Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions

Akinori Hosoyamada and Kan Yasuda

NTT Secure Platform Laboratories,
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan.
{hosoyamada.akinori,yasuda.kan}@lab.ntt.co.jp

Abstract. We present hash functions that are almost optimally one-way in the quantum setting. Our hash functions are based on the Merkle-Damgård construction iterating a Davies-Meyer compression function, which is built from a block cipher. The quantum setting that we use is a natural extention of the classical ideal cipher model. Recent work has revealed that symmetric-key schemes using a block cipher or a public permutation, such as CBC-MAC or the Even-Mansour cipher, can get completely broken with quantum superposition attacks, in polynomial time of the block size. Since many of the popular schemes are built from a block cipher or a permutation, the recent findings motivate us to study such schemes that are provably secure in the quantum setting. Unfortunately, no such schemes are known, unless one relies on certain algebraic assumptions. In this paper we present hash constructions that are provably one-way in the quantum setting without algebraic assumptions, solely based on the assumption that the underlying block cipher is ideal. To do this, we reduce one-wayness to a problem of finding a fixed point and then bound its success probability with a distinguishing advantage. We develop a generic tool that helps us prove indistinguishability of two quantum oracle distributions.

keywords symmetric key cryptography, provable security, Merkle-Damgård, Davies-Meyer, one-wayness, non-invertibility, preimage-resistance, derangement, fixed point, indistinguishability, quantum ideal cipher model

1 Introduction

The epoch-making work by Shor [26] revealed that widely used cryptographic schemes such as RSA, DSA and ECDSA would become insecure when a practical quantum computer becomes available. Since then, researchers have become increasingly interested in so-called *post-quantum* cryptography. Today there exist several schemes that claim to provide post-quantum security. Some of them are based on computational problems that are seemingly hard to solve even with quantum computers, like the lattice-based cryptography based on the shortest vector problem or its variants. Others are based on the assumption that there exist post-quantum-secure symmetric-key primitives, e.g. digital signatures based on one-way hash functions.

Two Levels of Post-Quantum Security. There are two notions of security against adversaries with quantum computers: *standard* security and *quantum* security [34]. In this paper we focus on the quantum security, because it is stronger. In the standard-security setting we assume that adversaries have quantum computers but can make only classical queries to the oracles. On the other hand, in the quantum-security setting, adversaries are allowed to make quantum superposition queries. In other words, that a scheme provides quantum security means that it will remain secure even in the far future when all computations and communications are done in quantum superposition states.

Post-Quantum Insecurity of Symmetric-Key Constructions. On the negative side, it has turned out that a number of symmetric-key constructions as well as many public-key schemes can be broken in polynomial time (of the block size) if adversaries are allowed to make quantum superposition queries. For example, such adversaries can distinguish 3-round Feistel ciphers from random [19], recover keys of Even-Mansour ciphers [20], forge various message authentication codes like CBC-MAC [17], by making only polynomially many queries. These attacks tell us that in general there is no guarantee that the classical security of a symmetric-key scheme implies its quantum security.

Quantum-Secure Schemes based on One-Way Functions. On the positive side, previous work [34,8,27] has shown that, if we assume the existence of one-way functions that are hard to invert even with quantum computers, then we can come up with a wide range of quantum-secure schemes. These include pseudo-random functions, message authentication codes, universal one-way hash functions, one-time signatures, and EU-CMA signature schemes. Thus, the existence of quantum-secure one-way functions is fundamental, just as in the classical setting, and the cryptographic hash functions in use like SHA-3 [23] and SHA-2 [22] are considered to be possible candidates also for the instantiation of these quantum-secure one-way functions.

Cryptographic Hash Functions Revisited. Recall that cryptographic hash functions are normally constructed only with public, "keyless" primitives, either from a public permutation or a block cipher having no secret keys (i.e. key inputs are public). For example, SHA-3 is constructed from a public permutation, and SHA-2 is essentially based on a public block cipher. The generic security (indifferentiability) of the sponge construction used in SHA-3 is proven in the random permutation model, and the security (one-wayness and collision resistance) of Davies-Meyer construction adopted by the SHA-2 compression function is proven in the ideal cipher model.

However, as mentioned above, we should carefully note that the classical provable security of these hash functions may not carry over to the quantum setting. For example, recently Carstens et al. [10] gave an evidence that SHA-3 is not indifferentiable in the quantum setting, based on a conjecture. There-

fore, here we would like to pose a fundamental question: do we have a provably quantum-secure construction of one-way hash functions?

1.1 Our Contributions

Our answer is positive; in this paper we show that the Merkle-Damgård iteration with the Davies-Meyer compression function is a quantum-secure one-way hash function. This has been a popular design used in MD5, SHA-1 and SHA-2. Indeed, our construction is essentially identical to the modes of operation used in these traditional hash functions, except for minor differences in padding rules, initialization vectors, and input-size restrictions on the underlying block cipher.

Our contributions come in three steps. First, we fix a security model in which we prove our main result. Second, we develop a generic tool for bounding quantum oracle indistinguishability. Finally, we use the tool to prove our main result.

1. **Introducing the Quantum Ideal Cipher Model.** As the first step we introduce the *quantum ideal cipher* model, which, as the name suggests, naturally extends the ideal cipher model in the classical setting. Similarly to the classical case, we treat the underlying block cipher as an ideal cipher E, i.e., E_k is a random permutation for each key k. We then allow quantum adversaries to make both forward and backward queries to the cipher. In our model, a table of all values for the ideal cipher E is determined at the beginning of each game, and the oracle that computes $E_{(\cdot)}(\cdot)$ and $E^{-1}_{(\cdot)}(\cdot)$ are given to the adversary. Following the style of previous work in the classical setting, we consider (quantum) information-theoretic adversaries that have no limitation on computational resources, such as time or the number of available qubits. We only bound the number q of queries that the adversary makes to its oracles.
2. **A Generic Tool for Quantum Indistinguishability.** The second step is to develop a proof tool to upper-bound quantum oracle distinguishing advantages. The tool can be applied to any pair (D_1, D_2) of distributions on an arbitrary (finite) set of functions (Proposition 3.1.) The tool enables us to obtain an upper bound by mere combinatorial enumeration and associated probability computations. There is a simplified version of the tool corresponding to the special case when D_1 and D_2 are distributions on a set of boolean functions (having some fixed domain size) with D_2 being a degenerate distribution at the zero function (Proposition 3.2.) In fact this simplified version suffices to prove our main result. Our tool is developed by generalizing and integrating several existing techniques [6,28,2,16] corresponding to some limited cases of the simplified version. However, previous work treats only the case that D_1 is some specific distributions, and no previous work seems suitable to our situation. We developed our tool so that it looks familiar to researchers on symmetric-key provable security (like coefficient-H technique).
3. **One-Wayness of Merkle-Damgård with Davies-Meyer.** The final but main contribution of this paper is to give almost optimal security bound for

quantum one-wayness of the Merkle-Damgård construction with a Davies-Meyer compression function. That is, any quantum query adversary needs to make about $2^{n/2}$ queries to invert the function with n-bit output. This bound is almost optimal since the Grover search can find a preimage of random functions with $O(2^{n/2})$ quantum queries, and it is proven that the Grover search is optimal strategy to find a preimage of random functions [16]. In our proof, the input length of functions can be exponentially long but must be fixed. We stress that this is the first proof for quantum security on symmetric key schemes based on public block ciphers.

