The Gap Is Sensitive to Size of Preimages: Collapsing Property Doesn't Go Beyond Quantum Collision-Resistance for Preimages Bounded Hash Functions

Shujiao Cao[1,2] and Rui Xue[1,2(✉)]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
{caoshujiao, xuerui}@iie.ac.cn

Abstract. As an enhancement of quantum collision-resistance, the collapsing property of hash functions proposed by Unruh (EUROCRYPT 2016) emphasizes the hardness for distinguishing a superposition state of a hash value from a collapsed one. The collapsing property trivially implies the quantum collision-resistance. However, it remains to be unknown whether there is a reduction from the collapsing hash functions to the quantum collision-resistant hash functions. In this paper, we further study the relations between these two properties and derive two intriguing results as follows:

- Firstly, when the size of preimages of each hash value is bounded by some polynomial, we demonstrate that the collapsing property and the collision-resistance must hold simultaneously. This result is proved via a semi-black-box manner by taking advantage of the invertibility of a unitary quantum circuit.
- Next, we further consider the relations between these two properties in the exponential-sized preimages case. By giving a construction of polynomial bounded hash functions, which preserves the quantum collision-resistance, we show the existence of collapsing hash functions is implied by the quantum collision-resistant hash functions when the size of preimages is not too large to the expected value.

Our results indicate that the gap between these two properties is sensitive to the size of preimages. As a corollary, our results also reveal the non-existence of polynomial bounded equivocal collision-resistant hash functions.

Keywords: quantum collision-resistance, collapsing property, equivocal collision-resistance, hash function

1 Introduction

As a central property of hash functions, collision-resistance plays an important role in the development of cryptography. It emphasizes the hardness of finding two distinct inputs which share the same hash value. The collision-resistant hash functions can be used to construct many cryptographic objects, such as the digital signature, the Merkle tree, and succinct (zero-knowledge) arguments [25,29,6]. Indeed, the existence of collision-resistant hash function yields the existence of the primitives in MiniCrypt such as the one-way function and the pseudorandom generator. It can increase the efficiency of cryptographic schemes than simply using the one-way function in many cases. And it has been proven that the opposite direction is infeasible via the black-box reduction [36]. As a variant of collision-resistance, some other properties such as preimage resistance and second-preimage resistance have been extended and studied by Rogaway and Shrimpton [34].

When the collision-resistance is considered in the quantum case, it should also be infeasible to generate a collision for any quantum efficient adversary. Namely for a quantum secure collision-resistant hash function H_n, there doesn't exist any quantum adversary $\mathcal{A}$ that finds a distinct pair $x_0 \neq x_1$ such that $H_n(x_0) = H_n(x_1)$. However, it seems that the quantum collision-resistance is still inadequate in the quantum setting. In order to devise a quantum commitment that achieves a post-quantum secure binding property, Unruh proposed the notion of collapsing hash function, which is stronger than the quantum collision-resistant hash function [38]. Informally, a function H_n is collapsing, if given a superposition $\sum a_{x,z}|x, H(x), z\rangle$, any quantum efficient adversary can not detect wether the input register or the output register has been measured. Notice that the collapsing property implies the quantum collision-resistance trivially, since if there exists an adversary $\mathcal{A}$ that finds a distinct pair $x_0 \neq x_1$ such that $y = H_n(x_0) = H_n(x_1)$, it is easy to generate and check the state $(|x_0, y\rangle + |x_1, y\rangle)/\sqrt{2}$, which hence breaks the collapsing property of H_n. In the other direction, Unruh gave evidence showing that there exists a construction $H_n^{\mathcal{O}}$ that is quantum collision-resistant but not collapsing relative to a quantum oracle $\mathcal{O}$ [38]. Then, several quantum analogues of properties such as preimage resistance and second-preimage resistance have been formalized and discussed in [23,20]. Zhandry proved that the existence of quantum collision-resistant hash functions which is not collapsing implies the existence of quantum lightning in infinity-often sense [43]. Moreover, Amos et al. proposed another quantum security definition of hash functions called the equivocal collision-resistant hash functions and derived a construction relative to a classical oracle, which also yields a classical oracle construction of non-collapsing quantum collision-resistant hash functions [4].

However, these results don't rule out the reduction from the collapsing hash functions to the quantum collision-resistant hash functions. It remains to be unknown whether we can construct the collapsing hash functions from the quantum collision-resistant hash functions in a black-box (or non-black-box) manner. That hence raise the motivation of this work:

Does the existence of quantum collision-resistant hash functions imply the existence of collapsing hash functions?

This motivated us to further study the relations of these properties theoretically. If there is a universal construction of collapsing hash functions from quantum collision-resistant hash functions, if not, can we set up a quantum black-box barrier between these two primitives?

1.1 Our Result

In this paper, we further investigate the relations between quantum collision-resistance and collapsing property and get a surprising result. Although there is a oracle-aided construction separates these two post-quantum security definitions, these two primitives might be equivalent in many cases.

In order to exhibit our results, we firstly classify these hash functions by the upper bound of the size of preimages. Informally, we call a collection of functions $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}_{n\in\mathbb{N}}$ is $\delta(n)$-bounded if any hash value of $H_n(k, \cdot)$ has at most $\delta(n)$ preimages for any $k \in \mathbf{K}$ [3]. We denote it as regular bounded and polynomial bounded for simplicity if $\delta(n)$ is $O(|\mathbf{X}/\mathbf{Y}|)$ or $\mathtt{poly}(n)$ for some postive polynomial $\mathtt{poly}(\cdot)$ respectively. And $\{H_n\}_{n\in\mathbb{N}}$ is almost $\delta(n)$-bounded if it is $\delta(n)$-bounded with overwhelming probability over the randomness of the evaluation key (the almost regular bounded and almost polynomial bounded are defined accordingly). Hence our results can be discussed separately according to the size of preimages.

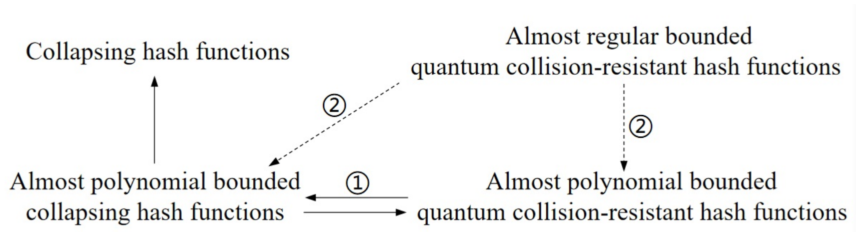

Fig. 1. The arrow "$A \to B$" means that the primitive A satisfies the property of B. The dotted arrow $A \dashrightarrow B$ indicates that if the primitive A exists, then so does B. The ①, ② are the main results proved in this paper, and other directions are implied naturally by their definitions.

Our main results can be described as the Figure 1, where ① represents our first result. That is, for any (almost) polynomial bounded hash functions, we can prove that surprisingly, the collapsing property is equivalent to the property of quantum collision-resistance.

Theorem 1 (informal). *For any collection of (almost) polynomial bounded hash functions $\{H_n\}$, it is collapsing iff it satisfies the quantum collision-resistance.*

[3] In the following part, we always assume the functions as $\{H_n : \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$ namely $\mathbf{X} = \{0,1\}^n$, $\mathbf{K} = \{0,1\}^{l(n)}$ and $\mathbf{Y} = \{0,1\}^{m(n)}$. Moreover, we always assume $\{H_n\}$ is compressing, namely $m(n) < n$ for all $n \in \mathbb{N}$, and $|\mathbf{X}|/|\mathbf{Y}| > C$ for general $H_n : \mathbf{X} \to \mathbf{Y}$, where $C > 1$ is a constant.

Then, as a corollary of that theorem, we can directly derive the non-existence of any polynomial bounded equivocal collision-resistant hash functions.

Corollary 1 (informal). *There doesn't exist any (almost) polynomial bounded quantum collision-resistant hash function that satisfies the equivocal property.*

The corollary above indicates that if we want to construct the equivocal collision-resistant hash functions, the input space of that function must be superpolynomially larger than the output space.

Then, as the second part of our results (which is exhibited as ② in Figure 1) we further explore the relations when the preimages are exponentially large. Based on the equivalence in the polynomial bounded case and construction of (almost) polynomial bounded hash functions from (almost) regular bounded hash functions which preserves the quantum collision-resistance, we prove the existence of (almost) polynomial bounded collapsing hash functions is implied by the (almost) regular bounded quantum collision-resistant hash functions. That hence implies the reduction from polynomial bounded collapsing hash functions to the (almost) regular bounded quantum collision-resistant hash functions.

Theorem 2 (informal). *The existence of (almost) polynomial bounded collapsing hash functions is implied by the existence of (almost) regular bounded quantum collision-resistant hash functions.*

Our result demonstrates that the gap between these two properties is sensitive to the size of preimages. Namely, fewer preimages and more regularity the hash functions have, more "close" these properties are.

As an application of that part, we show that Ajtai's construction of hash functions based on the short integer solution (**SIS**) problem is (almost) regular bounded [2,18].

Corollary 2 (informal). *There exists a construction of collapsing hash functions based on the short integer solution (*__SIS__*) assumption.*

1.2 Technical Overview

In this part, we show our main technique involved in this paper. We start by a detailed description of hash functions. A collection of hash functions $\{H_n : \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$ usually consists of two probabilistic polynomial-time algorithms $\texttt{Gen}$ and $\texttt{Eval}$, where $\texttt{Gen}(1^n)$ outputs an evaluation key $k \in \{0,1\}^{l(n)}$ with the security parameter 1^n as its input, and $\texttt{Eval}(k,\cdot)$ calculates the function $H_n(k,\cdot)$. The properties such as collision-resistance and collapsing property of $\{H_n\}$ stress that any quantum polynomial-time adversary $\mathcal{A}$ who gets the evaluation key k generated by $\texttt{Gen}(1^n)$ can not break the security of $H_n(k,\cdot)$ (e.g. can not find a collision of $H_n(k,\cdot)$ for a collection of collision-resistant hash functions $\{H_n\}$).

Recall that a collection of hash functions $\{H_n : \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$ is $\delta(n)$-bounded if it holds that

$$|\{x \mid H_n(k,x) = y\}| \leq \delta(n) \tag{1}$$

for any valid $k \in \{0,1\}^{l(n)}$ and $y \in \{0,1\}^{m(n)}$. In that case, we denote by regular bounded and polynomial bounded if $\delta(n) = O(2^{n-m(n)})$ and $\delta(n) = \texttt{poly}(n)$ for some positive polynomial $\texttt{poly}(\cdot)$ respectively. Similar definitions can be derived when we consider it in the keyless setting (i.e. the form $\{H_n : \times\{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$). And it is almost $\delta(n)$-bounded, if $H_n(k,\cdot)$ is $\delta(n)$-bounded with overwhelming probability, where the randomness is taken over the $k \leftarrow \texttt{Gen}(1^n)$.

The equivalence in bounded case. Since the key generation algorithm `Gen` seems not involved in our first result, without loss of generality, we sometimes assume the hash functions are constructed in the keyless setting for convenience. Namely, the key generation algorithm $\texttt{Gen}(1^n)$ generates the evaluation key deterministically for each security parameter. Therefore we denote by the collection of hash functions as $\{H_n : \{0,1\}^n \rightarrow \{0,1\}^m\}_{n \in \mathbb{N}}$ for simplicity. In that case, the quantum collision-resistance stresses the quantum hardness for finding a collision of H_n, and the collapsing property indicates that there is no (computational) difference between measuring the input register or the output register of H_n.

When the preimages of H_n are limited by some polynomial, we intent to take advantage of the invertibility of a quantum circuit and show the equivalence between these two properties. The strategy is that, assuming there exists a quantum adversary $\mathcal{A}$ that breaks the collapsing property of a hash function H_n efficiently, then we can construct another quantum polynomial-time adversary $\mathcal{B}$ breaks the quantum collision-resistance of H_n as well. In order to make it clear, we divide the adversary $\mathcal{A}$ of the collapsing experiment into two phases $\mathcal{A}_1, \mathcal{A}_2$, which is formalized in Figure 2.

