PAPER *Special Section on Discrete Mathematics and Its Applications*

# Quantum Collision Resistance of Double-Block-Length Hashing

**Shoichi HIROSE**[†a)], ***Member and*** **Hidenori KUWAKADO**[††b)], ***Senior Member***

**SUMMARY** In 2005, Nandi introduced a class of double-block-length compression functions $h^{\pi}(x) := (h(x), h(\pi(x)))$, where $h$ is a random oracle with an $n$-bit output and $\pi$ is a non-cryptographic public permutation. Nandi demonstrated that the collision resistance of $h^{\pi}$ is optimal if $\pi$ has no fixed point in the classical setting. Our study explores the collision resistance of $h^{\pi}$ and the Merkle-Damgård hash function using $h^{\pi}$ in the quantum random oracle model. Firstly, we reveal that the quantum collision resistance of $h^{\pi}$ may not be optimal even if $\pi$ has no fixed point. If $\pi$ is an involution, then a colliding pair of inputs can be found for $h^{\pi}$ with only $O(2^{n/2})$ queries by the Grover search. Secondly, we present a sufficient condition on $\pi$ for the optimal quantum collision resistance of $h^{\pi}$. This condition states that any collision attack needs $\Omega(2^{2n/3})$ queries to find a colliding pair of inputs. The proof uses the recent technique of Zhandry's compressed oracle. Thirdly, we show that the quantum collision resistance of the Merkle-Damgård hash function using $h^{\pi}$ can be optimal even if $\pi$ is an involution. Finally, we discuss the quantum collision resistance of double-block-length compression functions using a block cipher.

***key words:*** *hash function, compression function, double-block-length, Grover's search, Zhandry's compressed oracle*

## 1. Introduction

### 1.1 Background

In the field of cryptography, hash functions play a crucial role and are used in almost all cryptographic schemes. SHS, which stands for Secure Hash Standard, is a standardized family of hash functions [1]. They are called iterated hash functions because of their sequential chaining structure of a compression function, as proposed by Merkle [2] and Damgård [3]. Each hash function in SHS has its own dedicated compression function. Another common method of constructing a compression function is to use a block cipher, as seen in examples like MDC-2 and MDC-4 [4]. MDC-2 has been standardized in ISO/IEC 10118-2 [5], and both MDC-2 and MDC-4 use double-block-length (DBL) construction to achieve a high level of collision resistance. Essentially, the output length of a DBL compression function is double the output length of the underlying block cipher.

In a study by Nandi [6], the security of a specific type of DBL compression functions in the random oracle model was explored. These compression functions were defined as $h^{\pi}(x) := (h(x), h(\pi(x)))$, where $h : \{0,1\}^m \rightarrow \{0,1\}^n$ and $\pi$ is a non-cryptographic public permutation over $\{0,1\}^m$. It was discovered that the collision resistance of $h^{\pi}$ is optimal if $h$ is a random oracle and $\pi$ has no fixed point. In other words, any attack on $h^{\pi}$ would require $\Omega(2^n)$ queries to $h$.

With the recent surge in post-quantum cryptography, analyzing the security of cryptographic schemes against quantum attacks has become a crucial research topic.

### 1.2 Our Contribution

We analyze the quantum collision resistance of the class of DBL compression functions $h^{\pi}$ and the Merkle-Damgård hash functions using them assuming that $h$ is a random oracle. We assume that adversaries are allowed to make superposition queries to their oracles. Firstly, we show that an adversary can find a colliding pair of inputs for $h^{\pi}$ with only $O(2^{n/2})$ queries simply by using the Grover search [7] if $\pi$ is an involution. It implies that the quantum collision resistance of $h^{\pi}$ is not optimal. Secondly, we present a sufficient condition on $\pi$ for the quantum collision resistance of $h^{\pi}$ to be optimal, that is, for any adversary to need $\Omega(2^{2n/3})$ queries to find a colliding pair of inputs for $h^{\pi}$. The proof uses the technique of Zhandry's compressed oracle [8], and it is similar to the proof for the lower bound of quantum collision resistance by Liu and Zhandry [9]. We give two simple examples of $\pi$ satisfying the sufficient condition. Thirdly, we show that we can construct an optimally quantum-collision-resistant Merkle-Damgård hash function by using $h^{\pi}$ even if $\pi$ is an involution. As far as we know, no result has been reported on the quantum collision resistance of the Merkle-Damgård hash function using a DBL compression function. Finally, we make some remarks on DBL compression functions using a block cipher. In particular, we show that the quantum collision resistance of the DBL compression functions proposed by Lai and Massey [10] and by Hirose [11] is not optimal. A Grover oracle of the collision attack is also presented, which is similar to that of the quantum exhaustive key search of a block cipher [12], [13].

This paper is an extended version of our conference paper [14]. It extends the sufficient condition on $\pi$ for the optimal quantum collision resistance of $h^{\pi}$. It discusses the quantum collision resistance of Merkle-Damgård hash functions using Nandi's DBL compression functions, while our conference paper did not discuss it. It also includes the analysis of the quantum collision resistance of the DBL

Manuscript received September 19, 2023.
Manuscript revised January 29, 2024.
Manuscript publicized March 4, 2024.

[†]Faculty of Engineering, University of Fukui, Fukui-shi, 910-8507 Japan.
[††]Faculty of Informatics, Kansai University, Takatsuki-shi, 569-1095 Japan.
a) E-mail: hrs_shch@u-fukui.ac.jp
b) E-mail: kuwakado@kansai-u.ac.jp

DOI: 10.1587/transfun.2023DMP0007

Copyright © 2024 The Institute of Electronics, Information and Communication Engineers

compression functions by Lai and Massey.

### 1.3 Other Related Work

Brassard et al. [15] presented an algorithm that can find a colliding pair of inputs for any $r$-to-one hash function by making $O((N_\mathrm{d}/r)^{1/3})$ quantum queries, where $N_\mathrm{d}$ is the size of the domain of the given hash function. Zhandry [16] later demonstrated that the quantum query complexity to detect a colliding pair of inputs for any hash function with a range of size $N_\mathrm{r}$ is $\Theta(N_\mathrm{r}^{1/3})$.

Chauhan et al. [17] presented a quantum collision attack on the DBL compression function [11] that is instantiated with AES-256. The attack employs a quantum version [18], [19] of the rebound attack [20].

DBL compression functions that use a tweakable block cipher are employed by the leakage-resilient AEAD mode TEDT [21] and a family of lightweight cryptographic schemes called Romulus [22].

### 1.4 Organization

In Sect. 2, necessary notations and definitions are introduced for the upcoming discussions. The construction of DBL compression functions proposed by Nandi and their classical collision resistance are described in Sect. 3. Section 4 discusses the quantum collision resistance of Nandi's DBL compression functions, while Sect. 5 focuses on the quantum collision resistance of Merkle-Damgård hash functions using Nandi's DBL compression functions. In Sect. 6, remarks are made on the quantum collision resistance of DBL compression functions using a block cipher. A brief concluding remark is given in Sect. 7.

## 2. Preliminaries

Let $[n_1, n_2]$ be the set of integers between $n_1$ and $n_2$ inclusive, where $n_1$ and $n_2$ are integers such that $n_1 \le n_2$.

### 2.1 Collision Resistance

For a hash function, a pair of inputs are called colliding if they are distinct and mapped to the same output by the hash function. Collision resistance is the intractability of finding a colliding pair of inputs.

Let $\mathsf{H}^P$ be a hash function using a component $P$. The collision resistance of $\mathsf{H}^P$ is often discussed under the assumption that $P$ is an ideal primitive such as a random oracle or an ideal block cipher [23]. It is measured by the number of queries to $P$ required to find a colliding pair of inputs for $\mathsf{H}^P$.

### 2.2 Merkle-Damgård Hash Function

The Merkle-Damgård construction of a hash function [2], [3] simply iterates a compression function. Let $\mathsf{MD}^F : \{0,1\}^* \to \{0,1\}^\ell$ be a Merkle-Damgård hash function using a compression function $F : \{0,1\}^m \to \{0,1\}^\ell$, where $m > \ell$. $\mathsf{MD}^F$ is described in Algorithm 1. $\mathtt{pad} : \{0,1\}^* \to (\{0,1\}^{m-\ell})^+$ is called a padding function. It usually appends a sequence to an input so that the output length is a multiple of $m - \ell$. $\mathsf{MD}^F$ first applies $\mathtt{pad}$ to an input $M \in \{0,1\}^*$ and divides the resultant sequence into blocks of length $m - \ell$.

