres (IDP) measurement [8,15,23], as a general measurement, can explicitly distinguish them. This "unambiguous" means knowing deterministically whether successful discrimination is achieved, though the measurement may still yield inconclusive results. Under the assumption of equal prior probabilities for the two states, the probability of obtaining a deterministic result with IDP measurement is $1 - |\langle\varphi|\psi\rangle|$, known as the IDP limit. The maximum average success probability of distinguishing multiple non-orthogonal quantum states is given by $P_r(succeed) = \sum_{j=1}^{n} \eta_j P_j$, where η_j represents the prior probability and P_j is the probability of successfully discriminating the system under the condition of $|\varphi_j\rangle$. However, note that Chefles [5] proved that a necessary and sufficient condition for the existence of unambiguous measurement strategies is that these states must be linearly independent. As the quantum states in set Q are linearly dependent, the unambiguous quantum state discrimination (UQSD) [3,6] strategy is not applicable.

In fact, for the proposed classical to quantum function f, if the input can be derived based on $|\varphi\rangle$, then it will lead to the breaking of the BB84 protocol [29]. More precisely, the purpose of the BB84 protocol is to establish a shared key between two parties. Alice encodes classical bits into qubits using randomly chosen base (for each classical bit, Alice chooses one at random between the computational basis and the Hadamard basis), and sends the qubits to Bob. If one can derive the inputs from the outputs of the above function f , then an adversary can derive the base and classical bits chosen by Alice from the qubits she sends to Bob, and thus can get all the information Alice sends to Bob without being detected. This contradicts that BB84 protocol is unconditionally secure. The security of both the quantum function f and the BB84 protocol relies on the difficulty of decoding qubits into classical bits without additional information. This difficulty arises from the no-cloning theorem and superposition properties in quantum mechanics. Therefore, the proposed quantum one-way function's security can be deduced from the security of the BB84 protocol. In other words, if $f : x \to |\varphi\rangle$ can be reversed, then an adversary could also effectively eavesdrop on the BB84 protocol. The unconditional security of the BB84 protocol has been proven [19,25], thus the quantum one-way function $f : x \to |\varphi\rangle$ satisfies one-wayness. The fundamental principles of quantum mechanics guarantee that f is unconditionally irreversible.

3 Conclusion

In this paper, by constructing a classical to quantum function that is not just irreversible within polynomial-time but unconditionally irreversible, we prove for the first time the existence of quantum one-way functions. In fact, the one-wayness of this function lies at the heart of the security of many quantum cryptographic protocols [1,2,7,26] and is the reason why quantum cryptography can surpass classical cryptography to achieve unconditional security.

References

1. X. B. An, H. Zhang, C. M. Zhang, W. Chen, S. Wang, Z. Q. Yin, Q. Wang, D. Y. He, P. L. Hao, and S. F. Liu. Practical quantum digital signature with a gigahertz bb84 quantum key distribution system. *Optics letters*, 44(1):139–142, 2018.
2. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.
3. J. A. Bergou. Discrimination of quantum states. *Journal of Modern Optics*, 57(3):160–180, 2010.
4. H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.
5. A. Chefles. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, 239(6):339–347, 1998.
6. A. Chefles. Quantum state discrimination. *Contemporary Physics*, 41(6):401–424, 2000.
7. S. K. Chong and T. Hwang. Quantum key agreement protocol based on BB84. *Optics Communications*, 283(6):1192–1195, 2010.
8. D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126(5-6):303–306, 1988.
9. P. A. M. Dirac. *The principles of quantum mechanics*. Number 27. Oxford university press, 1981.
10. O. Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.
11. S. Goldwasser and M. Bellare. Lecture notes on cryptography. *Summer course "Cryptography and computer security" at MIT*, 1999:1999, 1996.
12. D. Gottesman and I. Chuang. Quantum digital signatures. *arXiv preprint quant-ph/0105032*, 2001.
13. L. A. Hemaspaandra, J. Rothe, and A. Saxena. Enforcing and defying associativity, commutativity, totality, and strong noninvertibility for one-way functions in complexity theory. In *Italian Conference on Theoretical Computer Science*, pages 265–279. Springer, 2005.
14. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 12–24, 1989.
15. I. D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257–259, 1987.
16. T. Koshiba and T. Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In *Theory of Quantum Computation, Communication, and Cryptography: 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13, 2009, Revised Selected Papers 4*, pages 33–46. Springer, 2009.
17. T. Koshiba and T. Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv preprint arXiv:1102.3441*, 2011.
18. T. Kovachy, P. Asenbaum, C. Overstreet, C. A. Donnelly, S. M. Dickerson, A. Sugarbaker, J. M. Hogan, and M. A. Kasevich. Quantum superposition at the half-metre scale. *Nature*, 528(7583):530–533, 2015.
19. H. K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *science*, 283(5410):2050–2056, 1999.

20. X. Lu and D. Feng. Quantum digital signature based on quantum one-way functions. In *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005.*, volume 1, pages 514–517. IEEE, 2005.
21. G. M. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A*, 77(3):032348, 2008.
22. J. L. Park. The concept of transition in quantum mechanics. *Foundations of physics*, 1:23–33, 1970.
23. A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128(1-2):19, 1988.
24. J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 387–394, 1990.
25. P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.
26. P. Wang, Y. K. Lei, and Y. T. Su. Unconditionally secure quantum bit commitment and quantum oblivious transfer. *Cryptology ePrint Archive*, 2023.
27. W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.
28. X. Xin, Z. Wang, Q. He, Q. Yang, and F. Li. New public-key quantum signature scheme with quantum one-way function. *International Journal of Theoretical Physics*, 58:3282–3294, 2019.
29. N. S. Yanofsky and M. A. Mannucci. *Quantum computing for computer scientists*. Cambridge University Press, 2008.