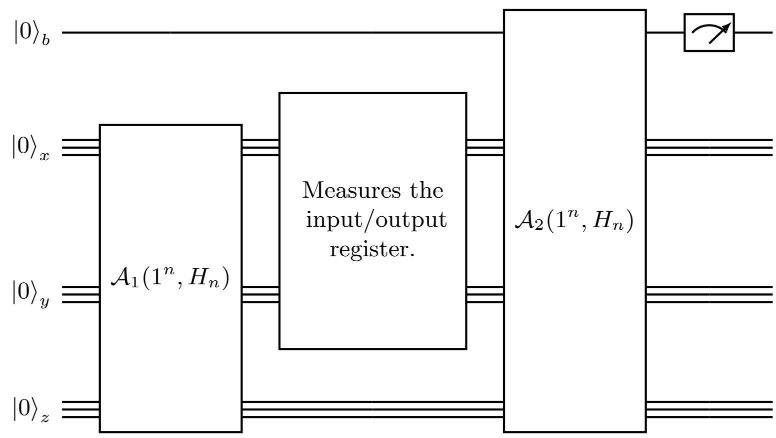

Fig. 2. The description of $\mathcal{A}$. Where the register of $|0\rangle_b$ stores the decision of $\mathcal{A}$, and $|0\rangle_x, |0\rangle_y$ store the input/ output of H_n respectively. $|0\rangle_z$ stores the auxiliary bits of $\mathcal{A}$. The second step means it would randomly toss a coin $b \leftarrow \{0,1\}$, when $b = 0$ it would measure the output register, and when $b = 1$ it would measure the input register.

At the first phase of the collapsing experiment, $\mathcal{A}_1$ gets the security parameter and the description of H_n as its input, then generates a challenge state ρ and sends it to the challenger, the challenger measures the input or the output register of ρ according to the tossed coin $b \leftarrow \{0,1\}$. In the second phase, $\mathcal{A}_2$ receives the resulting state $\rho_{(b)}$ sent by the challenger and inherited by $\mathcal{A}_1$, and made his decision b'. $\mathcal{A}$ wins the game iff it holds that $b' = b$.

Note that, when the size of preimages is bounded by some polynomial, the trace distance between $\rho_{(0)}$ and $\rho_{(1)}$ is smaller than 1 by a non-negligible amount, which means these two states are not extremely far from each other, therefore we can deduce that the states generated by $\mathcal{A}_2$ with inputs $\rho_{(0)}$ and $\rho_{(1)}$ are similar to each other with non-negligible amount. That gives possibility to restore one from another state by the power of the inverse of $\mathcal{A}_2$.

Inspired by this observation, assuming $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is unitary and breaks the collapsing property of H_n, if we measure the input register of the state ρ generated by the first phases $\mathcal{A}_1$ in the computational basis and get a preimage x of some hash value y, the resulting state $\rho_{(1)}$ should be non-negligibly "close" to $\rho_{(0)}$ (i.e. the state after measuring the output register of ρ). That implies the state $\mathcal{A}_2\rho_{(1)}\mathcal{A}_2^\dagger$ is not too "far" from $\mathcal{A}_2\rho_{(0)}\mathcal{A}_2^\dagger$. Therefore, if we apply $\mathcal{A}_2$ to $\rho_{(1)}$ and measuring the decision register, the resulting state after measuring is similar to the other case with a non-negligible amount. Therefore by applying the inverse $\mathcal{A}_2^\dagger$ to that state, we may "retrieve" the state $\rho_{(0)}$ with a non-negligible advantage. Then another preimage of the hash value y could be derived with non-negligible probability if measuring the input register again. This intuition tells us that when the preimages are bounded by some polynomial, the quantum collision-resistance and the collapsing property must hold simultaneously.

We now describe the procedure of $\mathcal{B}$ as Figure 3. Namely, $\mathcal{B}$ firstly invokes $\mathcal{A}_1, \mathcal{A}_2$ faithfully and measures the input register between these two phases and the decision register after running $\mathcal{A}_2$. Here we denote by x the measurement of the input register in that step. Then $\mathcal{B}$ runs the inverse of $\mathcal{A}_2$ and measures the input register in the computational basis and gets x^* in result. By the discussion above, we claim it holds that $x \neq x^*$ and $H_n(x) = H_n(x^*)$ with non-negligible probability. The formal proof of that result will be exhibited in Section 3.

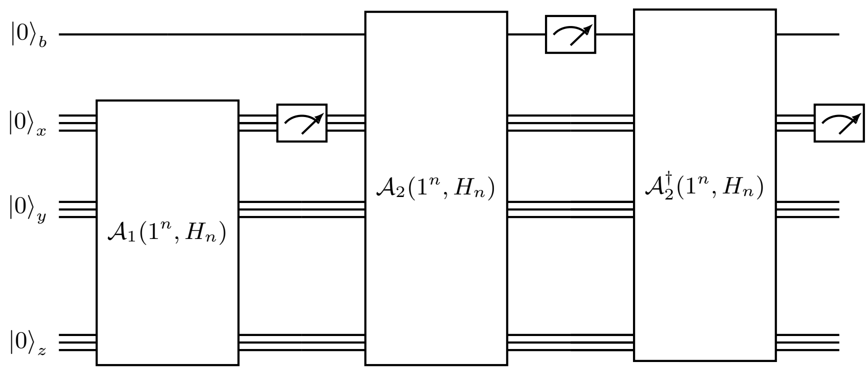

Fig. 3. The description of $\mathcal{B}$.

Note that the adversary $\mathcal{A}$ we considered can be of arbitrary form, it hence could be probably not unitary (and not invertible). That indicates the reduction above would be obstructed if it was treated in a fully black-box manner (in which case both the underlying implementation of the primitive and the adversary $\mathcal{A}$ are only treated as black-box). However, that problem can be circumvented if we consider it in a semi-black-box manner (that is, the underlying implementation of the primitive is still given as a black-box, while the description of the adversary $\mathcal{A}$ is given) [32]. In that case, the inverse of $\mathcal{A}_2$ exists because any general quantum circuit can be simulated by a unitary circuit equivalently (which is called the purification of that circuit, the existence of such simulation may refer to [1]). Therefore, we can assume the whole process of $(\mathcal{A}_1, \mathcal{A}_2)$ is unitary, then the inverse of $\mathcal{A}_2$ is its conjugate transpose $\mathcal{A}_2^\dagger$. That implies the feasibility of the quantum adversary $\mathcal{B}$ for breaking the quantum collision-resistance of H_n.

The relation in almost regular bounded case. The second result aims to study the relation between these two properties in a general case. We believe there might be a quantum collision-resistant hash function that is not collapsing due to the existing oracle-aided constructions [38,4]. However, that doesn't obstruct the reduction from collapsing hash functions to the quantum collision-resistant hash functions.

Therefore we consider whether we can construct polynomial bounded hash functions from unbounded hash functions. Unfortunately, a universal transformation is unknown due to the sophisticated structure of preimages unbounded hash functions. However, we can prove an implication relation for some specific types of hash functions. Namely, when the collection of hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ is almost regular bounded (i.e. almost $O(2^{n-m})$-bounded) and quantum collision-resistant, we can construct a collection of collapsing hash functions from it. The idea is simple, since the collapsing property and the quantum collision-resistance are equivalent in polynomial bounded case, it is sufficient to justify our result by constructing polynomial bounded hash functions from $O(2^{n-m})$-bounded hash functions that preserves the quantum collision-resistance.

To achieve that goal, we adopt the k-wise independent hash functions as our main tool involved in this construction. Note that, for k-wise independent hash functions $\{h : U \to [M]\}$, the probability that the distinct series $x_1, \dots, x_k$ have the same value of h is at most $1/|M|^k$. That inspires us, for any collection of hash functions $\{H_n : \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$, we can rarefy and smooth the preimages by concatenating the hash value $H_n(k,x)$ and the output $h(x)$ of $(\mathtt{poly}(n)+1)$-wise independent hash functions together. Namely, we construct a new collection of hash functions $\{H'_n : \{0,1\}^{l+|h|} \times \{0,1\}^n \to \{0,1\}^{n-1}\}$ such that $H'_n(h\|k, x) := h(x)\|H_n(k,x)$. Then it holds that $H'_n(k', x^*) = H'_n(k', x)$ iff $h(x^*) = h(x) \wedge H_n(k, x^*) = H_n(k,x)$. It is easy to show that the quantum collision-resistance (and hence the collapsing property) can be preserved by this construction. On the other hand, each hash value of $H'_n(h\|k, \cdot)$ has more than $\mathtt{poly}(n)$ preimages with negligible probability due to the property of the $(\mathtt{poly}(n)+1)$-wise independent hash functions, that indicates $H'_n(h\|k,\cdot)$ is $\mathtt{poly}(n)$-bounded with overwhelming probability, which hence proves that $\{H'_n\}$ is almost polynomial bounded quantum collision-resistant hash functions, and the collapsing property can be derived according to our first result.

To show an application of that result, we give a construction of collapsing hash functions from Ajtai's construction $\{H_A(\mathbf{x}) = A\mathbf{x}, A \in \mathbb{Z}_q^{n\times m}\}$ based on the short integer solution (**SIS**) problem by showing $\{H_A\}$ is almost regular bounded for $\mathbf{X} = \{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \le \beta/2\}$ and $\mathbf{Y} = \mathbb{Z}_q^n$. The idea is simple, notice that any vector $\mathbf{x} \in \mathbb{Z}_q^m$ in the input space $\mathbf{X}$ belongs to the sphere $B_{\beta/2}(\mathbf{0})$, we hence give a cell $P(\Lambda_q^\perp(A), \mathbf{x})$ that contains each vector $\mathbf{x} \in \mathbf{X}$ disjointedly and show each cell is contained in a sphere $B_{\beta'/2}(\mathbf{0})$ which is slightly larger than $B_{\beta/2}(\mathbf{0})$. Then we can get an upper bounded of the size of preimages which is the volume of $B_{\beta'/2}(\mathbf{0})$ divided by the volume of the cell. Since the size of $\mathbf{X}$ is approximatively equals to the volume of $B_{\beta/2}(\mathbf{0})$, and $B_{\beta'/2}(\mathbf{0})$ is slightly larger than $B_{\beta/2}(\mathbf{0})$, we can deduce that Ajtai's construction is almost regular bounded. Hence it's feasible to transform it into a collapsing one based on our construction.

1.3 Related Works

Comparation to concurrent work. The concurrent work by Zhandry also discusses the relation between the two security definitions and gets the same equivalence result independently as ours but from different perspectives [44]. He gives a generalized transformation from any quantum collision-resistant hash function that satisfies a certain regularity condition called "semi-regularity" to the collapsing hash functions. Using that transformation, he derives several constructions of collapsing hash functions from different assumptions such as the learning parity with noise (**LPN**) problem, and some problems arising from isogenies on elliptic curves. These results greatly expand known results (since the only standard-model construction of collapsing hash functions before that was based on the learning with error (**LWE**) problem).

From a different perspective, our work mainly aims to figure out the implication relations between the collapsing hash functions and the quantum collision-resistant hash functions in various cases, and we consider the existence of some related primitives such as the equivocal collision-resistant hash functions. As an application, we construct collapsing hash functions from Ajtai's construction based on the quantum hardness of the short integer solution (**SIS**) problem.

The collapsing hash functions. The concept of collapsing hash functions is proposed by Unruh to achieve the post-quantum binding property for commitment scheme [38]. He showed the random function satisfies the collapsing property, and gave an instance of a quantum collision-resistant hash function that is not collapsing relative to a quantum oracle (which is constructed by Ambainis et al. in [3]). Then he gave a concrete construction in his later work [37], which also shows the collapsing is preserved under the Merkle-Damgård construction. Czajkowski et al. proved the Sponge construction also preserves the collapsing property under some suitable assumptions [15] (which is originally in [39]). Fehr proposed a formalism and a framework which could obtain simpler proofs for the collapsing property [17]. The relations of the security notions of cryptographic hash functions against quantum attacks are further studied by Hamlin and Song in [20]. Moreover, Zhandry showed the existence of non-collapsing quantum collision-resistant hash functions implies the quantum lighting in an infinite-often sense. Then Amos et al. proposed the notion of equivocal collision-resistant hash functions, which is collision-resistant but not collapsing, and gave a classical oracle construction, which also yields a classical oracle construction separates the collapsing property and the quantum collision-resistance [4].