**Algorithm 1** Merkle-Damgård hash function $\mathsf{MD}^F$

```
function $\mathsf{MD}^F(M)$
    $M_1 \| M_2 \| \cdots \| M_l \leftarrow \mathtt{pad}(M)$;  ▷ $M_i \in \{0,1\}^{m-\ell}$ for $1 \le i \le l$.
    $V_0 \leftarrow IV$;  ▷ $IV \in \{0,1\}^\ell$ is a constant.
    for $i = 1$ to $l$ do
        $V_i \leftarrow F(V_{i-1} \| M_i)$;
    end for
    return $V_l$;
end function
```

$\mathtt{pad}$ is called suffix-free if, for every distinct $M, M' \in \{0,1\}^*$, each of $\mathtt{pad}(M)$ and $\mathtt{pad}(M')$ is not a suffix of the other. Namely, there exists no $u \in \{0,1\}^*$ satisfying $\mathtt{pad}(M) = u \| \mathtt{pad}(M')$ or $\mathtt{pad}(M') = u \| \mathtt{pad}(M)$. $\mathsf{MD}^F$ with suffix-free $\mathtt{pad}$ is collision-resistant if $F$ is collision-resistant [24]. Thus, we assume that $\mathtt{pad}$ is suffix-free.

### 2.3 Quantum Computation

We assume the quantum circuit model for quantum computation [25]. We further assume that any unitary transformation can be accomplished by a quantum circuit. For a unitary transformation $U$, let $U^\dagger$ be its Hermitian conjugate.

There are specific quantum gates that are present in the remaining parts. The quantum gates $I$, $X$, and $H$ are applied to a single qubit and are defined as follows:

$$I := |0\rangle\langle 0| + |1\rangle\langle 1| ;$$
$$X := |1\rangle\langle 0| + |0\rangle\langle 1| ;$$
$$H := \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1| .$$

The controlled NOT is a quantum gate for two qubits defined as $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$. The Toffoli gate is a quantum gate for three qubits defined as $(I \otimes I - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes X$.

#### 2.3.1 Grover Search

The Grover search [7] is a quantum algorithm to find an element in $f^{-1}(1) := \{x \mid f(x) = 1\}$ for a given Boolean function $f : \{0,1\}^m \to \{0,1\}$. The Grover search uses a unitary operator $O_f$ such that $O_f(|x\rangle \otimes |z\rangle) := |x\rangle \otimes |z \oplus f(x)\rangle$, where $x \in \{0,1\}^m$ and $z \in \{0,1\}$. Thus, $O_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)} |x\rangle \otimes |-\rangle$, where $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$. $O_f$ is called the Grover oracle.

The Grover search proceeds as follows. It first prepares the state

$$H^{\otimes(m+1)}(I^{\otimes m} \otimes X)(|0^m\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} |x\rangle \otimes |-\rangle .$$

Then, it repeatedly applies the Grover operator

$$G := ((H^{\otimes m}(2\left|0^m\right\rangle\left\langle 0^m\right| - I^{\otimes m})H^{\otimes m}) \otimes I)O_f$$

to the state. Finally, it measures the first $m$ qubits. By applying the Grover operator $q$ times, one can find an element in $f^{-1}(1)$ with probability $O(q^2|f^{-1}(1)|/2^m)$.

### 2.3.2 Zhandry's Compressed Oracle [8]

Suppose that a quantum adversary $\mathbf{A}$ has access to a random oracle $R : \{0,1\}^m \to \{0,1\}^\ell$. Let $|x,z,w\rangle$ be a basis state of $\mathbf{A}$, where $x \in \{0,1\}^m$ is a query register, $z \in \{0,1\}^\ell$ is a response register, and $w \in \{0,1\}^l$ is a private working register. Additionally, let $|T_R\rangle$ be a basis state of the random oracle $R$, defined as $|R(0)\rangle \otimes |R(1)\rangle \otimes \cdots \otimes |R(2^m-1)\rangle$. $T_R$ is a binary string of length $\ell 2^m$.

A unitary operator $\mathsf{StO}$ such that

$$\mathsf{StO}(|x,z,w\rangle \otimes |T_R\rangle) := |x, z \oplus R(x), w\rangle \otimes |T_R\rangle$$

represents a query of $\mathbf{A}$ to $R$ and the corresponding response. Zhandry introduced a unitary operator $\mathsf{PhO}$ such that

$$\mathsf{PhO}(|x,z,w\rangle \otimes |T_R\rangle) := |x,z,w\rangle \otimes \left((-1)^{R(x)\cdot z}\,|T_R\rangle\right),$$

which is equivalent to $\mathsf{StO}$ in that

$$\begin{aligned}\mathsf{PhO} = (I^{\otimes m} \otimes H^{\otimes \ell} \otimes I^{\otimes l} \otimes I^{\otimes \ell 2^m}) \circ \mathsf{StO} \\ \circ\, (I^{\otimes m} \otimes H^{\otimes \ell} \otimes I^{\otimes l} \otimes I^{\otimes \ell 2^m}).\end{aligned}$$

Zhandry named $\mathsf{StO}$ and $\mathsf{PhO}$ a standard oracle and a phase oracle, respectively. For these oracles, the random oracle is initialized to the uniform superposition of all the basis states:

$$\frac{1}{\sqrt{2^{\ell 2^m}}} \sum_{T_R \in \{0,1\}^{\ell 2^m}} |T_R\rangle\,.$$

Zhandry further introduced the compressed standard oracle and the compressed phase oracle, which both implement the lazy evaluation of a quantum random oracle. He confirmed that these oracles are equivalent to the standard and phase oracles. Here, we will only focus on the compressed phase oracle.

The compressed phase oracle simulates the random oracle by a superposition of databases. Suppose that $\mathbf{A}$ is allowed to make at most $q$ quantum queries to the random oracle. Then, a database $D$ is an element in $((\{0,1\}^m \cup \{\bot\}) \times \{0,1\}^\ell)^q$. Specifically, $D$ is represented as

$$\underbrace{((x_1,y_1),(x_2,y_2),\ldots,(x_k,y_k),(\bot,0^\ell),\ldots,(\bot,0^\ell)),}_{q\text{ elements in }(\{0,1\}^m \cup \{\bot\}) \times \{0,1\}^\ell}$$

where $x_i \neq \bot$ for $i \in [1,k]$ and $x_1 < x_2 < \cdots < x_k$. For $(x_i,y_i) \in \{0,1\}^m \times \{0,1\}^\ell$, let $(x_i,y_i) \in D$ and $D(x_i) = y_i$ represent that $(x_i,y_i)$ appears in $D$. For $x_i \in \{0,1\}^m$, let $D(x_i) = \bot$ represent that $(x_i,y_i) \notin D$ for any $y_i \in \{0,1\}^\ell$. $D(x_i) = y_i$ means that the random oracle $R$ is specified to output $y_i$ for the input $x_i$. $D(x_i) = \bot$ means that the output of the random oracle $R$ is not yet specified for the input $x_i$. Let $|D|$ represent the number of elements $(x,y)$ in $D$ such that $x \neq \bot$.

For a database $D$ such that $D(x) = \bot$ and $|D| < q$, let $D \cup (x,y)$ represent that $(\bot, 0^\ell)$ is removed from $D$ and $(x,y)$ is added to $D$ in its appropriate position. To describe how the compressed phase oracle processes a query, a unitary operator $\mathsf{StdDecomp}_x$ over a database is introduced. It works as follows:

- For $D$ such that $D(x) = \bot$ and $|D| < q$,

$$\mathsf{StdDecomp}_x\,|D\rangle = \frac{1}{\sqrt{2^\ell}} \sum_{y \in \{0,1\}^\ell} |D \cup (x,y)\rangle\,.$$

- For $D$ such that $D(x) = \bot$ and $|D| < q$,

$$\mathsf{StdDecomp}_x\Big(\frac{1}{\sqrt{2^\ell}} \sum_{y \in \{0,1\}^\ell} (-1)^{z\cdot y}\,|D \cup (x,y)\rangle\Big)$$
$$= \begin{cases} \dfrac{1}{\sqrt{2^\ell}} \displaystyle\sum_{y \in \{0,1\}^\ell} (-1)^{z\cdot y}\,|D \cup (x,y)\rangle & \text{if } z \neq 0^\ell, \\ |D\rangle & \text{if } z = 0^\ell. \end{cases}$$

Let $\mathsf{StdDecomp}$ be a unitary operator over $|x,z,w\rangle \otimes |D\rangle$ defined as follows:

$$\begin{aligned}&\mathsf{StdDecomp}(|x,z,w\rangle \otimes |D\rangle) \\ &\qquad := |x,z,w\rangle \otimes (\mathsf{StdDecomp}_x\,|D\rangle).\end{aligned}$$

Let $\mathsf{CPhO}'$ be a unitary operator such that

$$\mathsf{CPhO}'(|x,z,w\rangle \otimes |D\rangle) := (-1)^{z\cdot D(x)}\,|x,z,w\rangle \otimes |D\rangle\,,$$

where $D(x) \neq \bot$. The compressed phase oracle $\mathsf{CPhO}$ is defined as follows:

$$\mathsf{CPhO} := \mathsf{StdDecomp} \circ \mathsf{CPhO}' \circ \mathsf{StdDecomp}\,.$$

Initially, only $(\bot, 0^\ell)$'s appear in the database.