Technical Details. In this paper we give exact security bounds without any asymptotic notation, because security parameters of symmetric-key schemes are usually fixed to some constant.

This paper considers two security notions: non-invertibility and one-wayness. When we say $h : \{0,1\}^s \to \{0,1\}^n$ has one-wayness, we mean that any adversary cannot find a preimage of $y = h(x)$, where x is randomly chosen from $\{0,1\}^s$. [1] On the other hand, when we say h has non-invertibility, we mean that any adversary cannot find a preimage of y, where y is randomly chosen from $\{0,1\}^n$. These are similar but independent notions.

We firstly show non-invertibility of permutation with feedforward in the quantum ideal permutation model, secondly show both non-invertibility and one-wayness of Davies-Meyer constructions, and finally show both non-invertibility and one-wayness of Merkle-Damgård constructions. It might be unexpected that permutation with feedforward is non-invertible in the quantum setting although it uses only public permutation and XOR operation, which seems similar to the Even-Mansour ciphers that are broken by quantum superposition attacks.

Due to a technical reason, we need some restriction on usage of keys in Davies-Meyer construction. Similarly, we need a padding function for Merkle-Damgård construction. However, these do not mean restriction on available block ciphers. As a subsidiary result, we also show that any quantum query adversary needs to make about $2^{n/2}$ queries to find a fixed point of a public random permutation (which allow adversaries to make both forward and backward quantum queries). This is the first result on quantum query lower bound for a property related to public random permutations.

Our proof strategy is to reduce the problem of breaking security notions to the problem of distinguishing oracle distributions on boolean functions. A similar strategy can be found in [16]. Then indistinguishability between quantum oracle distributions is shown using our new proof tool described above. To reduce problems on public random permutations to problems on boolean functions, we try to approximate the uniform distribution on random permutations by combining distributions on boolean functions with the uniform distribution on derangements (permutations without fixed points).

[1] This security notion is also called *preimage resistance* (see [25] for example).

1.2 Related Work

There already exist powerful tools that aim to give quantum security bounds for cryptographic schemes. These tools include "one-way to hiding" lemma and quantum random oracle programming by Unruh [30,29], the rank method and oracle indistinguishability frameworks by Zhandry [34,35,8]. These tools do not seem to consider the situation where adversaries can make both forward and backward queries to public permutations or block ciphers. There exists previous work [1] that proves quantum security of Even-Mansour ciphers in a model where adversaries make both forward and backward queries to the underlying permutation, but it should be noted that the proof [1] requires a quantum computational hardness assumption (the hidden shift problem.)

A quantum version of the random oracle model is proposed by Boneh et al, [7], and many schemes are proven to be secure in this model ([35,29], for example). Regarding symmetric key schemes, several papers on quantum security already exist. They include work on quantum security of Carter-Wegman MACs [8], quantum PRP-PRF switching lemma [36], quantum security of the CBC, OFB, CTR, and XTS modes of operation [4], quantum generic security of random hash functions [16], and quantum security of NMAC [28]. With a computational assumption that *hidden shift problem* is hard to solve even with quantum computers, it is shown that Even-Mansour ciphers and CBC-MAC, which are broken in polynomial time with quantum queries, can be modified to have quantum security [1]. For standard security, i.e., with the assumption that adversaries have quantum computers but can make only classical queries, XOR of PRPs are proven to be secure [21]. Unruh introduced a security notion named *collapsing*, which is a generalized notion of collision-resistant in the quantum setting [32]. Unruh showed that Merkle-Damgård constructions are collapsing if underlying constructions are collapsing [31]. Czajkowski et al. showed that sponge constructions are also collapsing [11] (Note that they assume building permutations are one-way permutations or functions, and do not treat the usual sponge functions that are constructed from public permutations). Recently Zhandry [33] showed indifferentiability of the Merkle-Damgård construction in the quantum random oracle model (compression functions are assumed to be random functions).

2 Preliminaries

In this section we describe notation and definitions. For readers who are not familiar with quantum terminology, a brief explanation on quantum computation is given in this paper's full version [15].

Notation. Let $[i, \ldots, j]$ denote the set of integers $\{i, i+1, \ldots, j\}$ for $i < j$, and $[N]$ denote the set $[1, \ldots, N]$. For sets X and Y, let $\mathsf{Func}(X, Y)$ be the set of functions from X to Y. For a set X, let $\mathsf{Perm}(X)$ be the set of permutations

on X. Let $\mathsf{Ciph}(m,n)$ denote the set

$$\{E \in \mathsf{Func}(\{0,1\}^m \times \{0,1\}^n, \{0,1\}^n) \mid E(k,\cdot) \in \mathsf{Perm}(\{0,1\}^n) \text{ for each } k\},$$

where "$\cdot$" means arbitrary inputs.

We call an element of $\mathsf{Ciph}(m,n)$ an *n-bit block cipher* with an m-bit key. For each $E \in \mathsf{Ciph}(m,n)$ and $k \in \{0,1\}^m$, let E_k denote the permutation $E(k,\cdot)$. For a distribution D, let $\Pr_{x\sim D}[\mathsf{event}]$ denote the probability that event occurs when x is sampled according to the distribution D. For two distributions D_1 and D_2, let $\Delta(D_1,D_2)$ denote the total variation distance D_1 and D_2. Let $\mathsf{td}(\rho_1,\rho_2)$ denote the trace distance between density matrices ρ_1 and ρ_2. For a random variable V that takes values in a set X, define a distribution $D_V : X \to [0,1]$ by $D_V(x) = \Pr[V = x]$ for each $x \in X$. We call D_V the distribution of V. If we write $x \xleftarrow{D} X$, then it means to sample x according to the distribution D on X.

Derangements. A permutation $P_0 \in \mathsf{Perm}(X)$ is called a *derangement* if P_0 has no fixed point, i.e. if there is no element $x \in X$ such that $P_0(x) = x$. The set of derangements on a set X is denoted as $\mathsf{Der}(X)$. The number of derangements on a set of size N is written as $!N$. The following formula is well-known [14]:

Lemma 2.1. *We have* $!N = N! \cdot \sum_{i=0}^{N} \frac{(-1)^i}{i!} = \left\lfloor \frac{N!}{e} + \frac{1}{2} \right\rfloor$, *where* $\lfloor\cdot\rfloor$ *is the floor function.*

A proof of this lemma is given in this paper's full version [15].

