12

Quantum algorithm for finding collisions of hash functions

Toward secure cryptography against quantum attacks

Abstract

Recently, the security analysis of ciphers against quantum attacks is rapidly growing in importance, since quantum computers could make strong attacks on them in the future. For such a security analysis, it is crucial to evaluate how fast quantum computers can solve the problems used to break ciphers. Among others, it is one of the major problems to find a multi-collision of random hash functions, essential primitives used ubiquitously in cryptosystems. In this work, we provide a novel quantum algorithm that solves this problem. This algorithm is the fastest among all possible ones in the sense that it achieves the theoretical limit. Our result would contribute to enhancing the security of hash-based ciphers in the quantum-computer era.

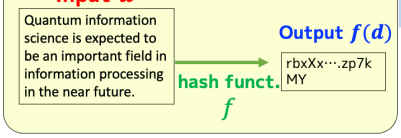
Background and Our Result

- **The security of cryptosystems is based on how much time is required to attack them** (e.g., even the fastest computers take a billion years for breaking some cipher).
- As quantum computers have been actively developed recently, **the security analysis of ciphers against quantum attacks** is rapidly growing in importance.

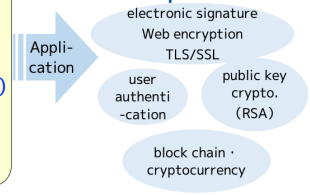
We provide a **fastest quantum algorithm that finds a multi-collision of a hash function,** an important cryptographic primitive.
⇨Our result would contribute to the security analysis of various hash-based cryptosystems against quantum attacks.

Hash Functions

A hash function outputs a short string from which the original string is hard to infer.

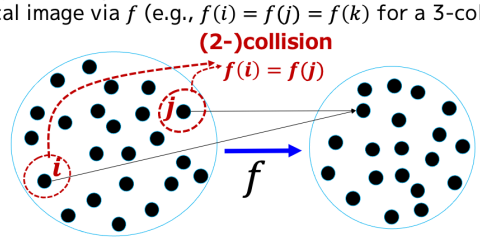


Various situations where tampering detections are required



Collision of Hash Functions

A pair of elements is called a **(2-)collision** if they have an identical image via f. Similarly, an **ℓ-collision** is defined as ℓ elements with an identical image via f (e.g., $f(i)=f(j)=f(k)$ for a 3-collision).



Finding a collision makes it possible to tamper electronic data.
⇨For assessing the security, it is necessary to estimate the hardness of (i.e., the time required for) finding collisions.
⇨**Such estimation requires algorithms for finding collisions.**

Driving force behind the improvement of security of hash functions has been the discovery of faster collision-finding algorithms

MD5 ['91] ➡ SHA-1 ['95] ➡ SHA-2 ['02] ➡ SHA-3 ['15]

Details of our Algorithm

We provide a theoretical bound on the run-time taken by our quantum algorithm to find a multi-collision for a given random hash function. Then, we illustrate the idea used in our algorithm.

For a given random hash function $f:\{1,\cdots,M\}\to\{1,\cdots,N\}$ $(M \geq N)$, **our quantum algorithm can find an ℓ-collision of f in $N^{\frac{1}{2}\left(1-\frac{1}{2^{\ell}-1}\right)}$ time.**
(assuming that f can be computed quickly).

◎This attains the theoretical time bound (matching with the lower bound [LZ20])

Comparison with Previous Bound [HSX17] on Time Complexity

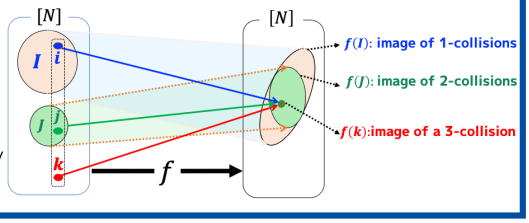
ℓ (multiplicity)	2	3	4	5	⋯	ℓ
Previous algorithm [HSX17]	$N^{\frac{1}{3}}$	$N^{\frac{4}{9}}$	$N^{\frac{13}{27}}$	$N^{\frac{40}{81}}$	⋯	$N^{\frac{1}{2}\left(1-\frac{1}{3^{\ell}-1}\right)}$
Our algorithm	$N^{\frac{1}{3}}$	$N^{\frac{3}{7}}$	$N^{\frac{7}{15}}$	$N^{\frac{15}{31}}$	⋯	$N^{\frac{1}{2}\left(1-\frac{1}{2^{\ell}-1}\right)}$

Ex.) In the case of $\ell=3$ and $N=2000$, ours is a **billion times faster** than the previous algorithm.
N:2000bit→ $N^{\frac{4}{9}}$: $N^{\frac{3}{7}} \approx 1,000,000,000:1$

Outline of Algorithm (3-collision case)

1. Sample subset $I \subset [N]$ and compute the image $f(I)$ of I, where $[N] \equiv \{1,\cdots,N\}$
2. Find a subset $J \subset [N] \setminus I$ that forms 2-collisions with elements in I, and compute $f(J)$.
3. Find an element $k \in [N] \setminus (I \cup J)$ that forms a 3-collision with an element pair in $I \times J$.
4. Output the triplet (i,j,k).

1. Sample subset I
2. Find $J \subset [N] \setminus I$ by using **quantum search**
3. Find $k \in [N] \setminus (I \cup J)$ by using **quantum search**



References

[1] A. Hosoyamada, Y. Sasaki, S. Tani, K. Xagawa, "Improved quantum multicollision-finding algorithm," in *Proc. 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019)*, pp. 350–367, vol. 11505, 2019.
[2] A. Hosoyamada, Y. Sasaki, S. Tani, K. Xagawa, "Quantum algorithm for the multicollision problem," *Theoretical Computer Science*, vol. 842, pp. 100–117, 2020.

Contact

Seiichiro Tani / Computing Theory Research Group, Media Information Laboratory
Email: cs-openhouse-ml@hco.ntt.co.jp