Zhandry showed the relationship between the output of an adversary on the random oracle and the entries of compressed standard/phase oracle database:

**Lemma 1 ([8])** Let $F$ be a random oracle producing an $\ell$-bit output for each input. Let $\mathbf{A}$ be a quantum algorithm making queries to $F$ and outputting a tuple $(x_1,\ldots,x_k; y_1,\ldots.y_k)$. Let $\mathcal{R}$ be a collection of such tuples. Suppose that, with probability $p$, $\mathbf{A}$ outputs a tuple such that (1) the tuple is in $\mathcal{R}$ and (2) $F(x_i) = y_i$ for every $i \in [1,k]$. Consider running $\mathbf{A}$ with the compressed standard/phase oracle and suppose that the database $D$ is measured after $\mathbf{A}$ produces its output. Let $p'$ be the probability that (1) the tuple is in $\mathcal{R}$ and (2) $D(x_i) = y_i$ for every $i \in [1,k]$. Then, $\sqrt{p} \le \sqrt{p'} + \sqrt{k/2^\ell}$.

## 3. Nandi's Class of DBL Compression Functions

Let $h : \{0,1\}^m \to \{0,1\}^n$ be a compression function such that $m > 2n$. Let $\pi$ be a permutation over $\{0,1\}^m$. An element $a \in \{0,1\}^m$ is called a fixed point of $\pi$ if $\pi(a) = a$.

Nandi [6] studied the classical collision resistance of a class of DBL compression functions $h^\pi : \{0,1\}^m \to \{0,1\}^{2n}$ such that

$$h^\pi(x) := (h(x), h(\pi(x)))$$

assuming that $h$ is a random oracle. He showed that the classical collision resistance of $h^\pi$ is optimal if $\pi$ has no fixed points:

**Theorem 1 (Theorem 1 [6])** Suppose that $h$ is a random oracle and that $\pi$ has no fixed points. Then, the probability that any classical adversary making at most $q$ queries succeeds in finding a colliding pair of inputs for $h^\pi$ is $O((q/2^n)^2)$ if $\pi \circ \pi$ has no fixed points, and $O(q/2^n)$ otherwise.

Strictly speaking, for Theorem 1, the collision resistance is optimal if the success probability is not $O(q/2^n)$ but $O((q/2^n)^2)$. However, in both of the cases, any classical adversary needs $\Omega(2^n)$ queries to find a colliding pair of inputs with some constant probability, and the collision resistance is said to be optimal.

The classical collision resistance of the MD hash function $\mathsf{MD}^{h^\pi}$ was also studied. It can be optimal even if $\pi$ has fixed points:

**Theorem 2 (Theorem 2 [6])** Suppose that $h$ is a random oracle and that $\pi$ is a permutation over $\{0,1\}^m$ such that $|\{v \mid \pi(v\|w) = v\|w \wedge v \in \{0,1\}^{2n}\}| = O(2^n)$. Then, the probability that any classical adversary making at most $q$ queries succeeds in finding a colliding pair of inputs for $\mathsf{MD}^{h^\pi}$ is $O(q/2^n)$.

The classical collision resitance of $\mathsf{MD}^{h^\pi}$ can be *strictly* optimal even if $\pi$ is an involution, that is, $\pi \circ \pi$ is the identity permutation:

**Theorem 3 (Theorem 2 [11])** Suppose that $h$ is a random oracle and that $\pi$ is an involution over $\{0,1\}^m$ without fixed points such that $\pi(v\|w) := \pi_{\mathrm{cv}}(v)\|w$, where $v \in \{0,1\}^{2n}$. Suppose that $\pi_{\mathrm{cv}}(v_0\|v_1) \neq v_1\|v_0$ for every $(v_0, v_1) \in \{0,1\}^n \times \{0,1\}^n$. Then, the probability that any classical adversary making at most $q$ queries succeeds in finding a colliding pair of inputs for $\mathsf{MD}^{h^\pi}$ is $O((q/2^n)^2)$.

An example of $\pi_{\mathrm{cv}}$ is $v_0\|v_1 \mapsto (v_0 \oplus c_0)\|(v_1 \oplus c_1)$, where $c_0$ and $c_1$ are distinct constants in $\{0,1\}^n$.

## 4. Quantum Collision Resistance of Nandi's DBL Compression Functions

Let $\pi$ be a permutation over $\{0,1\}^m$. Then, for every $x \in \{0,1\}^m$, there exists some positive integer $i$ satisfying

$$\pi^i(x) := \underbrace{(\pi \circ \pi \circ \cdots \circ \pi)}_{i}(x) = x.$$

Let $\overset{\pi}{\sim}$ be the relation between elements in $\{0,1\}^m$ such that $x \overset{\pi}{\sim} x'$ if and only if there exists some positive integer $i'$ such that $\pi^{i'}(x) = x'$. Then, $\overset{\pi}{\sim}$ is an equivalence relation, and $C^\pi(x) := \{x' \mid x \overset{\pi}{\sim} x'\}$ is an equivalence class. The equivalence classes form a partition of $\{0,1\}^m$. Namely, $C^\pi(x) \cap C^\pi(\tilde{x}) = \emptyset$ if $C^\pi(x) \neq C^\pi(\tilde{x})$, and $\bigcup_{x \in \{0,1\}^m} C^\pi(x) = \{0,1\}^m$.

In the remaining parts of this paper, it is assumed that all the equivalence classes for $\overset{\pi}{\sim}$ have the same cardinality greater than 1. Then, there exists some positive integer $\gamma$ such that $|C^\pi(x)| = 2^\gamma$ for every $x$, and $\pi$ has no fixed points.

A colliding pair of inputs for $h^\pi$ are divided into two classes based on whether they belong to the same equivalence class for $\overset{\pi}{\sim}$ or not. We call them an intraclass colliding pair if they belong to the same equivalence class and an interclass colliding pair otherwise.

### 4.1 Finding an Intraclass Colliding Pair

The quantum complexity to find an intraclass colliding pair of inputs differs depending on whether the cardinality of the equivalence classes equals 2 or not.

Notice that $\pi$ is an involution with no fixed points if and only if $|C^\pi(x)| = |\{x, \pi(x)\}| = 2$ for every $x$. An intraclass colliding pair of inputs for $h^\pi$ can be found with $O(2^{n/2})$ queries if $\pi$ is an involution with no fixed points:

**Theorem 4** Suppose that $h$ is a random oracle and that $\pi$ is an involution with no fixed points. Then, an adversary making at most $q$ quantum queries is able to find an intraclass colliding pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ with probability $O(q^2/2^n)$.

**Proof** Since $\pi$ is an involution,

$$h^\pi(\pi(x)) = (h(\pi(x)), h(\pi^2(x))) = (h(\pi(x)), h(x)).$$

Thus, if $h(x) = h(\pi(x))$, then $h^\pi(x) = h^\pi(\pi(x))$. Let $f : \{0,1\}^m \to \{0,1\}$ be a Boolean function such that $f(x) = 1$ if and only if $h(x) = h(\pi(x))$. Then, since $h$ is a random oracle, the expected cardinality of $\{x \mid f(x) = 1\}$ is $2^{m-n}$. Thus, the probability that a colliding pair of inputs for $h^\pi$ are found by the Grover search to $f$ is $O(q^2/2^n)$, where $q$ is the number of its iterations. □

Let $\mathcal{X}^\pi := \{x \mid x \in \{0,1\}^m$ is the lexicographically first element in $C^\pi(x)\}$. Then, $|\mathcal{X}^\pi| = 2^{m-\gamma}$. Let $g : \mathcal{X}^\pi \to \{0,1\}^{2^\gamma n}$ be a function such that

$$g(x) := (h(x), h(\pi(x)), h(\pi^2(x)), \ldots, h(\pi^{2^\gamma - 1}(x))).$$

Then, $g$ is a random oracle if $h$ is a random oracle.

The problem to find an intraclass colliding pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ is equivalent to the problem to find an input $x \in \mathcal{X}^\pi$ for $g$ satisfying $(h(\pi^{j_1}(x)), h(\pi^{j_1+1}(x))) = (h(\pi^{j_2}(x)), h(\pi^{j_2+1}(x)))$ for some $j_1$ and $j_2$ such that $0 \leq j_1 < j_2 \leq 2^\gamma - 1$, where $\pi^0(x) = \pi^{2^\gamma}(x) = x$.

If the cardinality of the equivalence classes with respect to $\overset{\pi}{\sim}$ equals $2^\gamma$ for some constant integer $\gamma \geq 2$, then, any quantum adversary needs $\Omega(2^n)$ queries to find an intraclass colliding pair of inputs for $h^\pi$:

**Theorem 5** For $\pi$, suppose that there exists a constant $\gamma \geq 2$ such that $|C^\pi(x)| = 2^\gamma$ for every $x \in \{0,1\}^m$. Then, the probability that any adversary making at most $q$ quantum queries to $g$ succeeds in finding an intraclass colliding pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ is $O((q/2^n)^2)$.

