Quantum collision-resistance of non-uniformly distributed functions*

Ehsan Ebrahimi Targhi, Gelo Tabia, Dominique Unruh

University of Tartu

April 25, 2015

Abstract

We study the quantum query complexity of finding a collision for a function f whose outputs are chosen according to a distribution with min-entropy k. We prove that $\Omega(2^{k/9})$ quantum queries are necessary to find a collision for function f.

Keywords: Quantum, Collision, Non-uniform distribution, Query complexity.

The problem and motivation: Let D be a distribution with min-entropy k over set Y and f be a function whose outputs are drawn according to the distribution D. In this paper, we study the difficulty of finding a collision for unknown function f in the quantum query model. Recall that a collision for function f consists of two distinct inputs x_1 and x_2 such that $f(x_1) = f(x_2)$. Classically, by application of the birthday attack it is easy to observe that $\Theta(2^{k/2})$ queries are necessary and sufficient to find a collision with constant probability. However, in quantum query model this number of queries may be high for the reason that one quantum query may contain the whole input-output values of function.

Zhandry [Zha15] shows that $\Theta(2^{k/3})$ quantum queries are necessary and sufficient to find a collision for the function f when D is a uniform distribution. However, he leaves the non-uniform case as an open problem. One motivation for studying the quantum collision problem for non-uniform distribution is the interest in proving the security of classical cryptographic schemes against quantum adversaries. Hash functions are a crucial cryptographic primitive that are used to construct many encryption schemes and cryptographic schemes. They are usually modeled as a random function and they are used inside to other functions. Therefore the output of combination of a function and a random function may not be distributed uniformly and finding a collision for this non-uniform distribution may break the security of the scheme. For example the well-known Fujisaki-Okamoto construction [FO99] uses a random function to produce the randomness for an encryption scheme. The security relies on the fact that the adversary can not find two inputs of the random function that lead to the same ciphertext. This is roughly equivalent to saying that $Enc \circ H$ is collision-resistant where Enc stands for the encryption function and H is a random function. In fact, our result is a crucial ingredient for analyzing a variant of Fujisaki-Okamoto construction in the quantum setting [ETU15].

Our Contribution: We prove an $\Omega(2^{k/9})$ lower bound for the quantum query complexity of the function f. The proof procedure is as follows. We apply the Leftover Hash Lemma [HILL93] to the function f to extract the number of bits that are indistinguishable from uniformly random bits. After applying the Leftover Hash Lemma, the output distribution of $h \circ f$, where h is a

*Full paper: `http://www.cs.ut.ee/~unruh/collision.pdf`

universal hash function, is indistinguishable from the uniform distribution over a set. Let A be a quantum adversary that has quantum access to f and finds a collision for f. Using the existence of A, we show that there exists a quantum algorithm B that has quantum access to $h \circ f$ and finds a collision for $h \circ f$ with the same probability and the same number of queries as algorithm A. Theorem 1.1 by Zhandry [Zha12] shows that two distribution are indistinguishable if and only if they are oracle-indistinguishable. Therefore, $h \circ f$ is indistinguishable from a random function (recall that the output of $h \circ f$ is indistinguishable from the uniform distribution by Leftover Hash Lemma) and as a result any algorithm B that finds a collision should not be able to differentiate between $h \circ f$ and a random function. By using an existing result for finding a collision for a random function presented by Zhandry [Zha15, Theorem 3.1], we obtain an upper bound for the probability of finding a collision for function $h \circ f$. Note that a collision for f is a collision for $h \circ f$. Therefore, we get an upper bound for the probability of success for the quantum collision problem applied to the function f. Following, we present the main theorem of our work:

Theorem 1. *Let D be a distribution over set Y with $H_\infty(D) \geq k$ and X be some other set. Let O be a function drawn from distribution D^X, where D^X is the distributions of functions from X to Y where for each $x \in X$, $D^X(x)$ is chosen independently according to D. Then any quantum algorithm A making q query to O returns a collision for O with probability at most $\frac{C(q+1)^{9/5}}{2^{k/5}}$. That is,*

$$\Pr[\mathsf{Coll}(O; A^O) : O \leftarrow D^X] \leq \frac{C(q+1)^{9/5}}{2^{k/5}}.$$

The existing lower bounds: The quantum collision problem has been studied in various previous works. Following, we mention the existing results on the number of queries that are necessary to find a collision. An $\Omega(N^{1/3})$ lower bound for function f is given by Aaronson and Shi [AS04] and Ambainis [Amb05] where f is a two-to-one function with the same domain and co-domain and N is the domain size. Yuen [Yue14] proves an $\Omega(N^{1/5}/\text{polylog}N)$ lower bound for the quantum collision problem for a random function f with same domain and co-domain. He reduces the distinguishing between a random function and a random permutation problem to the distinguishing between a function with r-to-one part and a function without r-to-one part. His proof is a merger of using the r-to-one lower bound from [AS04] and using the quantum adversary method [Amb00]. Zhandry [Zha15] improves the Yuen's bound to the $\Omega(N^{1/3})$ and also removes the same size domain and co-domain constraint. He uses the existing result from [Zha12] to prove his bound.

The existing upper bounds: The sufficient number of quantum queries to find a collision is given in the following works. A quantum algorithm that requires $O(N^{1/3})$ quantum queries and finds a collision for any two-to-one function f with overwhelming probability is given by Brassard, Hϕyer and Tapp [BHT97]. Ambainis [Amb07] gives a quantum algorithm that requires $O(N^{2/3})$ queries to find two equal elements among N given elements and therefore it is an algorithm for finding a collision in an arbitrary function f given the promise that f has at least one collision. Yuen [Yue14] shows that the collision-finding algorithm from [BHT97] is able to produce a collision for a random function with same domain and co-domain using $O(N^{1/3})$ queries. Zhandry shows that $O(M^{1/3})$ queries are adequate to find a collision for a random function $f : [N] \to [M]$ where $N = \Omega(M^{1/2})$. He uses Ambainis's element distinctness algorithm [Amb07] as a black box in his proof. Zhandry's bound also implies that we can not expect a lower bound for the query complexity of finding a collision for a non-uniform function better than $O(2^{k/3})$.

References

[Amb00] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 636–643, 2000.

[Amb05] Andris Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1(1):37–46, 2005.

[Amb07] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007.

[AS04] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, July 2004.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. *ACM SIGACT News (Cryptology Column)*, 28:14–19, 1997.

[ETU15] Ehsan Ebrahimi Targhi and Dominique Unruh. Quantum security of the Fujisaki-Okamoto transform. 2015. Available at `http://www.cs.ut.ee/~unruh/qro.pdf`.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 537–554, London, UK, UK, 1999. Springer-Verlag.

[HILL93] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Construction of a pseudo-random generator from any one-way function. *SIAM Journal on Computing*, 28:12–24, 1993.

[Yue14] Henry Yuen. A quantum lower bound for distinguishing random functions from random permutations. *Quantum Information & Computation*, 14(13-14):1089–1097, 2014.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687, 2012.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015.