Davies-Meyer and Merkle-Damgård Constructions. For an n-bit block cipher E with an m-bit key, we define a function $\mathsf{DM}^E \in \mathsf{Func}(\{0,1\}^m \times \{0,1\}^n, \{0,1\}^n)$ by $\mathsf{DM}^E(z,x) = E_z(x) \oplus x$. We call DM^E the *Davies-Meyer construction* made from $E \in \mathsf{Ciph}(m,n)$. For a permutation $P \in \mathsf{Perm}(\{0,1\}^n)$, we define a function $\mathsf{FF}^P \in \mathsf{Func}(\{0,1\}^n)$ by $\mathsf{FF}^P(x) := P(x) \oplus x$. We call the function FF^P as *permutation P with feedforward*. The function FF can be regarded as a "fixed-key" version of DM.

For a function $h : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ and an integer $\ell > 0$, the *Merkle-Damgård construction* $\mathsf{MD}^h_\ell : \{0,1\}^n \times \{0,1\}^{m\ell} \to \{0,1\}^n$ is defined by

$$\mathsf{MD}^h_\ell(x, z_1, \ldots, z_\ell) := h(z_\ell, h(z_{\ell-1}, \cdots, h(z_2, h(z_1, x)) \cdots), \tag{1}$$

where $z_i \in \{0,1\}^m$ for each i. We consider the special case when h is the Davies-Meyer compression function, i.e., $h(z,x) = \mathsf{DM}^E(z,x)$ for an n-bit block cipher $E \in \mathsf{Ciph}(m,n)$. Fig. 1 illustrates $\mathsf{MD}^{\mathsf{DM}^E}_\ell$, the combination of a Davies-Meyer compression function with the Merkle-Damgård iteration.

Quantum oracles and quantum adversaries. For a function $f \in \mathsf{Func}(\{0,1\}^a, \{0,1\}^b)$, quantum oracle of f is defined as the unitary operator O_f such that $O_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$ for arbitrary $x \in \{0,1\}^a, y \in \{0,1\}^b$. By an abuse of

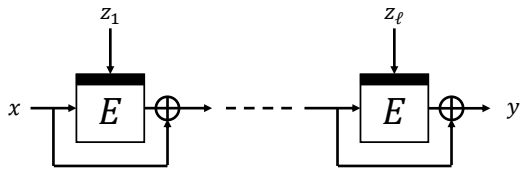

Fig. 1. The Merkle-Damgård construction with a Davies-Meyer compression function

notation, let O_f also denote the $(a+b+c)$-qubit unitary operator $O_f \otimes I_c$ that maps $|x\rangle |y\rangle |z\rangle$ to $|x\rangle |y \oplus f(x)\rangle |z\rangle$ for any c.

This paper discusses on information theoretic quantum query adversary. That is, we fix a constant q and assume that a quantum adversary $\mathcal{A}$ can make at most q quantum queries, but we assume no other limitation for $\mathcal{A}$ about quantum computational resources such as time or the number of available qubits. Following the previous works that treat quantum oracle query adversary ([5,7,35,34,8,28], for example), we model $\mathcal{A}$ as a sequence of unitary operators $U_q O_f U_{q-1} \cdots O_f U_0$. We write $\mathcal{A}^O(x) = y$ for the event that a quantum adversary $\mathcal{A}$ takes x as input, makes quantum queries to O, and finally outputs y.

If quantum oracle O is dependent on some distribution, then the state of a quantum query algorithm $\mathcal{A}$ is described as a density operator. Suppose $O = O_f$ for a function f, which is sampled according to a distribution D_1 on $\mathsf{Func}(\{0,1\}^a, \{0,1\}^b)$. Then, the state of $\mathcal{A}$ with input x after the i-th query becomes $|\phi_f^i\rangle := U_i O_f U_{i-1} O_f \cdots O_f U_0 |0, x, 0\rangle$ with probability $p_1^f := \Pr_{F \sim D_1}[F = f]$. This mixed state is described as

$$\rho_1^i = \sum_f p_1^f |\phi_f^i\rangle \langle \phi_f^i| . \tag{2}$$

Quantum oracle distinguishing advantage. Following previous works (see [34], for example), we define quantum oracle distinguishing advantage as follows. Let D_1, D_2 be two distributions on a set of functions. Assume that a quantum algorithm $\mathcal{A}$ is allowed to access the quantum oracle of a function that is chosen according to either D_1 or D_2. Suppose $\mathcal{A}$ can make at most q queries, and finally outputs the result 1 or 0. Then, we define the distinguishing advantage of $\mathcal{A}$ by

$$\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A}) := \left| \Pr_{f \sim D_1}[\mathcal{A}^{O_f}() = 1] - \Pr_{g \sim D_2}[\mathcal{A}^{O_g}() = 1] \right| .$$

In addition, we define

$$\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(q) := \max_{\mathcal{A}} \left\{ \mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A}) \right\},$$

where the maximum is taken over all quantum-query algorithms, each making at most q quantum queries.

Distinguishing advantages can be bounded by the trace distance and total variational distance. Let ρ_1^i be the density operator defined by (2), and ρ_2^i be the density operator that is similarly defined according to the distribution D_2. Then we can show the following lemma:

Lemma 2.2. *For any quantum algorithm $\mathcal{A}$ that makes at most q queries,*

$$\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A}) \leq \mathsf{td}(\rho_1^q, \rho_2^q) \tag{3}$$

and

$$\mathsf{td}(\rho_1^q, \rho_2^q) \leq \Delta(D_1, D_2) \tag{4}$$

hold.

The inequality (4) trivially follows from definitions and the proof of inequality (3) is also straightforward, but a proof of the lemma is given in this paper's full version [15] for readers who are not used to quantum computation.

2.1 Modeling Public Random Permutations and Block Ciphers in the Quantum Setting

To model public ideal permutations and block ciphers, here we introduce quantum ideal permutation model and quantum ideal cipher model, which are quantum versions of the classical ideal permutation model and ideal cipher model, respectively. There already exist works on quantum provable security [1] in the models that are essentially same to our quantum random permutation model. However, this is the first paper on provable security that treats ideal cipher model in the quantum setting. We begin with formalizing quantum oracles of public permutations and block ciphers, and then introduce quantum ideal permutation model and quantum ideal cipher model.

Quantum oracles of public permutations and ciphers. Here we describe how to formalize quantum oracles of public permutations and block ciphers. For an n-bit public permutation P, we define a function $P^{\pm} : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ by

$$P^{\pm}(b,x) = \begin{cases} P(x) & \text{if } b = 0, \\ P^{-1}(x) & \text{if } b = 1. \end{cases}$$

For a distribution D on $\mathsf{Perm}(\{0,1\}^n)$, let $D^{\pm}$ be the associated distribution on $\mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$ defined by $D^{\pm}(f) = \Pr_{P \sim D}[P^{\pm} = f]$. For any public permutation P, we assume that the quantum oracle $O_{P^{\pm}}$ is available. This models the situation that both of forward and backward quantum queries to the public permutation P are allowed.