**Proof** Let $\mathcal{Y}_{\mathrm{c1}}$ be the sets of $y := (y_0, y_1, \ldots, y_{2^\gamma-1}) \in (\{0,1\}^n)^{2^\gamma}$ satisfying $(y_{j_1}, y_{j_1+1 \bmod 2^\gamma}) = (y_{j_2}, y_{j_2+1 \bmod 2^\gamma})$ for some $j_1$ and $j_2$ such that $0 \leq j_1 < j_2 \leq 2^\gamma - 1$. Then, $|\mathcal{Y}_{\mathrm{c1}}| \leq 2^{\gamma-1}(2^\gamma - 1)2^{(2^\gamma-2)n}$.

Let $P_{\mathrm{c1}}$ be the projection spanned by all the states containing a database $D$ for $g$ including at least one tuple in $\mathcal{X}^\pi \times \mathcal{Y}_{\mathrm{c1}}$. Then,

$$P_{\mathrm{c1}} = \sum_{x,z,w} \sum_{D \in \mathcal{D}_{\mathrm{c1}}} |x, z, w, D\rangle \langle x, z, w, D| \,,$$

where $\mathcal{D}_{\mathrm{c1}} = \{D \mid D \text{ has at least one tuple in } \mathcal{X}^\pi \times \mathcal{Y}_{\mathrm{c1}}\}$.

For $k \in [1, q]$, let $|\psi_{k-1}\rangle$ be the state right before the $k$-th oracle query is made and $\left|\psi'_k\right\rangle$ be the state right after the $k$-th oracle query is made. Let $\left|\psi'_0\right\rangle$ be the initial state and $\left|\psi_q\right\rangle$ be the state right before the measurement. Let $O_g$ be the operator making an oracle query to $g$. Then, $\left|\psi'_k\right\rangle = O_g |\psi_{k-1}\rangle$. For $k \in [0, q]$, let $U_k$ be the operator such that $|\psi_k\rangle = U_k \left|\psi'_k\right\rangle$. Thus, $U_k$ represents the local computation on $|x, z, w\rangle$ by the adversary and it does not affect the database.

The probability that a colliding pair of inputs for $h^\pi$ in the same equivalence class is found is $\|P_{\mathrm{c1}} \left|\psi_q\right\rangle\|^2 := \left\langle\psi_q\right| P_{\mathrm{c1}}^\dagger P_{\mathrm{c1}} \left|\psi_q\right\rangle = \left\langle\psi_q\right| P_{\mathrm{c1}} \left|\psi_q\right\rangle$.

Let us evaluate an upper bound on $\|P_{\mathrm{c1}} |\psi_k\rangle\|$. Since $U_k$ does not affect the database,

$$\|P_{\mathrm{c1}} |\psi_k\rangle\| = \|P_{\mathrm{c1}} U_k \left|\psi'_k\right\rangle\| = \|P_{\mathrm{c1}} \left|\psi'_k\right\rangle\|.$$

In addition,

$$\begin{aligned}
\|P_{\mathrm{c1}} \left|\psi'_k\right\rangle\| &= \|P_{\mathrm{c1}} O_g |\psi_{k-1}\rangle\| \\
&= \|P_{\mathrm{c1}} O_g (P_{\mathrm{c1}} + (I^{\otimes L} - P_{\mathrm{c1}})) |\psi_{k-1}\rangle\| \\
&\leq \|P_{\mathrm{c1}} O_g P_{\mathrm{c1}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c1}} O_g (I^{\otimes L} - P_{\mathrm{c1}}) |\psi_{k-1}\rangle\| \\
&\leq \|P_{\mathrm{c1}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c1}} O_g (I^{\otimes L} - P_{\mathrm{c1}}) |\psi_{k-1}\rangle\|,
\end{aligned}$$

where $L$ is the number of qubits in $|\psi_{k-1}\rangle$. For the last term, let

$$|\psi_{k-1}\rangle = \sum_{x,z,w} \sum_{D} \alpha_{x,z,w,D} |x, z, w\rangle \otimes |D\rangle \,.$$

Then,

$$\begin{aligned}
&\|P_{\mathrm{c1}} O_g (I^{\otimes L} - P_{\mathrm{c1}}) |\psi_{k-1}\rangle\| \\
&\quad = \left\| P_{\mathrm{c1}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c1}}} \alpha_{x,z,w,D} |x, z, w\rangle \otimes |D\rangle \right\|.
\end{aligned}$$

For any $D \notin \mathcal{D}_{\mathrm{c1}}$, if $D(x) \neq \perp$, then $D(x) \notin \mathcal{Y}_{\mathrm{c1}}$. Thus,

$$\begin{aligned}
&\left\| P_{\mathrm{c1}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c1}}} \alpha_{x,z,w,D} |x, z, w\rangle \otimes |D\rangle \right\| \\
&= \Bigg\| P_{\mathrm{c1}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c1}},\\ D(x) = \perp}} \frac{1}{\sqrt{2^{2^\gamma n}}} \sum_{y'} \\
&\qquad (-1)^{z \cdot y'} \alpha_{x,z,w,D} |x, z, w\rangle \otimes |D \cup (x, y')\rangle \Bigg\| \\
&= \Bigg\| \frac{1}{\sqrt{2^{2^\gamma n}}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c1}},\\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_{\mathrm{c1}}} \\
&\qquad (-1)^{z \cdot y'} \alpha_{x,z,w,D} |x, z, w\rangle \otimes |D \cup (x, y')\rangle \Bigg\| \\
&= \Bigg( \frac{1}{2^{2^\gamma n}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c1}},\\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_{\mathrm{c1}}} |\alpha_{x,z,w,D}|^2 \Bigg)^{1/2} \\
&\leq \Bigg( \frac{2^{\gamma-1}(2^\gamma - 1)2^{(2^\gamma-2)n}}{2^{2^\gamma n}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c1}},\\ D(x) = \perp}} |\alpha_{x,z,w,D}|^2 \Bigg)^{1/2} \\
&\leq \frac{\sqrt{2^{\gamma-1}(2^\gamma - 1)}}{2^n}.
\end{aligned}$$

Thus,

$$\|P_{\mathrm{c1}} |\psi_k\rangle\| \leq \|P_{\mathrm{c1}} |\psi_{k-1}\rangle\| + 2^{\gamma-1/2}/2^n,$$

which implies $\|P_{\mathrm{c1}} \left|\psi_q\right\rangle\| = O(q/2^n)$ since $\gamma$ is constant. This completes the proof together with Lemma 1. □

### 4.2 Finding an Interclass Colliding Pair

The following theorem implies that, to find an interclass colliding pair of inputs for $h^\pi$, any quantum adversary needs $\Omega(2^{2n/3})$ queries. The proof is similar to that of Theorem 4 by Liu and Zhandry [9].

**Theorem 6** For $\pi$, suppose that there exists a constant integer $\gamma \geq 1$ such that $|C^\pi(x)| = 2^\gamma$ for every $x \in \{0,1\}^m$. Then, for any adversary making at most $q$ quantum queries to $g$, the probability that it succeeds in finding an interclass colliding pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ is $O(q^3/2^{2n})$.

**Proof** The problem to find an interclass colliding pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ is equivalent to the problem to find a pair of inputs $x, x' \in \mathcal{X}^\pi$ for $g$ satisfying $C^\pi(x) \neq C^\pi(x')$ and $(h(\pi^i(x)), h(\pi^{i+1}(x))) = (h(\pi^j(x')), h(\pi^{j+1}(x')))$ for some $i, j \in [0, 2^\gamma - 1]$, where $\pi^0(x) = \pi^{2^\gamma}(x) = x$ and $\pi^0(x') = \pi^{2^\gamma}(x') = x'$.

Let $P_{\mathrm{c2}}$ be the projection spanned by all the states containing a database $D$ for $g$ including at least a pair of tuples $(x^*, y^*)$ and $(x^{**}, y^{**})$ in $\mathcal{X}^\pi \times (\{0,1\}^n)^{2^\gamma}$ such that $(y^*_i, y^*_{i+1 \bmod 2^\gamma}) = (y^{**}_j, y^{**}_{j+1 \bmod 2^\gamma})$ for some $i, j \in [0, 2^\gamma - 1]$, where $y^* = (y^*_0, y^*_1, \ldots, y^*_{2^\gamma-1})$ and $y^{**} = (y^{**}_0, y^{**}_1, \ldots, y^{**}_{2^\gamma-1})$. Then,

$$P_{\mathrm{c2}} = \sum_{x,z,w} \sum_{D \in \mathcal{D}_{\mathrm{c2}}} |x,z,w,D\rangle \langle x,z,w,D| ,$$

where $\mathcal{D}_{\mathrm{c2}}$ is the set of the databases including at least a pair of tuples described above.