The relations of variant hash functions. The relations of security notions of cryptographic hash functions are studied comprehensively in both classical and quantum setting (such as [34,20]). As for the existence in the black-box manner, Hsiao and Reyzin set up a fully black-box barrier from the public-coin collision-resistant hash functions to the secret-coin collision-resistant hash functions by the two-oracle technique [22]. Simon showed the impossibility of (relativized) reduction from the collision-resistant hash functions to one-way permutation [36]. This impossibility is lifted into a quantum fully black-box setting by Hosoyamada and Yamakawa [21], which also rules out the quantum fully black-box reduction from the quantum-computable (classical-computable) collapsing hash functionsto the quantum-computable (classical-computable) one-way permutation. Asharov and Segev showed the non-existence of fully black-box construction of collision-resistant hash functions from indistinguishability obfuscator, which indicates that the collision-resistant hash function doesn't belong to the world Obfustopia [5]. As a weaker notion, the multi-collision resistant hash function was studied in [7,9], which also showed a fully black-box barrier from one-way permutation to that primitive. Inspired by Impagliazzo's five worlds [24], Komargodski et al. defined four worlds of hashing-related primitives in classical setting [26], which are Hashomania, Minihash, Unihash, Nocrypt respectively. Hashomania denotes the world that the collision-resistant hash function exists. Minihash is the world that multiple collision resistant hash exists. Unihash denotes only one-way functions exist, and Nocrypt is the world that has no one-way function. They also showed a fully black-box barrier from the multiple collision resistant hash functions to the collision-resistant hash functions. Then Komargodski et al. studied the distributional collision resistant hash functions [27], which is firstly introduced by [16], they showed the distributional collision-resistan hash functions can be guaranteed by the existence of multi-collision resistance hash in a non-black-box (and infinitely-often) case, and also implied by the the average case hardness of statistical zero-knowledge. Then Bitansky et al. showed that primitive might be stronger than one-way functions by giving a construction of constant-round statistically hiding commitment scheme [8], which seems impossible from one-way function in the fully black-box case [19].

Although there have been a lot of studies about the security notions of hash functions in the classical world. Many relations remain to be unknown in the quantum setting. Therefore, in this paper, we further study the relations of post-quantum security definitions of hash functions theoretically and take the first step to show whether collapsing hash belongs to the quantum analogue of Hashomania.

2 Preliminary

2.1 Notations

We use $\mathbb{N}$ and $\mathbb{R}$ to denote the set of positive integers and real numbers respectively, $\|\rho_1, \rho_1\|_{tr}$ is the trace distance between two mixed states ρ_1, ρ_1, and $\mathrm{Tr}(\rho)$ denotes ρ's trace. The length of a string x is denoted as $|x|$, and when refered to a set X, let $|X|$ be its Cardinality. The mathematical expectation of a random variable H is $\mathrm{E}[H]$. A function $f : \mathbb{N} \to \mathbb{R}$ is called negligible, if for any positive polynomial $p(n)$, it holds $1/p(n) > f(n)$ for all sufficiently large n. It is easy to see that for a non-negligible $f(n)$, there is some positive polynomial $p(\cdot)$ such that $1/p(n) < f(n)$ for infinite many $n \in \mathbb{N}$. For a hash function $H_n : \{0,1\}^n \to \{0,1\}^m$, we let $H_n^{-1}(y)$ denote the set of preimage for any $y \in \{0,1\}^m$, and when $y \notin H_n(\{0,1\}^n)$, let $H_n^{-1}(y) = \emptyset$.

2.2 Quantum Computation

In this part, we introduce some background information on quantum computation, we assume the familiarity with basic notions in [31]. A quantum state is a vector with norm 1 in a Hilbert space, which we usually denote it by $|\phi\rangle$. And in this work, we usually consider that state in binary form, for example

$$|\phi\rangle := \sum_x a_x |x\rangle$$

for $x \in \{0,1\}^n$ and $\sum |a_x|^2 = 1$. The family of pure states $\{|x\rangle\}_{x\in\{0,1\}^n}$ is called the computational basis of that space. The combination of two states $|\phi_1\rangle$, $|\phi_2\rangle$ is the tensor product $|\phi_1\rangle \otimes |\phi_2\rangle$ and we denote by $|\phi_1, \phi_2\rangle$ for simplicity.

A quantum algorithm $\mathcal{A}$ is made up by the composition of a series of basis gates, which can be unitary (such as the Hadamard gates, Toffoli gates, and the CNOT gates), and non-unitary (such as the ancillary gates and the erasure gates). A collection of functions $\{H_n\}$ is called quantum-computable if there exists a family of polynomial-time uniform quantum circuits $\{\mathcal{C}_n\}$ to implement it, and permits the superposition calculation, namely

$$\sum_{x,y} a_{x,y}|x,y\rangle \xrightarrow{\mathcal{C}_n} \sum_{x,y} a_{x,y}|x, y \oplus H_n(x)\rangle$$

for any possible $\sum_{x,y} a_{x,y}|x,y\rangle$ (or we can define it in the bounded-error case, i.e. the distance between $\mathcal{C}_n|x,y\rangle$ and the actual $|x, y \oplus H_n(x)\rangle$ is at least 2/3).

For a general quantum circuit $\mathcal{C}$, the output is denoted by the mixed state $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$ such that $\sum_i p_i = 1$. If $\mathcal{C}$ is polynomial-time quantum circuit, we can simulate it equivalently by some unitary circuits $\mathcal{C}'$ efficiently [1]. We denote by $|\phi\rangle$ the output of $\mathcal{C}'$, then we have

$$\operatorname*{Tr}_z |\phi\rangle\langle\phi| = \rho,$$

where Tr_z is the partial trace respect to some auxiliary registers added in $\mathcal{C}'$. We hence say $|\phi\rangle$ is the *purification* of ρ and $\mathcal{C}'$ is the *purified circuit* of $\mathcal{C}$. And when we measure a state $|\phi\rangle$ (in some basis such as $\{|x\rangle\}_{x\in\{0,1\}^n}$), the probability that we get x in result is $|\langle x|\phi\rangle|^2$ and when measuring a mixed state ρ, the corresponding probability is $\langle x|\rho|x\rangle$.

For a quantum algorithm $\mathcal{A}$, we denote by $[\mathcal{A}(x) \to z]$ the process that it takes the classical information x as its input and output the measurement z, and the corresponding probability is denote as

$$\Pr[\mathcal{A}(x) \to z].$$

When $\mathcal{A}$ is unitary, that probability can be denoted as $\||z\rangle\langle z| \otimes I \circ \mathcal{A}|x, 0\rangle\|^2$, where 0 stores the auxiliary qubits of $\mathcal{A}$, and I is the identity on the rest registers.

2.3 The Quantum Security of Hash Functions

In this part, we will introduce several security definitions of hash functions $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}_{n\in\mathbb{N}}$. We usually assume the hash functions follow the binary form $\{H_n : \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\in\mathbb{N}}$, namely $\mathbf{X} = \{0,1\}^n$, $\mathbf{K} = \{0,1\}^{l(n)}$, and $\mathbf{Y} = \{0,1\}^{m(n)}$. The parameters $l(n)$ and $m(n)$ are bounded by some polynomial of n. They are denoted as l and m in brief when there is no confusion. We will always assume that $\{H_n\}$ is compressing, namely it holds that $n > m$ for all sufficiently large $n \in \mathbb{N}$, and $\{H_n\}$ is keyless if $l(n) = 0$.

The following definition of quantum collision-resistant hash functions is adapted from [21], which provides a classification due to the implementation environment [4].

[4] We will always follow this classification in the following definitions. It's not important to the proof in our result, but we believe it can help us clarify the underlying relations of each primitive with different perspectives.

Definition 1 (Quantum collision-resistant hash function [21]). *A collection of hash functions* $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ *is quantum-computable (or classical-computable) quantum collision-resistant hash functions if there exists a pair of efficient quantum (classical) algorithms* Gen *and* Eval *such that:*

- $\texttt{Gen}(1^n)$: *The key generation algorithm takes the security parameter* 1^n *as its input, and output an evaluation key* $k \in \{0,1\}^l$.
- $\texttt{Eval}(k, x)$ *The evaluation algorithm calculates the hash function* $H_n(k,\cdot)$ *for an evaluation key* $k \in \{0,1\}^l$ *and returns the hash value* $y = H_n(k, x)$.

For any quantum efficient adversary $\mathcal{A}$*, we have*

$$\Pr_{k\leftarrow\texttt{Gen}(1^n)}[\mathcal{A}(1^n, k) \to (x_0, x_1), H_n(k, x_0) = H_n(k, x_0)] \leq \texttt{negl}(n) \tag{2}$$

for any $n \in \mathbb{N}$*. The probability above is taken over the choice of* $k \leftarrow \texttt{Gen}(1^n)$ *and the randomness inside* $\mathcal{A}$*. Where* $\texttt{negl}(\cdot)$ *is a negligible function.*

Next, we introduce the definition of collapsing hash functions, which is originally defined by Unruh [38], here we adapt it slightly to achieve the consistency of this work.

Definition 2 (Collapsing Hash Functions [38]). *A collection of hash functions* $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ *is quantum-computable (classical-computable) collapsing hash functions, if there exists a pair of efficient quantum (classical) algorithms* Gen *and* Eval *as Definition 1, and withstands the attack of any quantum efficient adversary* $\mathcal{A}$ *in the following experiment* $\texttt{Exp}^{coll}_{\mathcal{A}}(n)$*:*

- *The adversary* $\mathcal{A}$ *is divided into two phases* $\mathcal{A}_1$, $\mathcal{A}_2$ *in that experiment.*
- *In the first phase,* $\mathcal{A}_1$ *is given the security parameter* 1^n *along with an evaluation key* $k \leftarrow \texttt{Gen}(1^n)$ *as its input and generates the following state:*

$$|\phi\rangle := \sum_{x,y} \alpha_{x,y,z}|x, y, z\rangle \tag{3}$$

  Where $x \in \{0,1\}^n$ *and* $y \in \{0,1\}^{m(n)}$ *denote the input/output of* $H_n(k,\cdot)$ *respectively and* z *is the auxiliary string. Then* $\mathcal{A}_1$ *sends the registers containing the input/output of* $H_n(k,\cdot)$ *to the challenger.*
- *The challenger randomly chooses a coin* $b \leftarrow \{0,1\}$*. If* $b = 0$*, it would measure the output register of the receiving state in the computational basis; If* $b = 1$*, it would measure the input register.*
- *Then the challenger returns the resulting state to the adversary* $\mathcal{A}_2$*.*
- *After receiving the state from the challenger and inheriting the information from* $\mathcal{A}_1$*. The second phase* $\mathcal{A}_2$ *outputs his decision* $b' \in \{0,1\}$ *and wins iff* $b' = b$*.*

We let $\texttt{Exp}^{coll}_{\mathcal{A}}(n) = 1$ *whenever the adversary* $\mathcal{A}$ *wins and* $\texttt{Exp}^{coll}_{\mathcal{A}}(n) = 0$ *otherwise. Then* $\{H_n\}_{n\in\mathbb{N}}$ *satisfies the collapsing property if*

$$\left|\Pr[\texttt{Exp}^{coll}_{\mathcal{A}}(n) = 1] - \frac{1}{2}\right| \leq \texttt{negl}(n) \tag{4}$$

for any quantum efficient adversary $\mathcal{A}$*, and for all* $n \in \mathbb{N}$*. Where* $\texttt{negl}(\cdot)$ *is a negligible function.*

Since the challenger can check the validity of $|\phi\rangle$ by invoking H_n again in the experiment, without loss of generality, we assume $\mathcal{A}_1$ always returns a valid state, which means the output register stores the correct hash value of the corresponding input.

To construct quantum lightning, one-shot chameleon hashing, and signatures schemes, Amos et al. further explored the quantum security of hash functions and proposed a new notion which is called the equivocal collision-resistant hash functions.

Definition 3 (Equivocal Collision-Resistant Hash Functions [4]). *A collection of hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ is quantum-computable (classical-computable) equivocal collision-resistant hash functions, if there exists a pair of efficient quantum (classical) algorithms* `Gen` *and* `Eval` *as in Definition 1, along with the following two efficient quantum algorithms $\mathcal{G}, \mathcal{E}$:*

- $\mathcal{G}(k)$: *The generation algorithm takes the evaluation key k as its input, and outputs a hash value y of $H_n(k, \cdot)$, a description of a predicate $\mathcal{P} : \{0,1\}^n \to \{0,1\}$, and a state $\rho_{y,\mathcal{P}}$ (which probably includes the information about the evaluation key and the description of $\mathcal{P}$).*
- $\mathcal{E}(b, \rho)$: *The equivocal algorithm takes a bit $b \in \{0,1\}$ along with a state ρ as its input, and outputs a preimage x.*

The correctness stresses that if $\mathcal{P}$, y and $\rho_{y,\mathcal{P}}$ is generated by $\mathcal{G}(k)$, then the output x of $\mathcal{E}(b, \rho_{y,\mathcal{P}})$ satisfies $H_n(k, x) = y$ and $\mathcal{P}(x) = b$ with overwhelming probability for any $b \in \{0,1\}$. And the security of $\{H_n\}$ also requires quantum collision-resistance against any quantum efficient adversary $\mathcal{A}$.