Similarly, if E is an n-bit block cipher with m-bit key, then we define a function $E^{\pm} : \{0,1\} \times \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ by

$$E^{\pm}(b,k,x) = \begin{cases} E_k(x) & \text{if } b = 0, \\ E_k^{-1}(x) & \text{if } b = 1. \end{cases}$$

For a distribution D on $\mathsf{Ciph}(m,n)$, let $D^{\pm}$ be the associated distribution on $\mathsf{Func}(\{0,1\}\times\{0,1\}^m\times\{0,1\}^n,\{0,1\}^n)$ defined by $D^{\pm}(f)=\Pr_{E\sim D}[E^{\pm}=f]$. For any public block cipher E, we assume that the quantum oracle $O_{E^{\pm}}$ is available. This models the situation that both of forward and backward quantum queries to a block cipher E are allowed.

Quantum ideal permutation model. Assume that P is a public permutation which is chosen from $\mathsf{Perm}(\{0,1\}^n)$ uniformly at random, and an adversary $\mathcal{A}$ is allowed to make at most q quantum queries to $P^{\pm}$, for some fixed number q. We call this model as *quantum ideal permutation model*. We say that a scheme constructed from a public permutation is secure (with regard to some quantum security notion) up to q quantum queries if no such quantum information theoretic adversary can break the security notion. We say that P is an ideal permutation if we assume the situation that quantum adversaries can access quantum oracle of P, and P is chosen from $\mathsf{Perm}(\{0,1\}^n)$ uniformly at random.

Quantum ideal cipher model. Assume that E is a public block cipher which is chosen from $\mathsf{Ciph}(m,n)$ uniformly at random, and an adversary $\mathcal{A}$ is allowed to make at most q quantum queries to $E^{\pm}$, for some fixed number q. We call this model as *quantum ideal cipher model*. Security in this model is defined similarly as in the quantum ideal permutation model. Similarly, we say that E is an ideal cipher if we assume the situation that quantum adversaries can access quantum oracle of E, and E is chosen from $\mathsf{Ciph}(m,n)$ uniformly at random.

2.2 Two Security Notions of : Non-Invertibility and One-Wayness.

This paper considers two security notions: non-invertibility and one-wayness. These are similar but independent notions (we give a separation proof in this paper's full version [15] for completeness). Let $h^F : \{0,1\}^s \to \{0,1\}^n$ be a function that is constructed from a function (or permutation) F, and O be a quantum oracle that is defined depending on F. We assume F is chosen from a set of functions $\mathcal{S}_F$ uniformly at random. The set $\mathcal{S}_F$ and how the oracle O is related to F depend on security models.

If we consider the quantum ideal permutation model, then $\mathcal{S}_F=\mathsf{Perm}(\{0,1\}^n)$, and O is defined as the oracle of $P^{\pm}$. We will consider the case that h^F is a permutation with feedforward. Similarly, if we consider the quantum ideal cipher model, then $\mathcal{S}_F=\mathsf{Ciph}(m,n)$, and O is defined as the oracle of $E^{\pm}$. We will consider the case that h^F is the Davies-Meyer constructions or Merkle-Damgård constructions.

Non-invertibility. For any quantum oracle query adversary $\mathcal{A}$, define the advantage of $\mathcal{A}$ to invert the function h^F by

$$\mathsf{Adv}^{inv}_{h^F}(\mathcal{A}) := \Pr_{F,y}[\mathcal{A}^O(y)=x\wedge h^F(x)=y], \tag{5}$$

where $F \in \mathcal{S}_F$ and $y \in \{0,1\}^n$ are chosen uniformly at random. In addition, we define

$$\mathsf{Adv}^{inv}_{h^F}(q) := \max_{\mathcal{A}}\{\mathsf{Adv}^{inv}_{h^F}(\mathcal{A})\}, \tag{6}$$

where the maximum is taken over all quantum-query algorithms, each making at most q quantum queries.

One-wayness. Similarly, define the advantage of $\mathcal{A}$ to break the one-wayness of the function h^F by

$$\mathsf{Adv}^{ow}_{h^F}(\mathcal{A}) := \Pr_{F,x'}[\mathcal{A}^O(h^F(x')) = x \wedge h^F(x) = h^F(x')], \tag{7}$$

where $F \in \mathcal{S}_F$ and $x' \in \{0,1\}^s$ are chosen uniformly at random. In addition, we define

$$\mathsf{Adv}^{ow}_{h^F}(q) := \max_{\mathcal{A}}\{\mathsf{Adv}^{ow}_{h^F}(\mathcal{A})\}, \tag{8}$$

where the maximum is taken over all quantum-query algorithms, each making at most q quantum queries.

Trivial upper bounds. We note here that there are trivial upper bounds of quantum query complexity for non-invertibility and one-wayness, if h^F is sufficiently random. The bound is given by simple application of the Grover search or its generalizations [13,9]. Given y, let consider to find x such that $h^F(x) = y$. Then, if $2^s/|(h^F)^{-1}(y)| \approx 2^n$, (which is the case when h^F is a truly random function and message space $\{0,1\}^s$ is much larger than range $\{0,1\}^n$) then we can find x such that $h^F(x) = y$ with about $\sqrt{2^n}$ quantum queries to h^F. We say h^F is almost optimally non-invertible or one-way if $\mathsf{Adv}^{inv}_{h^F}(q) = \tilde{O}(q/\sqrt{2^n})$ or $\mathsf{Adv}^{ow}_{h^F}(q) = \tilde{O}(q/\sqrt{2^n})$, respectively, since these imply that there is no way which is significantly better than the generic attack (the Grover search) to break one-wayness of h^F.

3 A Tool for Quantum Oracle Indistinguishability

Here we give a tool to upper bound quantum oracle distinguishing advantages $\mathsf{Adv}^{dist}_{D_1,D_2}$ with only classical probability calculation and purely combinatorial enumeration (Proposition 3.1). Our tool can be applied to *any* distributions D_1, D_2 on *any* (finite) set of functions $\mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$. In later sections, to show non-invertibility and one-wayness of functions, we treat only the cases that $c = 1$ and D_2 is the degenerate distribution with support on the zero function. Our tool can be somewhat simplified in those cases, and thus we give a simplified version of our tool (Proposition 3.2) for later use. We believe that the generalized version (Proposition 3.1) itself is also useful to give some quantum security bound for other schemes or other security notions. To show that the generalized version is also useful, an application is given in this paper's full version [15].