For $k \in [1,q]$, let $|\psi_{k-1}\rangle$ be the state right before the $k$-th oracle query is made and $\left|\psi'_k\right\rangle$ be the state right after the $k$-th oracle query is made. Let $\left|\psi'_0\right\rangle$ be the initial state and $\left|\psi_q\right\rangle$ be the state just before the measurement. Let $O_g$ be the operator making an oracle query. Then, $\left|\psi'_k\right\rangle = O_g |\psi_{k-1}\rangle$. For $k \in [0,q]$, let $U_k$ be the operator such that $|\psi_k\rangle = U_k \left|\psi'_k\right\rangle$. Thus, $U_k$ represents the local computation on $|x,z,w\rangle$ by the adversary and it does not affect the database.

A colliding pair of inputs $x$ and $x'$ for $h^\pi$ satisfying $C^\pi(x) \neq C^\pi(x')$ is found with probability at most $\|P_{\mathrm{c2}} \left|\psi_q\right\rangle\|^2$. In the remaining parts, an upper bound on $\|P_{\mathrm{c2}} |\psi_k\rangle\|$ is evaluated.

Since $U_k$ does not affect the database,

$$\|P_{\mathrm{c2}} |\psi_k\rangle\| = \|P_{\mathrm{c2}} U_k \left|\psi'_k\right\rangle\| = \|P_{\mathrm{c2}} \left|\psi'_k\right\rangle\|.$$

In addition,

$$\begin{aligned}
\|P_{\mathrm{c2}} \left|\psi'_k\right\rangle\| &= \|P_{\mathrm{c2}} O_g |\psi_{k-1}\rangle\| \\
&= \|P_{\mathrm{c2}} O_g (P_{\mathrm{c2}} + (I^{\otimes L} - P_{\mathrm{c2}})) |\psi_{k-1}\rangle\| \\
&\le \|P_{\mathrm{c2}} O_g P_{\mathrm{c2}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c2}} O_g (I^{\otimes L} - P_{\mathrm{c2}}) |\psi_{k-1}\rangle\| \\
&\le \|P_{\mathrm{c2}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c2}} O_g (I^{\otimes L} - P_{\mathrm{c2}}) |\psi_{k-1}\rangle\|,
\end{aligned}$$

where $L$ is the number of qubits in $|\psi_{k-1}\rangle$. For the last term, let

$$|\psi_{k-1}\rangle = \sum_{x,z,w} \sum_{D} \alpha_{x,z,w,D} |x,z,w\rangle \otimes |D\rangle .$$

Then,

$$\begin{aligned}
&\|P_{\mathrm{c2}} O_g (I^{\otimes L} - P_{\mathrm{c2}}) |\psi_{k-1}\rangle\| \\
&\quad = \left\| P_{\mathrm{c2}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c2}}} \alpha_{x,z,w,D} |x,z,w\rangle \otimes |D\rangle \right\|.
\end{aligned}$$

If $D(x) \neq \perp$, then $D \notin \mathcal{D}_{\mathrm{c2}}$ and the database after the application of $O_g$ has no pair of tuples containing a colliding pair of inputs for $h^\pi$. For $D \notin \mathcal{D}_{\mathrm{c2}}$, let $\mathcal{Y}_D$ be the set of $y' = (y'_0, y'_1, \ldots, y'_{2^\gamma-1}) \in (\{0,1\}^n)^{2^\gamma}$ such that there exists $(x^*, y^*) \in D$ satisfying $(y^*_i, y^*_{i+1 \bmod 2^\gamma}) = (y'_j, y'_{j+1 \bmod 2^\gamma})$ for some $i, j \in [0, 2^\gamma - 1]$. Then,

$$\begin{aligned}
&\left\| P_{\mathrm{c2}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c2}}} \alpha_{x,z,w,D} |x,z,w\rangle \otimes |D\rangle \right\| \\
&\quad = \Bigg\| P_{\mathrm{c2}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c2}},\\ D(x) = \perp}} \frac{1}{\sqrt{2^{2^\gamma n}}} \sum_{y'} \\
&\qquad\qquad (-1)^{z \cdot y'} \alpha_{x,z,w,D} |x,z,w\rangle \otimes |D \cup (x,y')\rangle \Bigg\| \\
&\quad = \Bigg\| \frac{1}{\sqrt{2^{2^\gamma n}}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c2}},\\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_D} \\
&\qquad\qquad (-1)^{z \cdot y'} \alpha_{x,z,w,D} |x,z,w\rangle \otimes |D \cup (x,y')\rangle \Bigg\| \\
&\quad = \Bigg( \frac{1}{2^{2^\gamma n}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c2}},\\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_D} |\alpha_{x,z,w,D}|^2 \Bigg)^{1/2} \\
&\quad \le \Bigg( \frac{2^{2\gamma} \cdot 2^{(2^\gamma-2)n} (k-1)}{2^{2^\gamma n}} \sum_{\substack{x,z,w,\\ x \in \mathcal{X}^\pi, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c2}},\\ D(x) = \perp}} |\alpha_{x,z,w,D}|^2 \Bigg)^{1/2} \\
&\quad \le \frac{2^\gamma \sqrt{k-1}}{2^n}.
\end{aligned}$$

Altogether,

$$\|P_{\mathrm{c2}} |\psi_k\rangle\| \le \|P_{\mathrm{c2}} |\psi_{k-1}\rangle\| + 2^\gamma \sqrt{k-1} / 2^n.$$

Thus,

$$\|P_{\mathrm{c2}} \left|\psi_q\right\rangle\| \le \frac{1}{2^{n-\gamma}} \sum_{k=1}^{q-1} \sqrt{k} \le \frac{(q-1)\sqrt{q-1}}{2^{n-\gamma}},$$

which implies $\|P_{\mathrm{c2}} \left|\psi_q\right\rangle\| = O(q^{3/2}/2^n)$ since $\gamma$ is constant. This completes the proof together with Lemma 1. □

### 4.3 Summary

The quantum collision resistance of $h^\pi$ is not optimal if $\pi$ is an involution with no fixed points:

**Corollary 1** Suppose that $h$ is a random oracle and that $\pi$ is a permutation satisfying $|C^\pi(x)| = 2$ for every $x \in \{0,1\}^m$. Then, an adversary making at most $q$ quantum queries can find a colliding pair of inputs for $h^\pi$ with probability $O(q^2/2^n)$.

Corollary 1 directly follows from Theorems 4 and 6. An example of an involution with no fixed points is $x \mapsto x \oplus c$, where $c$ is a non-zero constant.

The following corollary implies that the quantum collision resistance of $h^\pi$ is optimal if the cardinality of the equivalence classes with respect to $\overset{\pi}{\sim}$ equals $2^\gamma$ for some constant integer $\gamma \ge 2$. Namely, to find a colliding pair of inputs for $h^\pi$ with some constant probability, any quantum adversary needs $\Omega(2^{2n/3})$ queries:

**Corollary 2** For $\pi$, suppose that there exists a constant $\gamma \ge 2$ such that $|C^\pi(x)| = 2^\gamma$ for every $x \in \{0,1\}^m$. Then, for any adversary making at most $q$ quantum queries, the probability that it succeeds in finding a colliding pair of inputs for $h^\pi$ is $O(q^3/2^{2n})$.

Corollary 2 directly follows from Theorems 5 and 6. A permutation $\pi$ is interesting for instantiation of $h^\pi$ if it is very easy to compute and the cardinality of the equivalence classes with respect to $\overset{\pi}{\sim}$ equals 4.

**Example 1** Let $m$ be an even integer. Let $c \in \{0,1\}^{m/2} \setminus \{\mathbf{0}\}$ be a constant. Then, the following permutations over $\{0,1\}^m$

satisfy that the cardinality of their equivalence classes equals 4: $(x_0, x_1) \mapsto (x_0 \oplus x_1, x_1 \oplus c)$, where $x_0, x_1 \in \{0,1\}^{m/2}$.

**Example 2** Let $\gamma \geq 2$ and suppose that $2^{\gamma-1}$ divides $m$. Let $c \in \{0,1\}^{m/2^{\gamma-1}} \setminus \{\mathbf{0}\}$ be a constant. Then, the following permutations over $\{0,1\}^m$ satisfy that the cardinality of their equivalence classes equals $2^\gamma$: $(x_0, x_1, \ldots, x_{2^{\gamma-1}-1}) \mapsto (x_1, \ldots, x_{2^{\gamma-1}-1}, x_0 \oplus c)$, where $x_0, x_1, \ldots, x_{2^{\gamma-1}-1} \in \{0,1\}^{m/2^{\gamma-1}}$.

## 5. Quantum Collision Resistance of Merkle-Damgård Hash Functions Using Nandi's DBL Compression Functions

If there exists some integer $\gamma \geq 2$ such that the cardinality of the equivalence classes for $\overset{\pi}{\sim}$ equals $2^\gamma$, then the quantum collision resistance of $\mathsf{MD}^{h^\pi}$ is optimal:

**Corollary 3** Suppose that $h$ is a random oracle. For $\pi$, suppose that there exists a constant integer $\gamma \geq 2$ such that $|C^\pi(x)| = 2^\gamma$ for every $x \in \{0,1\}^m$. Then, the probability that any adversary making at most $q$ quantum queries succeeds in finding a colliding pair of inputs for $\mathsf{MD}^{h^\pi}$ is $O(q^3/2^{2n})$.