Notice that here we only consider the quantum implementations of $\mathcal{G}, \mathcal{E}$ in above definition. Since if they are classical, we can apparently get a collision by repeating $\mathcal{E}(b, \rho)$ with a copied ρ (if $\mathcal{G}$ is classical, the output of $\mathcal{G}$ should be classical as well). Moreover, we can see that the quantum collision-resistance is implied by the equivocal collision-resistance, and the equivocality also rules out the collapsing property, which is shown by the following lemma.

Lemma 1. *If $\{H_n\}$ is a collection of quantum-computable (classical-computable) equivocal collision-resistant hash functions, then it is not collapsing.*

That result was claimed originally by Amos et al. in [4] (Sec. 2) without an explicit proof. We will give a detailed proof for Lemma 1 via a non-black-box manner in Appendix A for completeness.

Then we derive the following definitions of (almost) $\delta(n)$-bounded (and regular bounded) to classify the hash functions by the size of preimages.

Definition 4 ($\delta(n)$-bounded). *A collection of hash functions $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}$ is $\delta(n)$-bounded if*

$$|\{x \mid H_n(k, x) = y\}| \leq \delta(n) \tag{5}$$

for all $n \in \mathbb{N}$, $k \in \text{supp}(\texttt{Gen}(1^n))$, and $y \in \{0,1\}^m$. Where $\text{supp}(\texttt{Gen}(1^n)) \subseteq \mathbf{K}$ denotes the support of the distribution of key generation algorithm $\texttt{Gen}(1^n)$. In addition, $\{H_n\}$ is almost $\delta(n)$-bounded if

$$\Pr_{k \leftarrow \texttt{Gen}(1^n)}[|\{x \mid H_n(k, x) = y\}| \leq \delta(n)] \geq 1 - \texttt{negl}(n) \tag{6}$$

for all $n \in \mathbb{N}$, and $y \in \mathbf{Y}$, where $\texttt{negl}(\cdot)$ denotes a negligible function.

Besides, $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}$ is called *regular bounded* if $\delta(n) = O(|\mathbf{X}|/|\mathbf{Y}|)$, which means the preimages could not be too large to the expected value. We say a collection of hash functions $\{H_n\}$ is *polynomial bounded*, if there exists a positive polynomial $\mathtt{poly}(\cdot)$ such that $\{H_n\}$ is $\mathtt{poly}(n)$-bounded. And the notions of *almost regular bounded* and *almost polynomial bounded* are defined accordingly.

In the following part, we will classify the hash functions by this notion and start our result in a polynomial bounded setting.

A function H_n is called *regular*, if all hash values have the same size of preimages (except the empty set). Base on that notion, Ristenpart and Shrimpton further proposed the definition of regularity [33], which is also highly relative to the almost regular bounded property. Here we adapt that notion to fit our content as follows.

Definition 5 (Regularity [33]). *A collection of hash functions $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}$ is $\Delta(n)$-regular if it holds that*

$$\sum_k \Pr[k = k' : \mathtt{Gen}(1^n) \to k'] \cdot \Delta(k, n) \leq \Delta(n),$$

where $\Delta(k, n)$ is given by

$$\Delta(k, n) := \max_y \frac{\big||\{x \mid H_n(k, x) = y\}| - |\mathbf{X}|/|\mathbf{Y}|\big|}{|\mathbf{X}|}.$$

In addition, we say $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}$ is nearly regular if $\Delta(n) \leq O(\frac{|\mathbf{X}|}{|\mathbf{Y}| \cdot n^{\omega(1)}})$.

Notice there are other definitions characterizing the regularity of hash functions such as [28], they also defined the *almost regularity*, we hence denote our notion by "nearly regular" instead of "almost regular" to avoid the potential confusion. It's easy to see that any regular hash function satisfies the nearly regular property, and by Markov's inequality, nearly regular hash function is almost regular bounded.

As a basic tool that will used in the second part of our result, we introduce the notion from k-wise independent hash functions, which is generalized by the universal hash functions.

Definition 6 (k-Wise Independent Hash Functions). *A family of hash functions $\{h : U \to [M]\}$ is called k-wise independent if for any k distinct inputs $x_1, \ldots x_k$ along with k outputs $y_1, \ldots, y_k$ (probably not distinct), it holds that*

$$\Pr_h[\wedge_{i=1}^k h(x_i) = y_i] \leq \frac{1}{M^k}. \tag{7}$$

That notion has plenty of applications in cryptography in both quantum and classical setting such as [35,14,41,11,37,10]. It can be implemented efficiently due to many concrete constructions such as [13,40].

3 The Equivalence in Polynomial Bounded Case

In this section, we will show the equivalence of the quantum collision-resistance and the collapsing property, when the preimages of each hash value are upper bounded by some polynomial of the input length. It is formalized as follows.

Theorem 3. *A collection of quantum-computable (classical-computable) polynomial bounded hash functions is collapsing if and only if it is quantum collision-resistant.*

Proof. By the definition of collapsing hash functions, it's trivial to obtain the collision-resistance from collapsing property for any quantum-computable (classical-computable) $\texttt{poly}(n)$-bounded hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$, where $\texttt{poly}(\cdot)$ is a positive polynomial. Hence it's sufficient to prove it on the other direction.

Since the evaluation key is not involved in this proof, without loss of generality, we consider this problem in the keyless setting (i.e. the collection of hash functions is denote by $\{H_n : \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$) for convenience, and the generalized result can be derived accordingly. We justify that result by making a contradiction. Assuming there exists a collection of quantum-computable (classical-computable) $\texttt{poly}(n)$-bounded hash functions $\{H_n : \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ for some positive polynomial $\texttt{poly}(\cdot)$ which is quantum collision-resistant but not collapsing, and $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is the corresponding quantum adversary that breaks the collapsing property of H_n. We now take advantage of $\mathcal{A}$ to construct a quantum collision-finding algorithm $\mathcal{B}$ as follows:

- $\mathcal{B}$ firstly invokes $\mathcal{A}_1(1^n)$ and produces the state ρ_1.
- $\mathcal{B}$ measures the input register of ρ_1 in the computational basis, and gets a measurement $x \in \{0,1\}^n$ with the resulting state ρ_2.
- Then $\mathcal{B}$ runs $\mathcal{A}_2$ on ρ_2 and measures the decision qubit b', and ρ_3 is the collapsed resulting state after measuring.
- $\mathcal{B}$ runs the inverse $\mathcal{A}_2^\dagger$ to ρ_3 and measures the input register in the computational basis, and gets the measurement x^*. Then outputs the pair (x, x^*) as its result.

First of all, we will justify the feasibility of $\mathcal{B}$. We consider that $\mathcal{B}$ is given the internal information of $\mathcal{A}_1, \mathcal{A}_2$ (which is stronger than only given the oracle access), in that case, we can assume both $\mathcal{A}_1, \mathcal{A}_2$ are unitary operations without loss of generality. Since if not, we can certainly replace them by their purified circuits. These processes are efficient as justified in [1]. Since $\mathcal{A}$ is an efficient quantum adversary, hence $\mathcal{B}$ is also an efficient quantum algorithm. The remaining part of this proof is to show that $\mathcal{B}$ breaks the collision-resistance of H_n with non-negligible probability, namely, the existence of some positive polynomial $\texttt{P}'(n)$ such that

$$\Pr[\mathcal{B}(1^n) \to (x, x^*), H_n(x) = H_n(x^*)] \geq \frac{1}{\texttt{P}'(n)} \tag{8}$$

for infinitely many $n \in \mathbb{N}$. Where $\texttt{P}'(n)$ is some positive polynomial.

Before showing that, we give some notations which are useful in the proof. Firstly, the procedure of $\mathcal{A}_1$ is expressed as follows:

$$\mathcal{A}_1|0\rangle = \sum_{x,y,z} \alpha_{x,y,z}|x, y, z\rangle. \tag{9}$$

Where x, y are stored in the input/ output registers respectively, and z is the corresponding auxiliary string. Without loss of generality, we assume $\mathcal{A}_1$ always produces valid state, namely it holds that $y = H_n(x)$ in equation (9) (since if not, we can check the validity of that state by invoking $H_n(\cdot)$ and refuse the noisy part). The second phase $\mathcal{A}_2$ runs on $|0, x, y, z\rangle$ as follows

$$A_2|0, x, y, z\rangle = \sum_{b',x',y',z'} \beta^{x,y,z}_{b',x',y',z'}|b', x', y', z'\rangle. \tag{10}$$

Where b' stores the decision bit of $\mathcal{A}_2$.

By our assumption, since $\mathcal{A}$ wins in $\mathtt{Exp}_{\mathcal{A}}^{coll}(n)$ with non-negligible advantage under our assumption, there exists a positive polynomial $\mathtt{P}(\cdot)$ such that

$$\left|\Pr[\mathtt{Exp}_{\mathcal{A}}^{coll}(n) = 1] - \frac{1}{2}\right| \geq \frac{1}{\mathtt{P}(n)}, \tag{11}$$

for infinitely many $n \in \mathbb{N}$.

Let $\rho_{(0)}$ denote the mixed state after measuring (tracing out) the output register of ρ_1 (i.e. $b = 0$), by the equation (9), it can be denoted as

$$\rho_{(0)} := \sum_y \Big(\sum_{x,z}^{x \in H_n^{-1}(y)} |\alpha_{x,y,z}|^2 \Big) \cdot |\phi_y\rangle\langle\phi_y|.$$

Where $|\phi_y\rangle := \sum_{x,z}^{x \in H_n^{-1}(y)} \alpha_{x,y,z}|x,y,z\rangle / \sqrt{(\sum_{x,z}|\alpha_{x,y,z}|^2)}$, and $\rho_{(1)}$ be the state in the case $b = 1$, which is

$$\rho_{(1)} := \sum_y \sum_x^{x \in H_n^{-1}(y)} \Big(\sum_z |\alpha_{x,y,z}|^2\Big) |\psi_{x,y}\rangle\langle\psi_{x,y}|.$$

Where $|\psi_{x,y}\rangle = \sum_z \alpha_{x,y,z}|x,y,z\rangle / \sqrt{(\sum_z |\alpha_{x,y,z}|^2)}$. Recall that

$$A_2|0,x,y,z\rangle = \sum_{b',x',y',z'} \beta_{b',x',y',z'}^{x,y,z} |b',x',y',z'\rangle.$$

Let $\mathbf{E}_{b,b'}$ be the event that the measurement of decision bit is b' after invoking the $\mathcal{A}_2$ on $|0\rangle\langle 0| \otimes \rho_{(b)}$, then we can denote the probability that $\mathbf{E}_{b,b'}$ occurs as

$$\Pr[\mathbf{E}_{0,b'}] = \sum_y \sum_{x',y',z'} \Big| \sum_{x,z}^{x \in H_n^{-1}(y)} \beta_{b',x',y',z'}^{x,y,z} \alpha_{x,y,z} \Big|^2 \tag{12}$$

for $b = 0$, and

$$\Pr[\mathbf{E}_{1,b'}] = \sum_y \sum_x^{x \in H_n^{-1}(y)} \sum_{x',y',z'} \Big| \sum_z \beta_{b',x',y',z'}^{x,y,z} \alpha_{x,y,z} \Big|^2 \tag{13}$$

for $b = 1$.