There already exist techniques to bound quantum oracle distinguishing advantages in the situations which are similar to our simplified version ($c = 1$ and

D_2 is the degenerate distribution with support on the zero function), but existing works treat only the case that D_1 is some specific distributions. (See proof of Lemma 37 in [3], proof of Lemma C.1 in [28], for example. Theorem 1 in [16] gives similar result as Lemma 37 in [3], but uses different analyzing technique by Zhandry [34].) On the other hand, our simplified tool (Proposition 3.2) enables us to treat *any* distribution D_1 on a (finite) set of boolean functions.

This section is organized as follows. First, we explain our motivations to develop quantum proof tools. Second, we describe our main tool. Third, we briefly explain how to apply them to give quantum security bounds in later sections.

3.1 Motivations: the coefficient H technique

In the classical setting, there exist several proof tools to prove oracle indistinguishability of symmetric key schemes. The *coefficient-H technique* developed by Patarin [24] is one of the most powerful tools. Below we explain essence of the technique.

Suppose we want to upper bound $\mathsf{Adv}^{dist}_{D_1,D_2}(\mathcal{A})$ for a (classical) information theoretic adversary $\mathcal{A}$, and distributions D_1, D_2. The technique allows $\mathcal{A}$ to obtain *transcripts* including all input-output pairs defined by queries. Let T_1, T_2 be the transcripts that correspond to the oracle distributions D_1 and D_2, respectively. Then, $\mathsf{T}_1, \mathsf{T}_2$ define distributions on a set of transcript $\mathcal{T}$. The coefficient-H technique divides $\mathcal{T}$ into a *good* set good and *bad* set bad. Roughly speaking, the technique gives a bound $\mathsf{Adv}^{dist}_{D_1,D_2}(\mathcal{A}) \leq \epsilon + \Pr[\mathsf{T}_2 \in \mathsf{bad}]$. The parameter ϵ is a small number that satisfies $\Pr[\mathsf{T}_1 = \tau]/\Pr[\mathsf{T}_2 = \tau] \geq 1 - \epsilon$ for any good transcript $\tau \in \mathsf{good}$. How good bound we can achieve depends on how well we define the set of transcripts $\mathcal{T}$, good sets good, and bad sets bad.

3.2 Our Main tool

Following the classical coefficient-H technique, we aim to develop a quantum proof tool so that: 1. It uses some good and bad sets, and 2. It gives an upper bound as a sum of an amount related to good events (like ϵ in the coefficient-H technique), and a bad probability. In addition, we make our tool so that we can obtain an upper bound with only classical probability calculation and purely combinatorial enumeration. We first describe a generalized version that D_1 and D_2 can be any distributions, and then explain how it is simplified in the case $c = 1$ and D_2 is the degenerate distribution.

Generalized version. Let D_1, D_2 be *any* distributions on *any* (finite) set of functions $\mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$. In addition, let $\bar{D}$ be an *arbitrary* distribution on the product space $\mathsf{Func}(\{0,1\}^n, \{0,1\}^c) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$ that satisfies

$$D_1(f) = \sum_g \bar{D}(f,g) \text{ for any } f \ \wedge D_2(g) = \sum_f \bar{D}(f,g) \text{ for any } g. \tag{9}$$

(In applications, even though D_1 and D_2 are given as indipendent distributions, we try to find a convenient distribution $\bar{D}$, just like we do so in the (classical) game-playing proof technique. See this paper's full version for a concrete example.)

For each $f, g \in \mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$, let $p_1^f, p_2^g, p^{f,g}$ denote $\Pr_{F\sim D_1}[F = f]$, $\Pr_{G\sim D_1}[G = g]$, and $\Pr_{(F,G)\sim\bar{D}}[(F,G) = (f,g)]$, respectively. In addition, define a boolean function $\delta(f,g) : \{0,1\}^n \to \{0,1\}$ by $\delta(f,g)(x) = 1$ if and only if $f(x) \neq g(x)$ for each pair (f,g). Let $\mathbf{0} \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$ be the zero function that maps x to 0 for any x. For each $g \in \mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$, let $\delta D|_g$ be the conditional distribution on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$ defined by $(\delta D|_g)(\gamma) = \Pr_{(F,G)\sim\bar{D}}[\delta(F,G) = \gamma | G = g]$ for any $\gamma \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$.

For each $g \in \mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$, take a "bad" set $\mathsf{bad}^g \subset \mathsf{Func}(\{0,1\}^n, \{0,1\}) \setminus \{\mathbf{0}\}$ arbitrarily (actually we select bad^g such that $\Pr_{\Gamma\sim\delta D|_g}[\Gamma \in \mathsf{bad}^g]$ is small), and define "good" set by $\mathsf{good}^g := \mathsf{Func}(\{0,1\}^n, \{0,1\}) \setminus (\{\mathbf{0}\} \cup \mathsf{bad}^g)$. Furthermore, decompose the good set good^g into smaller subsets $\{\mathsf{good}^g_\alpha\}_{\alpha\in A_g}$ (i.e. $\mathsf{good}^g = \bigcup_\alpha \mathsf{good}^g_\alpha$ and $\mathsf{good}^g_\alpha \cap \mathsf{good}^g_\beta = \emptyset$ for $\alpha \neq \beta$) such that the conditional probability $\Pr_{\Gamma\sim\delta D|_g}[\Gamma = \gamma | \Gamma \in \mathsf{good}^g_\alpha]$ is independent of γ (in other words, for each $\alpha \in A_g$, $\Pr_{\Gamma\sim\delta D|_g}[\Gamma = \gamma] = \Pr_{\Gamma\sim\delta D|_g}[\Gamma = \gamma']$ holds for $\gamma, \gamma' \in \mathsf{good}^g_\alpha$). In addition, define $\mathsf{bad}_{all} \subset (\mathsf{Func}(\{0,1\}^n, \{0,1\}^c))^2$ by $\mathsf{bad}_{all} := \{(f,g) | \delta(f,g) \in \mathsf{bad}^g\}$. For each g, $\alpha \in A_g$ and $\gamma \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$, let $p^{\mathsf{good}^g_\alpha}_{\delta D|_g} := \Pr_{\Gamma\sim\delta D|_g}[\Gamma \in \mathsf{good}^g_\alpha]$ and $p^{\gamma|\mathsf{good}^g_\alpha}_{\delta D|_g} := \Pr_{\Gamma\sim\delta D|_g}[\Gamma = \gamma | \Gamma \in \mathsf{good}^g_\alpha]$ (by assumption, $p^{\gamma|\mathsf{good}^g_\alpha}_{\delta D|_g}$ is independent of γ). Then the following proposition holds.