**Proof** The notation in Algorithm 1 is used in the proof.

Suppose that a colliding pair of inputs $M$ and $M'$ are found for $\mathsf{MD}^{h^\pi}$. Let $M_1\|M_2\|\cdots\|M_l \leftarrow \mathtt{pad}(M)$ and $M'_1\|M'_2\|\cdots\|M'_{l'} \leftarrow \mathtt{pad}(M')$. Then, since $\mathtt{pad}$ is suffix-free, there exists some $t \in [0, \min\{l, l'\} - 1]$ such that $V_{l-t-1}\|M_{l-t}$ and $V'_{l'-t-1}\|M'_{l'-t}$ are a colliding pair of inputs for $h^\pi$. Thus, the corollary follows from Theorems 5 and 6. □

The quantum collision resitance of $\mathsf{MD}^{h^\pi}$ can be optimal even if $\pi$ is an involution. Corollary 4 is a quantum version of Theorem 3.

**Corollary 4** Suppose that $h$ is a random oracle and that $\pi$ is an involution over $\{0,1\}^m$ without fixed points such that $\pi(v\|w) := \pi_{\mathrm{cv}}(v)\|w$, where $v \in \{0,1\}^{2n}$. Suppose that $\pi_{\mathrm{cv}}(v_0\|v_1) \neq v_1\|v_0$ for every $(v_0, v_1) \in \{0,1\}^n \times \{0,1\}^n$. Then, the probability that any quantum adversary making at most $q$ queries succeeds in finding a colliding pair of inputs for $\mathsf{MD}^{h^\pi}$ is $O(q^3/2^{2n})$.

**Proof** The notation in Algorithm 1 is used in the proof.

Notice that $|C^\pi(x)| = 2$ for every $x \in \{0,1\}^m$ and $\pi_{\mathrm{cv}}$ has no fixed points.

Suppose that a colliding pair of inputs $M$ and $M'$ are found for $\mathsf{MD}^{h^\pi}$. Let $M_1\|M_2\|\cdots\|M_l \leftarrow \mathtt{pad}(M)$ and $M'_1\|M'_2\|\cdots\|M'_{l'} \leftarrow \mathtt{pad}(M')$. Without loss of generality, suppose that $l \geq l'$. Then, since $\mathtt{pad}$ is suffix-free, there exists some $t \in [0, l'-1]$ such that $V_{l-t-1}\|M_{l-t}$ and $V'_{l'-t-1}\|M'_{l'-t}$ are a colliding pair of inputs for $h^\pi$. Let $t^* := \min\{t \mid V_{l-t-1}\|M_{l-t}$ and $V'_{l'-t-1}\|M'_{l'-t}$ are a colliding pair$\}$.

Suppose that $V_{l-t^*-1}\|M_{l-t^*}$ and $V'_{l'-t^*-1}\|M'_{l'-t^*}$ are an interclass colliding pair. Then, from Theorem 6, the success probability in finding them is $O(q^3/2^{2n})$.

Suppose that $V_{l-t^*-1}\|M_{l-t^*}$ and $V'_{l'-t^*-1}\|M'_{l'-t^*}$ are an intraclass colliding pair. Then,

$$\pi(V_{l-t^*-1}\|M_{l-t^*}) = \pi_{\mathrm{cv}}(V_{l-t^*-1})\|M_{l-t^*} = V'_{l'-t^*-1}\|M'_{l'-t^*}.$$

Thus, if $t^* = l' - 1$, then $M_{l-l'+j} = M'_j$ for every $j \in [1, l']$. It contradicts the assumption that $\mathtt{pad}$ is suffix-free. Thus, $t^* \leq l' - 2$. Since $\pi_{\mathrm{cv}}(V_{l-t^*-1}) = V'_{l'-t^*-1}$, $V_{l-t^*-1} \neq V'_{l'-t^*-1}$. Thus,

$$\pi_{\mathrm{cv}}(h^\pi(V_{l-t^*-2}\|M_{l-t^*-1})) = h^\pi(V'_{l'-t^*-2}\|M'_{l'-t^*-1}),$$

and $V_{l-t^*-2}\|M_{l-t^*-1} \neq V'_{l'-t^*-2}\|M'_{l'-t^*-1}$. In addition, since $\pi_{\mathrm{cv}}(v_0\|v_1) \neq v_1\|v_0$ for every $(v_0, v_1)$,

$$C^\pi(V_{l-t^*-2}\|M_{l-t^*-1}) \neq C^\pi(V'_{l'-t^*-2}\|M'_{l'-t^*-1}).$$

The problem to find such an interclass *pseudo-colliding* pair of inputs for $h^\pi$ with respect to $\overset{\pi}{\sim}$ is equivalent to the problem to find a pair of inputs $x, x' \in \mathcal{X}^\pi$ for $g$ (with $\gamma = 1$) satisfying $C^\pi(x) \neq C^\pi(x')$ and $\pi_{\mathrm{cv}}(h(\pi^i(x))\|h(\pi^{i+1}(x))) = h(\pi^j(x'))\|h(\pi^{j+1}(x'))$ for some $i, j \in [0,1]$, where $\pi^0(x) = \pi^2(x) = x$ and $\pi^0(x') = \pi^2(x') = x'$.

Let $P_{\mathrm{c3}}$ be the projection spanned by all the states containing a database $D$ for $g$ including at least a pair of tuples $(x^*, y^*)$ and $(x^{**}, y^{**})$ in $\mathcal{X}^\pi \times (\{0,1\}^n \times \{0,1\}^n)$ such that $\pi_{\mathrm{cv}}(y^*_i\|y^*_{i+1 \bmod 2}) = y^{**}_j\|y^{**}_{j+1 \bmod 2}$ for some $i, j \in [0,1]$, where $y^* = (y^*_0, y^*_1)$ and $y^{**} = (y^{**}_0, y^{**}_1)$. Then,

$$P_{\mathrm{c3}} = \sum_{x,z,w} \sum_{D \in \mathcal{D}_{\mathrm{c3}}} |x, z, w, D\rangle \langle x, z, w, D|,$$

where $\mathcal{D}_{\mathrm{c3}}$ is the set of the databases including at least a pair of tuples described above.

For $k \in [1, q]$, let $|\psi_{k-1}\rangle$ be the state right before the $k$-th oracle query is made and $|\psi'_k\rangle$ be the state right after the $k$-th oracle query is made. Let $|\psi'_0\rangle$ be the initial state and $|\psi_q\rangle$ be the state just before the measurement. Let $O_g$ be the operator making an oracle query. Then, $|\psi'_k\rangle = O_g |\psi_{k-1}\rangle$. For $k \in [0, q]$, let $U_k$ be the operator such that $|\psi_k\rangle = U_k |\psi'_k\rangle$. Thus, $U_k$ represents the local computation on $|x, z, w\rangle$ by the adversary and it does not affect the database.

A *pseudo-colliding* pair of inputs for $h^\pi$ is found with probability $\|P_{\mathrm{c3}} |\psi_q\rangle\|^2$. In the remaining parts, an upper bound on $\|P_{\mathrm{c3}} |\psi_k\rangle\|$ is evaluated.

Since $U_k$ does not affect the database,

$$\|P_{\mathrm{c3}} |\psi_k\rangle\| = \|P_{\mathrm{c3}} U_k |\psi'_k\rangle\| = \|P_{\mathrm{c3}} |\psi'_k\rangle\|.$$

In addition,

$$\begin{aligned}
\|P_{\mathrm{c3}} |\psi'_k\rangle\| &= \|P_{\mathrm{c3}} O_g |\psi_{k-1}\rangle\| \\
&= \|P_{\mathrm{c3}} O_g (P_{\mathrm{c3}} + (I^{\otimes L} - P_{\mathrm{c3}})) |\psi_{k-1}\rangle\| \\
&\leq \|P_{\mathrm{c3}} O_g P_{\mathrm{c3}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c3}} O_g (I^{\otimes L} - P_{\mathrm{c3}}) |\psi_{k-1}\rangle\| \\
&\leq \|P_{\mathrm{c3}} |\psi_{k-1}\rangle\| + \|P_{\mathrm{c3}} O_g (I^{\otimes L} - P_{\mathrm{c3}}) |\psi_{k-1}\rangle\|,
\end{aligned}$$

where $L$ is the number of qubits in $|\psi_{k-1}\rangle$. For the last term, let

$$|\psi_{k-1}\rangle = \sum_{x,z,w} \sum_{D} \alpha_{x,z,w,D} \, |x,z,w\rangle \otimes |D\rangle \, .$$

Then,

$$\begin{aligned} &\| P_{\mathrm{c3}} O_g (I^{\otimes L} - P_{\mathrm{c3}}) \, |\psi_{k-1}\rangle \, \| \\ &\quad = \left\| P_{\mathrm{c3}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c3}}} \alpha_{x,z,w,D} \, |x,z,w\rangle \otimes |D\rangle \right\| . \end{aligned}$$