Thus the success probability of $\mathcal{A}$ satisfies

$$\begin{aligned}
&4 \cdot \left|\Pr[\mathtt{Exp}_{\mathcal{A}}^{coll}(n) = 1] - \frac{1}{2}\right| \qquad (14)\\
&= \sum_{b'} \Big| \Pr[\mathbf{E}_{0,b'}] - \Pr[\mathbf{E}_{1,b'}] \Big| \\
&= \sum_{b'} \Big| \sum_{y,x',y',z'} \Big[\Big| \sum_{x,z}^{x \in H_n^{-1}(y)} \beta_{b',x',y',z'}^{x,y,z} \alpha_{x,y,z} \Big|^2 - \sum_{x \in H_n^{-1}(y)} \Big| \sum_z \beta_{b',x',y',z'}^{x,y,z} \alpha_{x,y,z} \Big|^2 \Big] \Big| \\
&= \sum_{b'} \Big| \sum_{x,y,x',y',z'}^{x \in H_n^{-1}(y)} \sum_{x^* \in H_n^{-1}(y)}^{x \neq x^*} \mathrm{Re}\Big(\big(\sum_z \beta_{b',x',y',z'}^{x,y,z} \alpha_{x,y,z}\big) \cdot \big(\sum_z \beta_{b',x',y',z'}^{x^*,y,z} \alpha_{x^*,y,z}\big) \Big) \Big|.
\end{aligned}$$

Where $\mathrm{Re}(a)$ denotes the real part of a (Here the situations that $x = x_0 \wedge x^* = x_1$ and $x = x_1 \wedge x^* = x_0$ are counted as two cases, that's the reason there is no coefficient 2 in the last equation of (14)).

Since we assume that $\mathcal{A}$ breaks the collapsing property of H_n with advantage $1/\mathtt{P}(n)$, from equation (14), we can deduce that

$$\sum_{b'} \Big| \sum_{x,y,x',y',z'}^{x \in H_n^{-1}(y)} \sum_{x^* \in H_n^{-1}(y)}^{x \neq x^*} \mathrm{Re}\Big(\big(\sum_z \beta^{x,y,z}_{b',x',y',z'} \alpha_{x,y,z} \big) \cdot \big(\sum_z \beta^{x^*,y,z}_{b',x',y',z'} \alpha_{x^*,y,z} \big) \Big) \Big| \geq \frac{4}{\mathtt{P}(n)} \tag{15}$$

for infinitely many $n \in \mathbb{N}$.

We now estimate the probability that $\mathcal{B}$ successfully finds a collision. Since we denote by ρ_2 the state that $\mathcal{B}$ just measures the input register of the state produced by $\mathcal{A}_1(1^n)$, we have

$$\rho_2 = \rho_{(1)} = \sum_y \sum_x^{x \in H_n^{-1}(y)} (\sum_z |\alpha_{x,y,z}|^2) |\psi_{x,y}\rangle\langle\psi_{x,y}|. \tag{16}$$

Therefore $\mathcal{A}_2(|0\rangle\langle 0| \otimes \rho_2)\mathcal{A}_2^\dagger$ is denoted as

$$\begin{aligned} &\sum_y \sum_x^{x \in H_n^{-1}(y)} (\sum_z |\alpha_{x,y,z}|^2) \mathcal{A}_2 |0, \psi_{x,y}\rangle\langle 0, \psi_{x,y}| \mathcal{A}_2^\dagger \\ &= \sum_y \sum_x^{x \in H_n^{-1}(y)} \big(\sum_{z,b',x',y',z'} \alpha_{x,y,z} \beta^{x,y,z}_{b',x',y',z'} |b', x', y', z'\rangle \big) \\ &\qquad \cdot \big(\sum_{z,b',x',y',z'} \bar{\alpha}_{x,y,z} \bar{\beta}^{x,y,z}_{b',x',y',z'} \langle b', x', y', z'| \big). \end{aligned}$$

Then ρ_3 can be denoted as

$$\begin{aligned} &\sum_y \sum_x^{x \in H_n^{-1}(y)} \sum_{b'} \big(\sum_{z,x',y',z'} \alpha_{x,y,z} \beta^{x,y,z}_{b',x',y',z'} |b', x', y', z'\rangle \big) \\ &\qquad \cdot \big(\sum_{z,x',y',z'} \bar{\alpha}_{x,y,z} \bar{\beta}^{x,y,z}_{b',x',y',z'} \langle b', x', y', z'| \big). \end{aligned}$$

The finial state before measuring is $\mathcal{A}_2^\dagger \rho_3 \mathcal{A}_2$, which can be denoted as follows

$$\begin{aligned} &\sum_y \sum_x^{x \in H_n^{-1}(y)} \sum_{b'} \big(\sum_{z,x',y',z'} \alpha_{x,y,z} \beta^{x,y,z}_{b',x',y',z'} \mathcal{A}_2^\dagger |b', x', y', z'\rangle \big) \\ &\qquad \cdot \big(\sum_{z,x',y',z'} \bar{\alpha}_{x,y,z} \bar{\beta}^{x,y,z}_{b',x',y',z'} \langle b', x', y', z'| \mathcal{A}_2 \big). \end{aligned}$$

To estimate the probability that the measurement of $\mathcal{A}_2^\dagger \rho_3 \mathcal{A}_2$ equals $|0, x^*, y, z^*\rangle$. Note that, for any $|0, x^*, y, z^*\rangle$, we have

$$\begin{aligned}
&\langle 0, x^*, y, z^*|(\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\mathcal{A}_2^\dagger|b', x', y', z'\rangle) \\
&\qquad\qquad \cdot (\sum_{z,x',y',z'} \bar{\alpha}_{x,y,z}\bar{\beta}^{x,y,z}_{b',x',y',z'}\langle b', x', y', z'|\mathcal{A}_2)|0, x^*, y, z^*\rangle \\
&= |(\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\langle 0, x^*, y, z^*|\mathcal{A}_2^\dagger|b', x', y', z'\rangle)|^2 \\
&= |(\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}(\sum_{b',x',y',z'} \bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}\langle b', x', y', z'|)|b', x', y', z'\rangle)|^2 \\
&= |\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}|^2
\end{aligned}$$

Therefore the probability that $\mathcal{B}$ finds a collision x, x^* is at least

$$\begin{aligned}
&\Pr[\mathcal{B}(1^n) \to (x, x^*), H_n(x) = H_n(x^*)] \qquad (17)\\
&\geq \sum_{x,y,b'}^{x \in H_n^{-1}(y)} \sum_{z^*,x^* \in H_n^{-1}(y)}^{x^* \neq x} \langle 0, x^*, y, z^*|(\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\mathcal{A}_2^\dagger|b', x', y', z'\rangle) \\
&\qquad\qquad \cdot (\sum_{z,x',y',z'} \bar{\alpha}_{x,y,z}\bar{\beta}^{x,y,z}_{b',x',y',z'}\langle b', x', y', z'|\mathcal{A}_2)|0, x^*, y, z^*\rangle \\
&= \sum_{x,y,b'}^{x \in H_n^{-1}(y)} \sum_{z^*,x^* \in H_n^{-1}(y)}^{x^* \neq x} |\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}|^2.
\end{aligned}$$

Since H_n is $\texttt{poly}(n)$-bounded, and $\sum_{x,y,z} |\alpha_{x,y,z}|^2 = 1$, it holds that

$$\sum_{x,y}^{x \in H_n^{-1}(y)} \sum_{z^*,x^* \in H_n^{-1}(y)}^{x^* \neq x} \sigma(x, y) \cdot |\bar{\alpha}_{x^*,y,z^*}|^2 \leq \texttt{poly}(n), \qquad (18)$$

According to the inequality (18) and

$$|\sum_{i=1}^{k} a_i b_i|^2 \leq (\sum_{i=1}^{k} |a_i|^2) \cdot (\sum_{i=1}^{k} |b_i|^2),$$

we can hence further deduce that

$$\sum_{x,y}^{x\in H_n^{-1}(y)} \sum_{z^*,x^*\in H_n^{-1}(y)}^{x^*\neq x} |(\sum_{z,x',y',z'} \alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}|^2 \tag{19}$$

$$\geq \Big(\sum_{x,y}^{x\in H_n^{-1}(y)} \sum_{z^*,x^*\in H_n^{-1}(y)}^{x^*\neq x} \Big| \sum_{z,x',y',z'} \bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}\alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\Big|^2\Big)$$

$$\cdot \Big(\sum_{x,y}^{x\in H_n^{-1}(y)} \sum_{z^*,x^*\in H_n^{-1}(y)}^{x^*\neq x} |\bar{\alpha}_{x^*,y,z^*}|^2 \Big)/\mathtt{poly}(n)$$

$$\geq \Big| \sum_{x,y}^{x\in H_n^{-1}(y)} \sum_{z^*,x^*\in H_n^{-1}(y)}^{x^*\neq x} \Big(\sum_{z,x',y',z'} \bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}\bar{\alpha}_{x^*,y,z^*}\alpha_{x,y,z}\beta^{x,y,z}_{b',x',y',z'}\Big)\Big|^2/\mathtt{poly}(n),$$

for both $b' = 0, 1$.

Combining the inequalities (17), (19) with (15), we can derive the probability that $\mathcal{B}$ finds a collision satisfies

$$\Pr[\mathcal{B}(1^n) \to (x, x^*), H_n(x) = H_n(x^*)]$$

$$\geq \sum_{b'} \Big| \sum_{x,y} \sum_{z^*,x^*\in H_n^{-1}(y)}^{x^*\neq x} \Big(\sum_{z,x',y',z'} \bar{\beta}^{x^*,y,z^*}_{b',x',y',z'}\bar{\alpha}_{0,x^*,y,z^*}\alpha_{0,x,y,z}\beta^{x,y,z}_{b',x',y',z'}\Big)\Big|^2/\mathtt{poly}(n)$$

$$\geq \frac{8}{\mathtt{p}(n)^2 \cdot \mathtt{poly}(n)}$$

for infinitely many $n \in \mathbb{N}$, which implies immediately that $\{H_n\}$ is not a collection of quantum-computable (classical-computable) collision-resistant hash functions. That hence completes the proof of Theorem 3. □

Notice that Theorem 3 is proved in the semi-black-box manner [32], that is because the inverse of the second phase of adversary $\mathcal{A}_2$ is usually inaccessible via the fully black-box reduction (because $\mathcal{A}_2$ could be probably non-unitary in general case).

Since the correctness of this proof is irrelevant to the evaluation key, that method can also be adapted slightly to fit the equivalence of the general hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$. Moreover, we can further generalize the Theorem 3 into the almost bounded case, which is the following corollary.

Corollary 3. *A collection of quantum-computable (classical-computable) almost polynomial bounded hash functions is collapsing if and only if it is quantum collision-resistant.*

The proof is very similar to the proof of Theorem 3 (the only difference is that we should ignore the unbounded part of k, whose ratio is at most negligible large), which is omitted here.

Theorem 3 indicates that the quantum collision-resistance and the collapsing property must be satisfied simultaneously for any polynomial bounded hash functions, since classical-computable (quantum-computable) equivocal collision-resistance hash functions can not satisfy the collapsing property due to Lemma 1, as a corollary, we can also show the non-existence of equivocal collision-resistant polynomial bounded hash functions as follows.

Corollary 4. *There doesn't exist almost polynomial bounded equivocal collision-resistant hash functions.*

The corollary above sheds light on how to circumvent a morass for constructing the equivocal collision-resistant hash functions. That is, the preimages shouldn't be too small for each hash value. Besides, our result also partially answers the open problem raised by Amos et al. in [4], which shows that the collapsing hash functions can be implied by the unequivocal hash function in polynomial bounded case.

Besides, since any collection of polynomial bounded quantum collision-resistant hash functions must satisfies the collapsing property simultaneously, we can further deduce that, for any construction that preserves the collision-resistance and the collapsing property such as the Sponge construction and the Merkle-Damgård construction [37,15,42], it's sufficient to guarantee the collapsing property if the underlying block functions are polynomial bounded and quantum collision-resistant.

4 The Implication in Regular bounded Case

In this section, we consider the case that the preimages are exponentially large. Firstly, we give a construction to show how to transform the almost regular bounded quantum collision-resistant hash functions to a collapsing one. Then, as an application, we show Ajtai's construction could meet the requirement of that almost regular bounded property, which hence implies a construction of collapsing hash functions based on the quantum hardness of short integer solution (**SIS**) problem.

4.1 A Construction of Collapsing Hash Functions

For a collection of (compressing) hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ with efficient quantum (classical) algorithms $\texttt{Gen}$ and $\texttt{Eval}$, we consider the following way to rarefy and smooth the preimages by extending the output size.