Proposition 3.1 (Generalized version). *Let D_1, D_2 be any distributions on $\mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$, and $\bar{D}$ be any distribution that satisfies (9). Let bad_{all}, $\mathsf{bad}^g, \mathsf{good}^g$, and $\{\mathsf{good}^g_\alpha\}_{\alpha\in A_g}$ be the sets as stated above. Then, for any quantum algorithm $\mathcal{A}$ that makes at most q quantum queries, $\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A})$ is upper bounded by*

$$2q \cdot \mathbf{E}_{G\sim D_2}\left[\sum_{\alpha\in A_G} p^{\mathsf{good}^G_\alpha}_{\delta D|_G} \sqrt{p^{\gamma|\mathsf{good}^G_\alpha}_{\delta D|_G} \cdot \max_x \left|\{\gamma \in \mathsf{good}^G_\alpha \mid \gamma(x) = 1\}\right|}\right] + 2q \cdot \Pr_{(F,G)\sim\bar{D}}[(F,G) \in \mathsf{bad}_{all}]. \tag{10}$$

A proof of this proposition is given in this paper's full version [15].

In later sections, we apply our tool only to the cases that $c = 1$ and D_2 is the degenerate distribution with support on the zero function $\mathbf{0}$. Description of our tool can be somewhat simplified in such cases, and below we give the simplified version for later use. To show that the generalized version itself is also useful, an application of Proposition 3.1 is given in this paper's full version [15].

Simplified version. Now we describe a simplified version of our tool. Let D_1, D_2 be distributions on a set of boolean functions $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, and

D_2 be the degenerate distribution with support on the zero function $\mathbf{0}$. D_1 can be any distribution.

Take a "bad" set $\mathsf{bad} \subset \mathsf{Func}(\{0,1\}^n, \{0,1\}) \setminus \{\mathbf{0}\}$ arbitrarily (actually we select bad such that $\Pr_{F\sim D_1}[F \in \mathsf{bad}]$ will be small), and define "good" set by $\mathsf{good} := \mathsf{Func}(\{0,1\}^n, \{0,1\}) \setminus (\{\mathbf{0}\} \cup \mathsf{bad})$. Furthermore, decompose the good set good into smaller subsets $\{\mathsf{good}_\alpha\}_\alpha$ (i.e. $\mathsf{good} = \bigcup_\alpha \mathsf{good}_\alpha$ and $\mathsf{good}_\alpha \cap \mathsf{good}_\beta = \emptyset$ for $\alpha \neq \beta$) such that the conditional probability $\Pr_{F\sim D_1}[F = f | F \in \mathsf{good}_\alpha]$ is independent of f (in other words, for each α, $\Pr_{F\sim D_1}[F = f] = \Pr_{F\sim D_1}[F = f']$ holds for $f, f' \in \mathsf{good}_\alpha$). Let $p_1^{\mathsf{good}_\alpha} := \Pr_{F\sim D_1}[F \in \mathsf{good}_\alpha]$ and $p_1^{f|\mathsf{good}_\alpha} := \Pr_{F\sim D_1}[F = f | F \in \mathsf{good}_\alpha]$ (by assumption, $p_1^{f|\mathsf{good}_\alpha}$ is independent of f). Then, the following proposition holds, which enables us to bound advantages of quantum adversaries with only classical probability calculations and purely combinatorial enumeration, without any quantum arguments.

Proposition 3.2 (Simplified version). *Let D_1 be any distribution on the set of boolean functions $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, and D_2 be the degenerate distribution with support on the zero function. Let $\mathsf{bad}, \mathsf{good}$, and $\{\mathsf{good}_\alpha\}_\alpha$ be the subsets of $\mathsf{Func}(\{0,1\}^n, \{0,1\})$ as stated above. Then, for any quantum algorithm $\mathcal{A}$ that makes at most q quantum queries, $\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A})$ is upper bounded by*

$$2q \sum_\alpha p_1^{\mathsf{good}_\alpha} \sqrt{p_1^{f|\mathsf{good}_\alpha} \cdot \max_x |\{f \in \mathsf{good}_\alpha \mid f(x) = 1\}|} + 2q \Pr_{F\sim D_1}[F \in \mathsf{bad}]. \tag{11}$$

This proposition follows as an immediate corollary of the generalized version Proposition 3.1 as below.

Proof (of Proposition 3.2). Now, D_1 and D_2 are distributions on a set of boolean functions $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, and D_2 is the degenerate distribution with support on the zero function $\mathbf{0}$. Let bad, good, and $\{\mathsf{good}_\alpha\}_\alpha$ be the sets in Proposition 3.2.

We translate notations in Proposition 3.2 to those in Proposition 3.1. Let $\bar{D}$ be the product distribution $D_1 \times D_2$. Let $\mathsf{bad}^g := \emptyset$, $\mathsf{good}^g_\alpha := \mathsf{Func}(\{0,1\}^n, \{0,1\}) \setminus \{\mathbf{0}\}$ for $g \neq \mathbf{0}$, and $\mathsf{bad}^{\mathbf{0}} := \mathsf{bad}$, $\mathsf{good}^{\mathbf{0}}_\alpha := \mathsf{good}_\alpha$.

Then, $\delta(f, \mathbf{0}) = f$ holds for any boolean function f, $\Pr_{G\sim D_2}[G = g] = 1$ holds if and only if $g = \mathbf{0}$, and $\delta D|_{\mathbf{0}} = D_1$ holds. In addition, we have $p^{\mathsf{good}^{\mathbf{0}}_\alpha}_{\delta D|_{\mathbf{0}}} = p_1^{\mathsf{good}_\alpha}$, and $p^{f|\mathsf{good}^{\mathbf{0}}_\alpha}_{\delta D|_{\mathbf{0}}} = p_1^{f|\mathsf{good}_\alpha}$ for any boolean function f. Moreover, $\mathsf{bad}_{all} = \{(f, \mathbf{0}) | f \in \mathsf{bad}^{\mathbf{0}}\}$ holds, which implies that $\Pr_{(F,G)\sim\bar{D}}[(F, G) \in \mathsf{bad}_{all}] = \Pr_{F\sim D_1}[F \in \mathsf{bad}]$. Therefore Proposition 3.2 follows from Proposition 3.1. □

Remark 3.1. We do not claim that our tool is all-around. Actually the condition that the probability $p^{\gamma|\mathsf{good}^g_\alpha}_{\delta D|_g}$ is independent of γ (in the generalized version) and $p_1^{f|\mathsf{good}_\alpha}$ is independent of f (in the simplified version) implicitly means that D_1 must have some "uniform" structure to obtain a good bound with our tool. See proofs of Lemma 4.3 and Lemma 5.1 for concrete examples.

3.3 How to give quantum security bound with our tool

Next, we describe how we apply Proposition 3.2 in later sections to give quantum security bounds, in a high-level fashion. Roughly speaking, we try to reduce a target problem to a problem of bounding distinguishing advantage between two distributions on a set of boolean functions, and then apply Proposition 3.2. This strategy itself is not new, but we believe our tool enables us to take the strategy for wider applications.