If $D(x) \neq \perp$, then $D \notin \mathcal{D}_{\mathrm{c3}}$ and the database after the application of $O_g$ has no pair of tuples containing a *pseudo-colliding* pair of inputs for $h^{\pi}$. For $D \notin \mathcal{D}_{\mathrm{c3}}$, let $\mathcal{Y}_D$ be the set of $y' = (y'_0, y'_1) \in \{0,1\}^n \times \{0,1\}^n$ such that there exists $(x^*, y^*) \in D$ satisfying $\pi_{\mathrm{cv}}(y^*_i \| y^*_{i+1 \bmod 2}) = y'_j \| y'_{j+1 \bmod 2}$ for some $i, j \in [0,1]$. Then,

$$\begin{aligned} &\left\| P_{\mathrm{c3}} O_g \sum_{x,z,w} \sum_{D \notin \mathcal{D}_{\mathrm{c3}}} \alpha_{x,z,w,D} \, |x,z,w\rangle \otimes |D\rangle \right\| \\ &\quad = \left\| P_{\mathrm{c3}} \sum_{\substack{x,z,w, \\ x \in \mathcal{X}^{\pi}, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c3}}, \\ D(x) = \perp}} \frac{1}{\sqrt{2^{2n}}} \sum_{y'} \right. \\ &\qquad\qquad \left. (-1)^{z \cdot y'} \alpha_{x,z,w,D} \, |x,z,w\rangle \otimes |D \cup (x,y')\rangle \right\| \\ &\quad = \left\| \frac{1}{\sqrt{2^{2n}}} \sum_{\substack{x,z,w, \\ x \in \mathcal{X}^{\pi}, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c3}}, \\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_D} \right. \\ &\qquad\qquad \left. (-1)^{z \cdot y'} \alpha_{x,z,w,D} \, |x,z,w\rangle \otimes |D \cup (x,y')\rangle \right\| \\ &\quad = \left( \frac{1}{2^{2n}} \sum_{\substack{x,z,w, \\ x \in \mathcal{X}^{\pi}, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c3}}, \\ D(x) = \perp}} \sum_{y' \in \mathcal{Y}_D} |\alpha_{x,z,w,D}|^2 \right)^{1/2} \\ &\quad \leq \left( \frac{2^2(k-1)}{2^{2n}} \sum_{\substack{x,z,w, \\ x \in \mathcal{X}^{\pi}, z \neq 0}} \sum_{\substack{D \notin \mathcal{D}_{\mathrm{c3}}, \\ D(x) = \perp}} |\alpha_{x,z,w,D}|^2 \right)^{1/2} \\ &\quad \leq \frac{2\sqrt{k-1}}{2^n} . \end{aligned}$$

Altogether,

$$\| P_{\mathrm{c3}} \, |\psi_k\rangle \, \| \leq \| P_{\mathrm{c3}} \, |\psi_{k-1}\rangle \, \| + 2\sqrt{k-1}/2^n .$$

Thus,

$$\| P_{\mathrm{c3}} \, |\psi_q\rangle \, \| \leq \frac{1}{2^{n-1}} \sum_{k=1}^{q-1} \sqrt{k} \leq \frac{(q-1)\sqrt{q-1}}{2^{n-1}} ,$$

which implies $\| P_{\mathrm{c3}} \, |\psi_q\rangle \, \|^2 = O(q^3/2^{2n})$. This completes the proof together with Lemma 1. □

## 6. Observation on DBL Compression Functions Using a Block Cipher

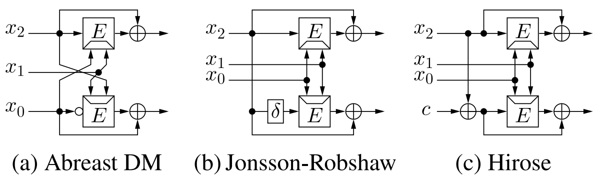


**Fig. 1** DBL compression functions using a block cipher. The message block input is $x_1$ for abreast Davies-Meyer and Hirose and $x_2$ for Jonsson-Robshaw.

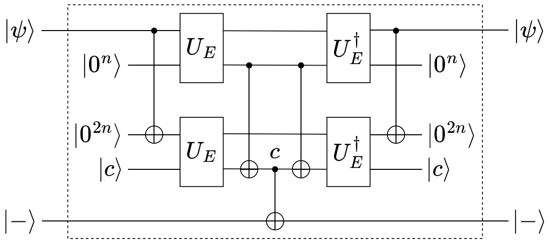


**Fig. 2** Grover oracle for the collision attack.

Let $E : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with its key space $\{0,1\}^{2n}$. Some observations are given on three DBL compression functions using the block cipher $E$, which are depicted in Fig. 1. Let $h_E : (\{0,1\}^n)^3 \to \{0,1\}^n$ be the compression function such that $h_E(x_0, x_1, x_2) := E((x_0, x_1), x_2) \oplus x_2$.

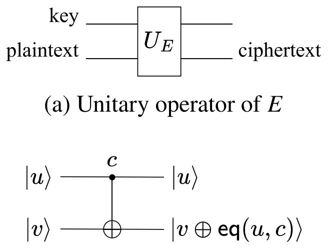
### 6.1 The Hirose Construction

Let $\varpi$ be a permutation over $(\{0,1\}^n)^3$ such that $\varpi(x_0, x_1, x_2) := (x_0, x_1, x_2 \oplus c)$, where $c \in \{0,1\}^n$ is a non-zero constant. Then, $h_E^{\varpi}$ represents the DBL compression function proposed by Hirose [11]. It is depicted in Fig. 1(c).

The DBL compression function $h_E^{\varpi}$ can be attacked using the collision attack presented in the proof of Theorem 4, since $\varpi$ is an involution. The Grover oracle of this attack is similar to that of the exhaustive key search for a block cipher by Jaques et al. [13] and is depicted in Fig. 2. The components of the oracle are specified in Fig. 3. $U_E$ is the unitary operator of $E$. In Fig. 3(b), $\mathsf{eq}$ is a predicate such that $\mathsf{eq}(u, c) = 1$ if and only if $u = c$, and the component is constructed using a controlled NOT gate, $O(n)$ Toffoli gates, $O(n)$ $X$ gates, and $O(n)$ additional qubits [25]. Notice that $E((x_0, x_1), x_2) = E((x_0, x_1), x_2 \oplus c) \oplus c$ if $h_E(x_0, x_1, x_2) = h_E(\varpi(x_0, x_1, x_2))$. The plaintext inputs to $U_E$ in the Grover oracle in Fig. 2 are fixed constants $0^n$ and $c$.

### 6.2 The Abreast Davies-Meyer Construction

Let $\xi$ be a permutation over $(\{0,1\}^n)^3$ such that $\xi(x_0, x_1, x_2) := (x_1, x_2, x_0 \oplus 1^n)$. Then, $\tilde{h}_E^{\xi}(x_0, x_1, x_2) := (h_E(x_0, x_1, x_2), h_E(\xi(x_0, x_1, x_2)) \oplus 1^n)$ represents the abreast Davies-Meyer (DM) DBL compression function proposed by Lai and Massey [10]. It is depicted in Fig. 1(a), where the operation '∘' is bitwise negation. Though $\xi$ is not an involution, $\xi^6$ is the identity permutation and, for every $x_0 \in \{0,1\}^n$,



(a) Unitary operator of $E$

(b) Flip the target qubit if $u = c$

**Fig. 3** Components of the Grover oracle in Fig. 2.

$\xi(x_0, x_0 \oplus 1^n, x_0) = (x_0 \oplus 1^n, x_0, x_0 \oplus 1^n) \neq (x_0, x_0 \oplus 1^n, x_0)$ and $\xi^2(x_0, x_0 \oplus 1^n, x_0) = (x_0, x_0 \oplus 1^n, x_0)$. Thus, $(x_0, x_0 \oplus 1^n, x_0)$ and $\xi(x_0, x_0 \oplus 1^n, x_0)$ are colliding pair of inputs for $\tilde{h}_E^{\xi}$ if and only if

$$h_E(x_0, x_0 \oplus 1^n, x_0) = h_E(\xi(x_0, x_0 \oplus 1^n, x_0)). \qquad (1)$$

If there exists $x_0$ satisfying Eq. (1) for $E$, then one can find a colliding pair of inputs for the abreast Davies-Meyer $\tilde{h}_E^{\xi}$ using the Grover search with $O(2^{n/2})$ iterations. The Grover search is applied to the Boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x_0) = 1$ if and only if $x_0$ satisfies Eq. (1). Eq. (1) holds if and only if $E((x_0, x_0 \oplus 1^n), x_0) = E((x_0 \oplus 1^n, x_0), x_0 \oplus 1^n) \oplus 1^n$. The number of unordered pairs, $((x_0, x_0 \oplus 1^n), x_0))$ and $((x_0 \oplus 1^n, x_0), x_0 \oplus 1^n)$, is $2^{n-1}$ for $x_0 \in \{0,1\}^n$. Suppose that $E$ is chosen uniformly at random. Then, the probability that there exists $x_0$ satisfying Eq. (1) is $1 - (1 - 2^{-n})^{2^{n-1}} \approx 1 - \mathrm{e}^{-1/2} \approx 0.3935$.