Firstly, we assume it holds that $n+1 > m(n)$ for all n, since if not, we have many way to extent that gap when $n+1 = m(n)$ such as using some iterations or just omitting one random bit of the output string (and let the information of that position be the additional key of the new hash). Then we construct the new hash functions $\{H'_n : \{0,1\}^{l+|h|} \times \{0,1\}^n \to \{0,1\}^{n-1}\}_{n\in\mathbb{N}}$, with the corresponding algorithms $\texttt{Gen}'$, $\texttt{Eval}$ which perform as follows:

- $\texttt{Gen}'(1^n)$: The key generation algorithm takes the security parameter 1^n as its input, and generates a $(\texttt{poly}(n)+1)$-wise independent hash function $h : \{0,1\}^n \to \{0,1\}^{n-m-1}$, where we denote by h it's description and the length is $|h|$. Then it invokes $k \leftarrow \texttt{Gen}(1^n)$ and returns $k' = h\|k$ as its output.
- $\texttt{Eval}'(k,x)$: The evaluation algorithm takes the evaluation key $k' = h\|k$ and $x \in \{0,1\}^n$ as its input, it firstly calculates $t := h(x)$, then invokes the evaluation algorithm of $H_n(k,\cdot)$ and gets $y = \texttt{Eval}(k,x)$. It would return $y' := t\|y$ as its output.

It is easy to show that $\{H'_n : \{0,1\}^{l+|h|} \times \{0,1\}^n \to \{0,1\}^{n-1}\}$ is quantum collision-resistant if $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ is. From the following lemma by Unruh, we can further deduce the similar preservation of the collapsing property for that construction.

Lemma 2 ([15]). *If $G_k \circ H_n(k,\cdot)$ is collapsing, and G_k is quantum polynomial-time computable, then $H_n(k,\cdot)$ is collapsing.*

If $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ is collapsing, and G_k is the operation that omits the first $n-m-1$ bits of its input, we have $G_k \circ H'_n(k',\cdot) = H_n(k,\cdot)$. That implies H'_n is also collapsing due to the Lemma 2. Then by such construction, we further derive the implication from the almost polynomial bounded collision-resistant hash functions to the almost regular bounded collapsing hash functions which is formed as the following theorem.

Theorem 4. *The existence of the quantum-computable (classical-computable) almost polynomial bounded collapsing hash functions is implied by the existence of the quantum-computable (classical-computable) almost regular bounded collision-resistant hash functions.*

Proof. To prove that theorem, according to the result in polynomial bounded case (i.e. Theorem 3), it is sufficient to give a construction from the almost regular bounded (i.e. almost $O(2^{n-m})$-bounded in that case) quantum collision-resistant hash functions $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ to almost $\mathtt{poly}(n)$-bounded quantum collision-resistant hash functions for some positive polynomial $\mathtt{poly}(\cdot)$. We hence prove that the construction of $\{H'_n\}$ at the beginning of the Section 4 could meet that satisfactory.

It is easy to derive that the quantum collision-resistance is preserved in the construction above. More specifically, $\{H'_n : \{0,1\}^{l+n} \times \{0,1\}^n \to \{0,1\}^{n-1}\}_{n\in\mathbb{N}}$ is a collection of quantum-computable (classical-computable) collision-resistant hash functions if $\{H_n : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$ is quantum-computable (classical-computable) collision-resistant. If not, there should exist an adversary $\mathcal{A}$ finding a collision x, x^* for H'_n with non-negligible probability. Since $H'_n(k',x^*) = H'_n(k',x)$ if and only if $h(x^*) = h(x)$ and $H_n(k,x^*) = H_n(k,x)$ hold simultaneously, therefore (x,x^*) is also a collision of $H_n(k,\cdot)$. Since the collection of functions $\{H'_n\}$ is constructed from $\{H_n\}$ efficiently, that means $\{H_n\}$ is not quantum collision-resistant either, which is obviously contradictory to our assumption.

Therefore to prove the theorem, it's sufficient to estimate the number of preimages of $H'_n(k',\cdot)$. Since $h : \{0,1\}^n \to \{0,1\}^{n-m-1}$ is a $(\mathtt{poly}(n)+1)$-wise independent hash function, we hence have

$$\Pr_h[h(x_1) = h(x_2) = \ldots = h(x_{\mathtt{poly}(n)+1})] \le (\frac{1}{2^{n-m-1}})^{\mathtt{poly}(n)+1} \tag{20}$$

for any distinct $x_1, \ldots x_{\mathtt{poly}(n)+1}$, where the probability is taken over the generation of the function h.

Recall that $H'_n(k',x^*) = H'_n(k',x)$ if and only if $h(x^*) = h(x)$ and $H_n(k,x^*) = H_n(k,x)$. We denote by **Bad** the event that $H'_n(k',\cdot)$ is not $\mathtt{poly}(n)$-bounded and $\mathbf{Bad}_y$ the event that y's preimages of $H'_n(k',\cdot)$ are not bounded by $\mathtt{poly}(n)$ for some specific $y \in \{0,1\}^{n-1}$, and $\mathbf{Good}_k$ denote $H_n(k,\cdot)$ is $O(2^{n-m})$-bounded for $k \in \{0,1\}^l$. For any $y \in \{0,1\}^{n-1}$, we denote by y_1 and y_2 the first $n-m-1$ bits and the last m bits of y respectively. Then, it holds that

$$\begin{aligned}\Pr_{k,h}[\mathbf{Bad}] &= \Pr_{k,h}\big[\bigvee_y \mathbf{Bad}_y\big] \leq \sum_y \Pr_{k,h}\left[\mathbf{Bad}_y\right] \quad (21)\\ &\leq \sum_y \Pr_{k,h}\Big[\big|\{x \mid H_n(k,x) = y_1 \wedge h(x) = y_2\}\big| > \mathtt{poly}(n)\Big]\\ &\leq \sum_y \Pr_{k,h}\Big[\big|\{x \mid H_n(k,x) = y_1 \wedge h(x) = y_2\}\big| > \mathtt{poly}(n) \mid \mathbf{Good}_k\Big] + \Pr_{k,h}[\neg\mathbf{Good}_k]\\ &\overset{*}{\leq} \sum_y (\frac{1}{2^{n-m-1}})^{\mathtt{poly}(n)+1} \cdot \frac{(C \cdot 2^{n-m}) \cdot \ldots \cdot (C \cdot 2^{n-m} - \mathtt{poly}(n))}{(\mathtt{poly}(n)+1)!} + \mathtt{negl}(n)\\ &\leq \frac{(2 \cdot C)^{\mathtt{poly}(n)+1} \cdot 2^{n-1}}{(\mathtt{poly}(n)+1)!} + \mathtt{negl}(n)\end{aligned}$$

which is also negligible for $n \in \mathbb{N}$, where $(*)$ follows from the definition of almost $O(2^{n-m})$-bounded hash functions and the property of $(\mathtt{poly}(n)+1)$-wise independent hash functions, $C > 0$ is a constant.

That implies, for any $O(2^{n-m})$-bounded $H_n(k,\cdot)$, the probability that the new hash $H'_n(h\|k,\cdot)$ is $\mathtt{poly}(n)$-bounded with overwhelming probability over the generation of h. Combining with the fact that $\{H_n\}'$ preserves the quantum collision-resistance, and the efficiency of k-wise independent hash functions, we can deduce that $\{H'_n\}$ is a collection of quantum-computable (classical-computable) almost $\mathtt{poly}(n)$-bounded collision-resistant hash functions if $\{H_n\}$ is quantum-computable (classical-computable) almost $O(2^{n-m})$-bounded (i.e. almost regular bounded) collision-resistant. That hence completes the proof of Theorem 4. □

Since any collection of nearly regular hash functions is almost regular bounded, therefore based on the Theorem 4, we obtain the implication from any nearly regular quantum collision-resistant hash functions as well.

Corollary 5. *The existence of the quantum-computable (classical-computable) almost polynomial bounded collapsing hash functions is implied by the existence of the quantum-computable (classical-computable) nearly regular collision-resistant hash functions.*

These results indicate the collapsing property is not inherently "stronger" than the quantum collision-resistance in many cases, which gives evidence to show that collapsing hash functions might not be a "higher leveled" quantum cryptographic primitive than quantum collision-resistant hash functions.

Remark 1. Notice that the form of the input/output space doesn't affect the correctness of the proof of Theorem 4. Therefore, by the same method, we can generalize result of Theorem 4 to any almost $O(|\mathbf{X}|/|\mathbf{Y}|)$-bounded hash functions $\{H_n : \mathbf{K} \times \mathbf{X} \to \mathbf{Y}\}$.

4.2 Application to Ajtai's Construction

As an application, we will show how to transform Ajtai's construction into a collapsing one assuming the quantum hardness of short integer solution problem.

Firstly, we introduce the short integer solution problem $\mathbf{SIS}_{n,m,q,\beta}$ as follows:

Definition 7 (Short Integer Solution Problem). *Let $A \in \mathbb{Z}_q^{n\times m}$ be a matrix which is chosen uniformly at random, the Short Integer Solution problem $\mathbf{SIS}_{n,m,q,\beta}$ is to find a nonzero vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that $A\mathbf{x} = \mathbf{0}$ and $\|\mathbf{x}\| \leq \beta$.*

Since we can trivially derive a solution of $A\mathbf{x} = \mathbf{0}$ when the parameters are chosen inappropriately (for example $\beta > q$). Therefore to guarantee it to be as hard as certain worst-case lattice problems [30], the hardness of $\mathbf{SIS}_{n,m,q,\beta}$ usually requires that $\beta \geq \sqrt{n\log q}$, $m \geq n\log q$ and $q \geq \beta\cdot\omega(\sqrt{n\log n})$. Then we introduce Ajtai's construction of a family of hash functions $\{H_A\}$ as follows [2,18]:

- $\texttt{Gen}(1^n)$: The key generation algorithm outputs a matrix $A \in \mathbb{Z}_q^{n\times m}$ uniformly at random as the evaluation key.
- $\texttt{Eval}(k, x)$: The evaluation algorithm takes a matrix $A \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^m$ as its input, and outputs $\mathbf{y} := H_A(\mathbf{x}) = A\mathbf{x} \bmod q$.

When the input space of $\{H_A\}$ belongs to the sphere $B_{\beta/2}(\mathbf{0}) := \{\mathbf{x} \mid \|x\| \leq \beta/2\}$, then it's not hard to see the quantum collision-resistance of Ajtai's construction assuming the quantum hardness of Short Integer Solution problem $\mathbf{SIS}_{n,m,q,\beta}$. Therefore, to adopt our construction, it's sufficient to prove that $\{H_A\}$ is almost $O(|B_{\beta/2}(\mathbf{0})|/q^n)$-bounded.

Theorem 5. *Assuming $\beta \geq m^3$, $m \geq n\log q$, and $q \geq \beta\cdot\omega(\sqrt{n\log n})$, then we have*

$$\Pr_A[\max_{\mathbf{y}} |\{\mathbf{x} \mid \|\mathbf{x}\| \leq \frac{\beta}{2} \wedge A\mathbf{x} = \mathbf{y} \bmod q\}| \leq O(\frac{\mathrm{vol}(B_{\beta/2}(\mathbf{0}))}{q^n})] \geq 1 - \frac{1}{2^m} - \frac{1}{q^{m-n}},$$

where the probability is taken over the randomness of $A \leftarrow \mathbb{Z}_q^{n\times m}$, and $\mathrm{vol}(B_{\beta/2}(\mathbf{0}))$ denotes the volume of sphere $B_{\beta/2}(\mathbf{0})$.

Proof. To prove that proposition, we will firstly estimate the size of preimages of $\mathbf{0} \in \mathbb{Z}_q^n$. Notice that $\det(\Lambda_q^{\perp}(A)) = q^n$ (or $\dim(\Lambda_q^{\perp}(A)) = m - n$) with probability at least $1 - 1/q^{m-n}$ over a random chosen $A \in \mathbb{Z}_q^{n\times m}$. In the case of $\det(\Lambda_q^{\perp}(A)) = q^n$, we consider the following cell

$$P(\Lambda_q^{\perp}(A), \mathbf{x}) := \{\sum_{i=1}^{m} a_i\mathbf{v}_i + \mathbf{x} : a_i \in [-1/2, 1/2)\}. \tag{22}$$

Where $\{\mathbf{v}_i \in \mathbb{Z}_q^m, i \in \{1,\ldots,m-n\}\}$ forms a basis of $\Lambda_q^{\perp}(A)$ with $\max_i\{\|v_i\|\} = \lambda_{m-n}(\Lambda_q^{\perp}(A))$ ($\lambda_{m-n}(\Lambda_q^{\perp}(A))$ is the $(m-n)$-th successive minimum). And $\{\mathbf{v}_i \in \mathbb{Z}_q^m, i \in \{m-n+1,\ldots,m\}\}$ forms a orthogonal basis with length 1 and orthogonal to the space spaned by $\{\mathbf{v}_i \in \mathbb{Z}_q^m, i \in \{1,\ldots,m-n\}\}$. Since for any $\mathbf{x}' \neq \mathbf{x} \in \mathbb{Z}_q^m$ satisfying $A\mathbf{x} = A\mathbf{x}' = \mathbf{0}$, the vector $\mathbf{x}-\mathbf{x}'$ is a linear combination of $\{\mathbf{v}_i \in \mathbb{Z}_q^m, i \in \{1,\ldots,m-n\}\}$, therefore each point $\mathbf{x} \in \Lambda_q^{\perp}(A)$ lies disjointedly in a cell $P(\Lambda_q^{\perp}(A), \mathbf{x})$.