Let $\mathcal{A}$ be a quantum query algorithm, and suppose that a problem to give a security proof is reduced to a problem to upper bound some distinguishing advantage $\mathsf{Adv}^{\mathsf{dist}}_{G_{\mathsf{real}},G_{\mathsf{ideal}}}(\mathcal{A})$. We introduce intermediate distributions (i.e. intermediate games) $G_1 = G_{\mathsf{ideal}}, G_2, \ldots, G_t = G_{\mathsf{real}}$ such that $\mathsf{Adv}^{\mathsf{dist}}_{G_i,G_{i+1}}(\mathcal{A})$ can be bounded using other techniques for $1 \leq i \leq t-2$. In addition, we assume $\mathsf{Adv}^{\mathsf{dist}}_{G_{t-1},G_t}(\mathcal{A})$ can be bounded by $\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{B})$ for some distributions D_1, D_2 on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, and another quantum query algorithm $\mathcal{B}$. Then we have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{dist}}_{G_{\mathsf{real}},G_{\mathsf{ideal}}}(\mathcal{A}) &\leq \mathsf{Adv}^{\mathsf{dist}}_{G_{t-1},G_t}(\mathcal{A}) + \sum_{i=1}^{t-2} \mathsf{Adv}^{\mathsf{dist}}_{G_i,G_{i+1}}(\mathcal{A}) \\ &\leq \mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{B}) + \sum_{i=1}^{t-2} \mathsf{Adv}^{\mathsf{dist}}_{G_i,G_{i+1}}(\mathcal{A}) \qquad (12)\end{aligned}$$

Hence, if $\mathsf{Adv}^{\mathsf{dist}}_{G_i,G_{i+1}}(\mathcal{A})$ can be upper bounded by other approaches for $1 \leq i \leq t-2$, then the remaining term can be bounded without any quantum argument, by using our tool. In later sections, we will upper bound $\mathsf{Adv}^{\mathsf{dist}}_{G_i,G_{i+1}}(\mathcal{A})$ by total variation distance $\Delta(G_i, G_{i+1})$. (Remember that $\mathsf{Adv}^{\mathsf{dist}}_{D,D'}(\mathcal{A}) \leq \Delta(D, D')$ holds for any distributions D and D' from Lemma 2.2.) Thus we upper bound the advantage $\mathsf{Adv}^{\mathsf{dist}}_{G_{\mathsf{real}},G_{\mathsf{ideal}}}(\mathcal{A})$ by purely combinatorial enumerating arguments.

4 Non-invertibility of Permutation with Feedforward in the Quantum Ideal Permutation Model

Now we apply the technique of Section 3 to show that permutation with feedforward is optimally non-invertible in the ideal permutation model. As one step in our proof, we also prove the difficulty to find a fixed point of random permutations (Proposition 4.1). We stress that this is the first results on quantum query lower bound for some property of random permutation P or some scheme constructed from P, in the model that both of forward and backward queries to permutation P are allowed. The goal of this section is to prove the following theorem.

Theorem 4.1. *Let $n \geq 32$. For any quantum algorithm $\mathcal{A}$ that makes at most q forward or backward queries to a public permutation P,*

$$\mathsf{Adv}^{inv}_{\mathsf{FF}^P}(\mathcal{A}) \leq \frac{4(e+1)(q+1)}{2^{n/2}} + \epsilon(n) \qquad (13)$$

holds, where $\epsilon(n) = \frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}$. *In particular,* $\mathcal{A}$ *cannot invert* FF^P *with constant probability for* $q \ll 2^{n/2}$.

Remark 4.1. We need the condition $n \geq 32$ for technical reasons. This assumption is reasonable since block lengths of block ciphers usually satisfiy it.

To show the above theorem, we begin with reducing the problem of finding a preimage of permutation with feedforward in the ideal permutation model to the problem of finding a fixed point of an ideal permutation. Let us define the advantage of a quantum algorithm $\mathcal{A}$ to find a fixed point of an ideal permutation by

$$\mathsf{Adv}_P^{fixpt}(\mathcal{A}) := \Pr_P[\mathcal{A}^{O_{P^\pm}}() = x \wedge P(x) = x],$$

here P is chosen uniformly at random, and

$$\mathsf{Adv}_P^{fixpt}(q) := \max_{\mathcal{A}} \left\{ \mathsf{Adv}_P^{fixpt}(\mathcal{A}) \right\},$$

where the maximum is taken over all quantum-query algorithms, each making at most q quantum queries.

Lemma 4.1. *For a quantum algorithm* $\mathcal{A}$ *that makes at most* q *quantum queries to* $O_{P^\pm}$*, there exists a quantum algorithm* $\mathcal{B}$ *that makes at most* q *quantum queries to* $O_{P^\pm}$ *such that* $\mathsf{Adv}^{inv}_{\mathsf{FF}^P}(\mathcal{A}) = \mathsf{Adv}_P^{fixpt}(\mathcal{B})$.

Proof. Given such algorithm $\mathcal{A}$, we construct $\mathcal{B}$ with the desired properties. Firstly, before making queries, $\mathcal{B}$ chooses $y \in \{0,1\}^n$ uniformly at random. $\mathcal{B}$ is given the oracle $O_{P^\pm}$ of the permutation P. Define another permutation P' by $P'(x) = P(x) \oplus y$. Then, the pair (P', y) follows the uniform distribution. If x satisfies $\mathsf{FF}_{P'}(x) = y$, then $P(x) = x$ holds. In addition, $\mathcal{B}$ can simulate the quantum oracle $O_{P'^\pm}$ using $O_{P^\pm}$ with no simulation overhead.

Then $\mathcal{B}$ runs $\mathcal{A}$, giving y as the target image. If $\mathcal{A}$ makes queries, then $\mathcal{B}$ answers using the oracle $O_{P'^\pm}$. Finally $\mathcal{B}$ outputs the final output of $\mathcal{A}$. This algorithm $\mathcal{B}$ obviously satisfies the desired property. □

From the above lemma, it suffices to upper bound Adv_P^{fixpt} to prove Theorem 4.1. Below we show the following proposition.

Proposition 4.1. *Let* $n \geq 32$*. For any quantum algorithm* $\mathcal{A}$ *that makes at most* q *forward or backward queries to a public permutation* P*,*

$$\mathsf{Adv}_P^{fixpt}(\mathcal{A}) \leq \frac{4(e+1)(q+1)}{2^{n/2}} + \epsilon(n) \tag{14}$$

holds, where $\epsilon(n) = \frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}$. *In particular,* $\mathcal{A}$ *cannot find a fixed point of* P *with constant probability for* $q \ll 2^{n/2}$.

Next, we reduce the problem of finding a fixed point of permutations to the problem of distinguishing two oracle distributions: random permutations and random derangements (permutations without fixed point). Let U be the

uniform distribution on $\mathsf{Perm}(\{0,1\}^n)$, and U_0 be the uniform distribution on $\mathsf{Der}(\{0,1\}^n) \subseteq \mathsf{Perm}(\{0,1\}^n)$. Then

$$\mathsf{Adv}_P^{fixpt}(q) \leq \mathsf{Adv}_{U^{\pm},U_0^{\pm}}^{dist}(q+1) \tag{15}$$

holds, since we can distinguish a permutation from derangements if we find its fixed point.