### 6.3 The Jonsson-Robshaw Construction

Let $\delta$ be a permutation over $\{0,1\}^n$ applying addition of 1 modulo 4 to the two most significant bits of an input. Then, $\hat{h}_E^{\delta}(x_0, x_1, x_2) := (E((x_0, x_1), x_2) \oplus x_2, E((x_0, x_1), \delta(x_2)) \oplus x_2)$ represents the DBL compression function proposed by Jonsson and Robshaw [26], which is depicted in Fig. 1(b).

Addition of 1 modulo 4 to $(b_1, b_0) \in \{0,1\}^2$ can be represented by a permutation shown in Example 1: $(b_1, b_0) \mapsto (b_1 \oplus b_0, b_0 \oplus 1)$. Thus, $\delta$ satisfies the sufficient condition for optimal quantum collision resistance. However, it is still an open question if $\hat{h}_E^{\delta}$ is optimally collision resistant against quantum adversaries in the ideal cipher model.

## 7. Conclusion

We have analyzed the quantum collision resistance of Nandi's class of compression functions $h^{\pi}$ and the Merkle-Damgård hash functions $\mathsf{MD}^{h^{\pi}}$ assuming that $h$ is a random oracle. Though our analysis has covered some permutations $\pi$ of practical interest, it leaves the quantum collision resistance for the other permutations as an open question. It is also an open question if there exists an optimally collision resistant DBL compression function using a block cipher against quantum adversaries in the ideal cipher model.

## Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP20K21798 and JP22K11914.

### References

[1] FIPS PUB 180-4, "Secure hash standard (SHS)," Aug. 2015.

[2] R.C. Merkle, "One way hash functions and DES," Advances in Cryptology - CRYPTO'89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, Aug. 1989, Proceedings, G. Brassard, ed., Lecture Notes in Computer Science, vol.435, pp.428–446, Springer, 1989.

[3] I. Damgård, "A design principle for hash functions," Advances in Cryptology - CRYPTO'89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, Aug. 1989, Proceedings, G. Brassard, ed., Lecture Notes in Computer Science, vol.435, pp.416–427, Springer, 1989.

[4] C.H. Meyer and M. Schilling, "Secure program load with manipulation detection code," Proc. 6th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM '88), pp.111–130, 1988.

[5] ISO/IEC 10118-2, "Information technology – security techniques – hash-functions – part 2: Hash-functions using an $n$-bit block cipher," 2010.

[6] M. Nandi, "Towards optimal double-length hash functions," Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, Dec. 2005, Proceedings, S. Maitra, C.E.V. Madhavan, and R. Venkatesan, eds., Lecture Notes in Computer Science, vol.3797, pp.77–89, Springer, 2005.

[7] L.K. Grover, "A fast quantum mechanical algorithm for database search," Proc. Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May1996, G.L. Miller, ed., pp.212–219, ACM, 1996.

[8] M. Zhandry, "How to record quantum queries, and applications to quantum indifferentiability," Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, Aug. 2019, Proceedings, Part II, A. Boldyreva and D. Micciancio, eds., Lecture Notes in Computer Science, vol.11693, pp.239–268, Springer, 2019.

[9] Q. Liu and M. Zhandry, "On finding quantum multi-collisions," Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 2019, Proceedings, Part III, Y. Ishai and V. Rijmen, eds., Lecture Notes in Computer Science, vol.11478, pp.189–218, Springer, 2019.

[10] X. Lai and J.L. Massey, "Hash function based on block ciphers," Advances in Cryptology - EUROCRYPT'92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 1992, Proceedings, R.A. Rueppel, ed., Lecture Notes in Computer Science, vol.658, pp.55–70, Springer, 1992.

[11] S. Hirose, "Some plausible constructions of double-block-length hash functions," Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 2006, Revised Selected Papers, M.J.B. Robshaw, ed., Lecture Notes in Computer Science, vol.4047, pp.210–225, Springer, 2006.

[12] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: Quantum resource estimates," Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, Feb. 2016, Proceedings, T. Takagi, ed., Lecture Notes in Computer Science, vol.9606, pp.29–43, Springer, 2016.

[13] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Crypto-

graphic Techniques, Zagreb, Croatia, May 2020, Proceedings, Part II, A. Canteaut and Y. Ishai, eds., Lecture Notes in Computer Science, vol.12106, pp.280–310, Springer, 2020.

[14] S. Hirose and H. Kuwakado, "A note on quantum collision resistance of double-block-length compression functions," Cryptography and Coding - 18th IMA International Conference, IMACC 2021, Virtual Event, Dec. 2021, Proceedings, M.B. Paterson, ed., Lecture Notes in Computer Science, vol.13129, pp.161–175, Springer, 2021.

[15] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," SIGACT News, vol.28, no.2, pp.14–19, 1997.

[16] M. Zhandry, "A note on the quantum collision and set equality problems," Quantum Information & Computation, vol.15, no.7&8, pp.557–567, 2015.

[17] A.K. Chauhan, A. Kumar, and S.K. Sanadhya, "Quantum free-start collision attacks on double block length hashing with round-reduced AES-256," IACR Transactions on Symmetric Cryptology, vol.2021, no.1, pp.316–336, 2021.

[18] X. Dong, S. Sun, D. Shi, F. Gao, X. Wang, and L. Hu, "Quantum collision attacks on AES-like hashing with low quantum random access memories," Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, Dec. 2020, Proceedings, Part II, S. Moriai and H. Wang, eds., Lecture Notes in Computer Science, vol.12492, pp.727–757, Springer, 2020.

[19] A. Hosoyamada and Y. Sasaki, "Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound," Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 2020, Proceedings, Part II, A. Canteaut and Y. Ishai, eds., Lecture Notes in Computer Science, vol.12106, pp.249–279, Springer, 2020.

[20] F. Mendel, C. Rechberger, M. Schläffer, and S.S. Thomsen, "The rebound attack: Cryptanalysis of reduced Whirlpool and Grøstl," Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, Feb. 2009, Revised Selected Papers, O. Dunkelman, ed., Lecture Notes in Computer Science, vol.5665, pp.260–276, Springer, 2009.

[21] F. Berti, C. Guo, O. Pereira, T. Peters, and F. Standaert, "TEDT, a leakage-resistant AEAD mode for high physical security applications," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol.2020, no.1, pp.256–320, 2020.

[22] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin, "New results on Romulus," NIST Lightweight Cryptography Workshop 2020, 2020. https://csrc.nist.gov/events/2020/lightweight-cryptography-workshop-2020

[23] J. Black, P. Rogaway, and T. Shrimpton, "Black-box analysis of the block-cipher-based hash-function constructions from PGV," Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, Aug. 2002, Proceedings, M. Yung, ed., Lecture Notes in Computer Science, vol.2442, pp.320–335, Springer, 2002.

[24] M. Nandi, "Characterizing padding rules of MD hash functions preserving collision security," Information Security and Privacy, 14th Australasian Conference, ACISP 2009, Brisbane, Australia, July 2009, Proceedings, C. Boyd and J.M.G. Nieto, eds., Lecture Notes in Computer Science, vol.5594, pp.171–184, Springer, 2009.

[25] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[26] J. Jonsson and M.J.B. Robshaw, "Securing RSA-KEM via the AES," Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, Jan. 2005, Proceedings, S. Vaudenay, ed., Lecture Notes in Computer Science, vol.3386, pp.29–46, Springer, 2005.

**Shoichi Hirose** received the B.E., M.E. and D.E. degrees in information science from Kyoto University, Kyoto, Japan, in 1988, 1990 and 1995, respectively. From 1990 to 1998, he was a research associate at Faculty of Engineering, Kyoto University. From 1998 to 2005, he was a lecturer at Graduate School of Informatics, Kyoto University. From 2005 to 2009, he was an associate professor at Faculty of Engineering, University of Fukui. From 2009, he is a professor at Graduate School of Engineering, University of Fukui. His research interests include cryptography and information security. He received Young Engineer Award from IEICE in 1997, and KDDI Foundation Research Award in 2008.

**Hidenori Kuwakado** received the B.E., M.E. and D.E. degrees from Kobe University in 1990, 1992, and 1999 respectively. He worked for Nippon Telegraph and Telephone Corporation from 1992 to 1996. From 1996 to 2002, he was a research associate in the Faculty of Engineering, Kobe University. From 2002 to 2007, he was an associate professor in the Faculty of Engineering, Kobe University. From 2007 to 2013, he was an associate professor in Graduate School of Engineering, Kobe University. Since 2013, he has been a professor in Faculty of Informatics, Kansai University. His research interests are in cryptography and information security.