On the other hand, for any vector $\mathbf{v} \in P(\Lambda_q^{\perp}(A), \mathbf{x})$, it holds that

$$\|\mathbf{v} - \mathbf{x}\| \leq (m\cdot\lambda_{m-n}(\Lambda_q^{\perp}(A)) + n)/2$$

Therefore the cell $P(\Lambda_q^{\perp}(A), \mathbf{x})$ of a point $\mathbf{x} \in \mathbb{Z}_q^m$ satisfying $H_A(\mathbf{x}) = A\mathbf{x} = \mathbf{0}$ and $\mathbf{x} \in B_{\beta/2}(\mathbf{0})$ should be contained in a larger sphere $B_{(\beta+m\cdot\lambda_{m-n}(\Lambda_q^{\perp}(A))+n)/2}(\mathbf{0})$. We hence have

$$\begin{aligned}|B_{\beta}(\mathbf{0}) \cap \Lambda_q^{\perp}(A)| &\leq \frac{\mathrm{vol}(B_{(\beta+m\cdot\lambda_{m-n}(\Lambda_q^{\perp}(A))+n)/2}(\mathbf{0}))}{\mathrm{vol}(P(\Lambda_q^{\perp}(A), \mathbf{0}))} \\ &= \frac{\mathrm{vol}(B_{(\beta+m\cdot\lambda_{m-n}(\Lambda_q^{\perp}(A))+n)/2}(\mathbf{0}))}{q^n},\end{aligned} \tag{23}$$

in the case that $\det(\Lambda_q^{\perp}(A)) = q^n$, where $\mathrm{vol}(\cdot)$ denotes the volume.

We notice that the covering radius μ satisfying $\mu(\Lambda_q^{\perp}(A)) > \lambda_{m-n}(\Lambda_q^{\perp}(A))/2$ and the fact that

$$\Pr_A[\frac{1}{\delta} \cdot \sqrt{m} \cdot q^{n/m} \leq 2\mu(\Lambda_q^{\perp}(A))] \leq 1/2^m, \tag{24}$$

for some constant $\delta > 0$. Therefore $\lambda_{m-n}(\Lambda_q^{\perp}(A)) < \frac{1}{\delta} \cdot \sqrt{m} \cdot q^{n/m}$ with probability at least $1 - 2^{-m}$. In that case, the inequality (23) is further estimated as follows.

$$\begin{aligned}
&\frac{\mathrm{vol}(B_{(\beta+m\cdot\lambda_{m-n}(\Lambda_q^{\perp}(A))+n)/2}(\mathbf{0}))}{q^n} \\
&\leq \frac{\mathrm{vol}(B_{(\beta+\frac{1}{\delta}\cdot m^{3/2}\cdot q^{n/m}+n)/2}(\mathbf{0}))}{q^n} \leq \frac{\pi^{m/2}\cdot(\beta+\frac{1}{\delta}\cdot m^{3/2}\cdot q^{n/m}+n)^m}{\mathbf{\Gamma}(m/2+1)\cdot 2^m\cdot q^n} \\
&\leq \frac{\pi^{m/2}\cdot(1+(\frac{1}{\delta}\cdot m^{3/2}\cdot q^{n/m}+n)/\beta)^m\cdot\beta^m}{\mathbf{\Gamma}(m/2+1)\cdot 2^m\cdot q^n} \leq \frac{\pi^{m/2}\cdot(1+O(\frac{1}{m}))^m\cdot\beta^m}{\mathbf{\Gamma}(m/2+1)\cdot 2^m\cdot q^n} \\
&\leq O(\frac{\pi^{m/2}\cdot(\beta/2)^m}{\mathbf{\Gamma}(m/2+1)\cdot q^n}) = O(\frac{\mathrm{vol}(B_{\beta/2}(\mathbf{0}))}{q^n}).
\end{aligned}$$

We now turn to estimate the size of preimages for any $\mathbf{y} \neq \mathbf{0}$. Let's assume there exists a $\mathbf{t} \in \mathbb{Z}_q^m$ such that $H_A(\mathbf{t}) = A\mathbf{t} = \mathbf{y} \bmod q$. It is equivalent to count the cardinality of set

$$\{\mathbf{x} : A\mathbf{x} = 0, \|\mathbf{x}+\mathbf{t}\| \leq \beta/2\}, \tag{25}$$

which is proved similarly as above, to be upper bounded by $O(\mathrm{vol}(B_{\beta/2}(\mathbf{0}))/q^n)$ under the same conditions which are $\frac{1}{\delta} \cdot \sqrt{m} \cdot q^{n/m} > 2\mu(\Lambda_q^{\perp}(A))$ and $\det(\Lambda_q^{\perp}(A)) = q^n$.

Therefore the size of preimages of $\{H_A\}$ is bounded by $O(\mathrm{vol}(B_{\beta/2}(\mathbf{0}))/q^n)$ with probability at least $1 - 2^{-m} - q^{n-m}$, which completes the proof of Theorem 5. □

Since the cardinality of $\{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \leq \beta/2\}$ is approximately equal to the volume of sphere $B_\beta(\mathbf{0})$, therefore the size of preimages for any $\mathbf{y}$ is upper bounded by $O(|\{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \leq \beta\}|/q^n)$ with overwhelming probability. That shows $\{H_A(\mathbf{x}) = A\mathbf{x}\}$ is a collection of almost regular bounded hash functions. Notice that the construction in the proof of Theorem 4 can also be applied to the cases that the input/output space are not in a binary form, which means we can transform Ajtai's construction into a collapsing one assuming the quantum hardness of $\mathbf{SIS}_{n,m,q,\beta}$.

Corollary 6. *Let $\{H_A : \mathbf{X} \to \mathbf{Y}\}$ denote Ajtai's construction of hash functions for $\mathbf{X} = \{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \leq \beta/2\}$ and $\mathbf{Y} = \mathbb{Z}_q^n$. Then*

$$H'_n(h\|A, \mathbf{x}) = (h(\mathbf{x}), A\mathbf{x}) \tag{26}$$

is classical-computable almost polynomial bounded collapsing hash functions assuming the quantum hardness of $\mathbf{SIS}_{n,m,q,\beta}$ for $\beta \geq m^3$, $m \geq n\log q$, and $q \geq \beta \cdot \omega(\sqrt{n\log n})$, where $c > 1$ is a constant. $h : \mathbf{X} \to \{0,1\}^r$ is $(\mathtt{poly}(n)+1)$-wise independent hash function satisfying $\log|\mathbf{X}|/|\mathbf{Y}| - C \leq r < \log|\mathbf{X}|/|\mathbf{Y}|$ for any constant $C > 0$.

5 Conclusion

In this paper, we prove that the collapsing property and the quantum collision-resistance must hold simultaneously when the size of preimages of a hash function are upper bounded by some polynomial, and further deduce that these two properties are in the "same level" under the meaning of implication in "almost regular bounded" case. Our result indicates that the collapsing hash functions belong to the quantum analogue of Hashomania [26] (i.e. the world that collision-resistance hash exists) in many restrictive cases. However, the relation between these two primitives remains open in more general cases. Actually, our result doesn't obstruct the way to construct the quantum collision-resistant hash functions which are not collapsing (in the case that the size of preimages is not bounded by some polynomial). Therefore, we believe it is important to find a concrete construction for that (and even a construction of equivocal collision-resistant hash functions). Besides, since we use the inverse of an quantum circuit in our proof of Theorem 3, which means our results are proved in a semi-black-box manner. We also think it is an intriguing problem that if the relation still holds in fully black-box case, or otherwise, if we can set up a quantum black-box barrier between these two primitives with some technique like the quantum two-oracle method [21,12]?

Acknowledgment We sincerely thank the anonymous reviewers of CRYPTO 2022 for their valuable comments on our paper, and Mark Zhandry for introducing his work to us during the preparation of the final version of our paper. This work was supported by National Natural Science Foundation of China (Grants No. 62172405).

A Proof of Lemma 1

We give a proof of Lemma 1 as follows.

Proof (of Lemma 1). Notice that if the state $\rho_{y,\mathcal{P}}$ output by $\mathcal{E}$ already contains the superposition of the preimages of y. One can obviously distinguishes the difference between measureing the input or the output register of $\rho_{y,\mathcal{P}}$ by invoking $\mathcal{E}$ which directly breaks the collapsing property. However, $\rho_{y,\mathcal{P}}$ may not contain the preimages of y directly. Therefore the main task is to construct a suitable state which contains the superposition of the preimages of y (namely, the challenging state output by the first phase of the adversary $\mathcal{A}$ that intends to break the collapsing property).

Since the evaluation key is not involved in this proof, without loss of generality, we consider this problem in the keyless setting, which is $\{H_n : \{0,1\}^n \to \{0,1\}^m\}_{n\in\mathbb{N}}$.

To proof that lemma, we firstly replace the original $\mathcal{G}$ and $\mathcal{E}$ by their purifications (i.e. assume they are unitary), then we can denote the output state of $\mathcal{G}$ as

$$|\psi\rangle = \sum_{\mathcal{P},y,z} a_{\mathcal{P},y,z}|\mathcal{P},y,z\rangle \otimes |\phi_{y,\mathcal{P},z}\rangle. \tag{27}$$

Where $|\phi_{y,\mathcal{P},z}\rangle$ is the corresponding output state state when the description is $\mathcal{P}$, the hash value equals y, and the auxiliary internal information of $\mathcal{G}$ is z. Then the actual output $\rho_{y,\mathcal{P}}$ equals to the collapsed state $|\psi\rangle$ after measuring the y, $\mathcal{P}$, and tracing out the auxiliary register z which is $\sum_z |a_{\mathcal{P},y,z}|^2 |\phi_{y,\mathcal{P},z}\rangle\langle\phi_{y,\mathcal{P},z}|/(\sum_z |a_{\mathcal{P},y,z}|^2)$. Here for convenience, we denote it equivalently by the following mixed state

$$\rho = \operatorname*{Tr}_{\mathcal{P},y,z} |\psi\rangle\langle\psi| = \sum_{\mathcal{P},y,z} |a_{\mathcal{P},y,z}|^2 |\mathcal{P},y,z\rangle\langle\mathcal{P},y,z| \otimes |\phi_{y,\mathcal{P},z}\rangle\langle\phi_{y,\mathcal{P},z}|.$$

Then the final state after invoking the purified $\mathcal{E}$ on $(b, \rho_{y,\mathcal{P}})$ can be denoted as

$$\rho^{(b)} := \mathcal{E}|b, 0\rangle\langle b, 0| \otimes \rho\mathcal{E}^{\dagger}. \tag{28}$$

Equivalently, we denote by $\mathcal{E}(0, \cdot)$ (or $\mathcal{E}(1, \cdot)$) the unitary operator for the case $b = 0$ (or $b = 1$). Since the correctness of the equivocal collision-resistant hash functions indicates that $\mathcal{E}$ recovers an preimage x of y satisfying $\mathcal{P}(x) = b$ with overwhelming probability, hence $\rho^{(b)}$ must contain the preimages of y with overwhelming probability. Therefore we can rewrite the state $\rho^{(b)}$ as follows [5]

$$\rho^{(b)} = \sum_{\mathcal{P},y,z} |a_{\mathcal{P},y,z}|^2 |\mathcal{P}, y, z, b\rangle\langle\mathcal{P}, y, z, b| \otimes (\sum_{x,w} \beta_{\mathcal{P},y,z,b,x,w}|x, w\rangle)(\sum_{x,w} \bar{\beta}_{\mathcal{P},y,z,b,x,w}\langle x, w|),$$

where x is the output that need to be measured after running $\mathcal{E}(b, \cdot)$, and it holds that

$$\sum_{\mathcal{P},y,z} |a_{\mathcal{P},y,z}|^2 \cdot \sum_{w,x}^{\mathcal{P}(x)=b, H_n(x)=y} |\beta_{\mathcal{P},y,z,b,x,w}|^2 \geq 1 - \mathtt{negl}(n) \tag{29}$$

for some negligible function $\mathtt{negl}(\cdot)$ due to the correctness of the equivocality. Since it may not always hold that $y = H_n(x)$, we hence add an additional register to $\rho^{(b)}$ in order to store the hash value $H_n(x)$, which we denote it by

$$\tilde{\rho}^{(b)} = \sum_{\mathcal{P},y,z} |a_{\mathcal{P},y,z}|^2 |\mathcal{P}, y, z, b\rangle\langle\mathcal{P}, y, z, b| \otimes (\sum_{x,w} \beta_{\mathcal{P},y,z,b,x,w}|x, H_n(x), w\rangle)(\sum_{x,w} \bar{\beta}_{\mathcal{P},y,z,b,x,w}\langle x, H_n(x), w|).$$

Hence $\tilde{\rho}^{(b)}$ contains the input and output of H_n, that inspires us to adopt that state as the challenging state in the collapsing experiment. More specifically, when we give the registers $x, H_n(x)$ of $\tilde{\rho}^{(0)}$ to the challenger of the collapsing game, then if it has been measured in the output register, the state $\rho^{(0)}$ would basically not change, which means we can retrieve some x satisfying $H_n(x) = y \wedge \mathcal{P}(x) = 1$ with overwhelming probability by invoking $\mathcal{E}(1, \cdot) \circ \mathcal{E}^{\dagger}(0, \cdot)$. On the other hand, if it has been measured in the input register, then the state $\rho^{(0)}$ would be probably collapsed and can not be reversible, if not, that implies we can get a collision of y with non-negligible probability.

The following is the description of the adversary $\mathcal{A}$ that breaks the collapsing property:

- $\mathcal{A}$ gets the description of the hash function $H_n(k, \cdot)$, and then invokes the purified $\mathcal{G}(1^n)$ to get the state ρ.
- $\mathcal{A}$ runs the operator $\mathcal{E}(0, \cdot)$ to the state $|0, 0\rangle\langle 0, 0| \otimes \rho$, and gets $\tilde{\rho}^{(0)}$ in result, then sends the input and output registers of $\tilde{\rho}^{(0)}$ to the challenger.
- After receiving the state $\tilde{\rho}^{(0)}_{(b^*)}$ from the challenger ($b^* = 0$ means the state after measuring (tracing out) the output register of $\tilde{\rho}^{(0)}$, and $b^* = 1$ denotes the state after measuring the input register), $\mathcal{A}$ invokes the $\mathcal{E}(1, \cdot) \circ \mathcal{E}^{\dagger}(0, \cdot)$ to that state and measures the result to get a measurement x and the corresponding y. It would output 0 if $\mathcal{P}(x) = 1 \wedge H_n(x) = y$, and output 1 if $\mathcal{P}(x) = 0 \wedge H_n(x) = y$ otherwise, it would returns a random bit $b' \leftarrow \{0, 1\}$ uniformly.

[5] To make it clear, we denote it as a mixed state where the measurement of $\mathcal{P}, y$ is replaced by the tracing out operation, and without loss of generality, we assume the register containing the bit b is not changed by $\mathcal{E}$.

We now estimate the advantage of $\mathcal{A}$. In the case that the challenger measures the output register, according to the correctness of the equivocality of H_n, we can deduce from inequality (29) that the trace distance between $\tilde{\rho}^{(0)}_{(0)}$ and $\tilde{\rho}^{(0)}$ is at most

$$\mathrm{TD}(\tilde{\rho}^{(0)}_{(0)}, \tilde{\rho}^{(0)}) \leq \mathtt{negl}_0(n)$$

for some negligible function $\mathtt{negl}_0(\cdot)$. That implies if we invoke the inverse $\mathcal{E}^\dagger(0,\cdot)$ in that case, we could recover the state $|0,0\rangle\langle 0,0| \otimes \rho$ with overwhelming probability. And hence we get the measurement x that satisfies $\mathcal{P}(x) = 1$ and $H_n(k,x) = y$ with overwhelming probability after invoking $\mathcal{E}$ again. Namely, we have

$$\Pr[\mathcal{A} \text{ outputs } 0 \mid b^* = 0] \geq 1 - \mathtt{negl}_1(n). \tag{30}$$

In the case that the challenger measures the input register (i.e. $b^* = 1$), the input register of $\tilde{\rho}^{(0)}$ would collapse to some x^* (which is the preimage of y with overwhelming probability due to the correctness of equivocality). Then we run the $\mathcal{E}(1,\cdot) \circ \mathcal{E}^\dagger(0,\cdot)$ and measure the result to get a measurement x and the corresponding $H_n(x)$. To estimate the probability that $\mathcal{A}$ wins in this case, we consider the following these events separately:

- The measurement x satisfies $\mathcal{P}(x) = 1 \wedge H_n(x) = y$, that implies we successfully find a collision x, x^*. Therefore the probability of that event occurs is bounded by some negligible function $\mathtt{negl}_2(\cdot)$ (otherwise it would induce an adversary breaks the quantum collision-resistance of $H_n(\cdot)$ with non-negligible probability).
- The measurement x satisfies $\mathcal{P}(x) = 0 \wedge H_n(x) = y$, then $\mathcal{A}$ would return 1 deterministically when that event occurs.
- The measurement x is not a preimage of y, then the probability that $\mathcal{A}$ returns 1 with probability exactly 1/2

That implies

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ outputs } 1 \mid b^* = 1] \\
&\quad = 1 - \Pr[\mathcal{P}(x) = 1 \wedge H_n(x) = y \mid b^* = 1] - \frac{1}{2}\Pr[H_n(x) \neq y \mid b^* = 1] \\
&\quad \geq \frac{1}{2} - \mathtt{negl}_2(n),
\end{aligned} \tag{31}$$

for some negligible function $\mathtt{negl}_2(\cdot)$.

Combining the inequality (30) with (31), we have

$$\begin{aligned}
&\left|\Pr[\mathtt{Exp}^{coll}_{\mathcal{A}}(n) = 1] - \frac{1}{2}\right| \\
&\quad \geq \left|\frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs } 1 \mid b^* = 1] + \frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs } 1 \mid b^* = 1] - \frac{1}{2}\right| \\
&\quad \geq \frac{1}{4} - \mathtt{negl}_1(n) - \mathtt{negl}_2(n),
\end{aligned} \tag{32}$$

which hence breaks the collapsing property of $H_n(\cdot)$. □

Note that the inverse of the operator $\mathcal{E}(\cdot)$ is involved in our proof, which is usually infeasible in the fully black-box sense (even the semi-black-box sense), that is because the process of purification requires the internal information of the equivocal hash functions. That implies we prove the Lemma 1 via a non-black-box manner. However, we believe it is also interesting to figure out if this result still holds in the black-box manner.

References

1. Dorit Aharonov, Alexei Y. Kitaev, and Noam Nisan. Quantum circuits with mixed states. In Jeffrey Scott Vitter, editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 20–30. ACM, 1998.
2. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 99–108. ACM, 1996.
3. Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 474–483. IEEE Computer Society, 2014.
4. Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 255–268. ACM, 2020.
5. Gilad Asharov and Gil Segev. Limits on the power of indistinguishability obfuscation and functional encryption. In Venkatesan Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 191–209. IEEE Computer Society, 2015.
6. Boaz Barak and Oded Goldreich. Universal arguments and their applications. *SIAM J. Comput.*, 38(5):1661–1694, 2008.
7. Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan. Multi-collision resistant hash functions and their applications. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 133–161. Springer, 2018.
8. Nir Bitansky, Iftach Haitner, Ilan Komargodski, and Eylon Yogev. Distributional collision resistance beyond one-way functions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 667–695. Springer, 2019.
9. Nir Bitansky, Yael Tauman Kalai, and Omer Paneth. Multi-collision resistance: a paradigm for keyless hash functions. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 671–684. ACM, 2018.
10. Nir Bitansky, Omer Paneth, and Daniel Wichs. Perfect structure on the edge of chaos - trapdoor permutations from indistinguishability obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, volume 9562 of *Lecture Notes in Computer Science*, pages 474–502. Springer, 2016.

11. Ran Canetti, Huijia Lin, Stefano Tessaro, and Vinod Vaikuntanathan. Obfuscation of probabilistic circuits and applications. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part II*, volume 9015 of *Lecture Notes in Computer Science*, pages 468–497. Springer, 2015.
12. Shujiao Cao and Rui Xue. Being a permutation is also orthogonal to one-wayness in quantum world: Impossibilities of quantum one-way permutations from one-wayness primitives. *Theor. Comput. Sci.*, 855:16–42, 2021.
13. Larry Carter and Mark N. Wegman. Universal classes of hash functions (extended abstract). In John E. Hopcroft, Emily P. Friedman, and Michael A. Harrison, editors, *Proceedings of the 9th Annual ACM Symposium on Theory of Computing, May 4-6, 1977, Boulder, Colorado, USA*, pages 106–112. ACM, 1977.
14. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2002.
15. Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and Dominique Unruh. Post-quantum security of the sponge construction. In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, volume 10786 of *Lecture Notes in Computer Science*, pages 185–204. Springer, 2018.
16. Bella Dubrov and Yuval Ishai. On the randomness complexity of efficient sampling. In Jon M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 711–720. ACM, 2006.
17. Serge Fehr. Classical proofs for the quantum collapsing property of classical hash functions. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 315–338. Springer, 2018.
18. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Collision-free hashing from lattice problems. *Electron. Colloquium Comput. Complex.*, (42), 1996.
19. Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. Finding collisions in interactive protocols - tight lower bounds on the round and communication complexities of statistically hiding commitments. *SIAM J. Comput.*, 44(1):193–242, 2015.
20. Ben Hamlin and Fang Song. Quantum security of hash functions and property-preservation of iterated hashing. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 329–349. Springer, 2019.
21. Akinori Hosoyamada and Takashi Yamakawa. Finding collisions in a quantum world: Quantum black-box separation of collision-resistance and one-wayness. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceed-*

ings, Part I, volume 12491 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2020.

22. Chun-Yuan Hsiao and Leonid Reyzin. Finding collisions on a public road, or do secure hash functions need secret coins? In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 92–105. Springer, 2004.
23. Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, volume 9614 of *Lecture Notes in Computer Science*, pages 387–416. Springer, 2016.
24. Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*, pages 134–147. IEEE Computer Society, 1995.
25. Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* CRC press, 2020.
26. Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 162–194. Springer, 2018.
27. Ilan Komargodski and Eylon Yogev. On distributional collision resistant hashing. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 303–327. Springer, 2018.
28. Noam Mazor and Jiapeng Zhang. Simple constructions from (almost) regular one-way functions. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part II*, volume 13043 of *Lecture Notes in Computer Science*, pages 457–485. Springer, 2021.
29. Ralph C. Merkle. A certified digital signature. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer, 1989.
30. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007.
31. Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.
32. Omer Reingold, Luca Trevisan, and Salil P. Vadhan. Notions of reducibility between cryptographic primitives. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2004.
33. Thomas Ristenpart and Thomas Shrimpton. How to build a hash function from any collision-resistant function. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application*

of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings, volume 4833 of *Lecture Notes in Computer Science*, pages 147–163. Springer, 2007.

34. Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2004.
35. John Rompel. One-way functions are necessary and sufficient for secure signatures. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 387–394. ACM, 1990.
36. Daniel R. Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, volume 1403 of *Lecture Notes in Computer Science*, pages 334–345. Springer, 1998.
37. Dominique Unruh. Collapse-binding quantum commitments without random oracles. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 166–195, 2016.
38. Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 497–527. Springer, 2016.
39. Dominique Unruh. Collapsing sponges: Post-quantum security of the sponge construction. *IACR Cryptol. ePrint Arch.*, page 282, 2017.
40. Mark N. Wegman and Larry Carter. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.*, 22(3):265–279, 1981.
41. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.
42. Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019.
43. Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 408–438. Springer, 2019.
44. Mark Zhandry. New constructions of collapsing hashes. *To Appear in CRYPTO 2022*, 2022.