To upper bound $\mathsf{Adv}_{U^{\pm},U_0^{\pm}}^{dist}(q+1)$, we apply the technique introduced in Section 3. That is, we reduce the problem of distinguishing $U^{\pm}$ and $U_0^{\pm}$ to the problem of distinguishing two distributions Λ and Λ_0 on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, introducing intermediate distributions (or games). Λ is the distribution which is defined according to the distribution of fixed points of random permutations, and Λ_0 is the degenerate distribution with support on the zero-function. To this end, in addition to Λ, Λ_0, below we define functions $\Phi : \mathsf{Der}(\{0,1\}^n) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}) \to \mathsf{Perm}(\{0,1\}^n)$, $\Phi' : \mathsf{Der}(\{0,1\}^n) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}) \to \mathsf{Func}(\{0,1\}^n, \{0,1\}^n)$, and distributions D_{num} on $[0, \ldots, 2^n]$, U_1' on $\mathsf{Perm}(\{0,1\}^n)$, and U_2' on $\mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$. In the notation of Section 3, $G_1 = G_{\mathsf{ideal}} = U^{\pm}$, $G_2 = U_1'^{\pm}$, $G_3 = U_2'$, and $G_4 = G_{\mathsf{real}} = U_0^{\pm}$, and $D_1 = \Lambda, D_2 = \Lambda_0$.

Here we briefly explain motivations to introduce U_1', U_2' and Φ, Φ'. Our goal is to reduce the problem of distinguishing $U^{\pm}$ from $U_0^{\pm}$ to the problem of distinguishing Λ from Λ_0. That is, we want a technique to simulate the oracle that follows the distribution $U^{\pm}$ or $U_0^{\pm}$ on $\mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$, given the oracle that follows the distribution Λ or Λ_0 on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, respectively, without any knowledge that which of Λ and Λ_0 is given. However, it is difficult to directly construct such a technique. Thus, we define an intermediate distribution U_1' that is close to U, and so that we can construct such a technique between $U_1'^{\pm}$ and $U_0^{\pm}$. The technique is as follows. Firstly, we define a map $\Phi : \mathsf{Der}(\{0,1\}^n) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}) \to \mathsf{Perm}(\{0,1\}^n)$ such that $\Phi(P_0, f)$ follows U_1' if (P_0, f) follows (U_0, Λ), and $\Phi(P_0, f)$ follows U_0 if (P_0, f) follows (U_0, Λ_0), respectively (actually Φ is firstly defined and then U_1' is defined using Φ). Secondly, given an oracle f that follows Λ or Λ_0, we choose $P_0 \in \mathsf{Der}(\{0,1\}^n)$ uniformly at random, and simulate the oracle of $(\Phi(P_0, f))^{\pm}$. Then, we can simulate the distributions $U_1'^{\pm}$ or $U_0^{\pm}$ according to which of Λ or Λ_0 is given. However, there is a problem: simulation cost of $U_1'^{\pm}$ might become very high. Thus we introduce another distribution U_2' and map Φ', to overcome the problem of simulation overhead. Details on simulation overhead will be explained later.

Now we give formal description of intermediate distributions and maps Φ, Φ'. In what follows, we identify a function $F \in \mathsf{Func}(\{0,1\}^n, \{0,1\}^n)$ with the associated graph G_F of which vertexes are n-bit strings. In the graph G_F, there is an edge from a vertex x to another vertex y if and only if $F(x) = y$. If F is a permutation P, then each connected component of G_P is a cycle, and isolated points correspond to fixed points of P.

Distribution D_{num}. Distribution D_{num} on $[0, \ldots, 2^n]$ is the distribution of the number of fixed points of random permutations. D_{num} is formally defined

by $D_{num}(\lambda) := \Pr_{P\sim U}[\lambda = |\{x|P(x) = x\}|]$. In other words, D_{num} is the distribution of the random variable that takes values in $[0, \ldots, 2^n]$ which is defined according to the following sampling.

1. $P \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$
2. $\lambda \leftarrow |\{x|P(x) = x\}|$
3. Return λ.

Distribution Λ. Distribution Λ on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$ is defined according to the distribution of fixed points of random permutations. For $P \in \mathsf{Perm}(\{0,1\}^n)$, define $f_P \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$ by $f_P(x) = 1$ if and only if $P(x) = x$. Then, Λ is formally defined by $\Lambda(f) := \Pr_{P\sim U}[f = f_P]$. In other words, Λ is the distribution of the random variable that takes values in $\mathsf{Func}(\{0,1\}^n, \{0,1\})$, which is defined according to the following sampling:

1. $P \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$
2. $f \leftarrow f_P$
3. Return f.

Distribution Λ_0. Distribution Λ_0 on $\mathsf{Func}(\{0,1\}^n, \{0,1\})$ is the degenerate distribution with support on the zero-function $\mathbf{0}$, which maps x to 0 for any x. Formally, Λ_0 is defined by $\Lambda_0(g) := 1$ if and only if $g = \mathbf{0}$.

Function Φ. Taking $P_0 \in \mathsf{Der}(\{0,1\}^n)$ and $f \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$ as inputs, we want to construct another permutation $P = \Phi(P_0, f)$ which has, informally speaking, the following properties:

1. $P(x) = x$ if and only if $f(x) = 1$ holds with high probability when P_0 and f are chosen uniformly at random.
2. If $f(x) = 0$, then $P(x) = P_0(x)$ for almost all x.

This function Φ is used later to approximate U by using U_0 and Λ.

Formally, function $\Phi : \mathsf{Der}(\{0,1\}^n) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}) \to \mathsf{Perm}(\{0,1\}^n)$ is defined by the following process.

1. Take $P_0 \in \mathsf{Perm}(\{0,1\}^n), f \in \mathsf{Func}(\{0,1\}^n)$ as inputs.
2. For each $x \in \{0,1\}^n$, define $P(x)$ by:
3. If $f(x) = 1$
4. $P(x) \leftarrow x$
5. Else
6. Calculate $\min\{i \mid f(P_0^i(x)) = 0\}$, $\mathsf{cnt} \leftarrow \min\{i \mid f(P_0^i(x)) = 0\}$
7. $P(x) \leftarrow P_0^{\mathsf{cnt}}(x)$
8. End If
9. $\Phi(P_0, f) \leftarrow P$

Figure 2 illustrates how $P = \Phi(P_0, f)$ is generated from P_0 and f. Each element x such that $f(x) = 1$ is converted to isolated points, and the edges $y \to x, x \to z$ are converted to new edges $y \to z, x \to x$. By definition, images of Φ are certainly in $\mathsf{Perm}(\{0,1\}^n)$. Note that $\Phi(P_0, f)^{-1} = \Phi(P_0^{-1}, f)$ holds.

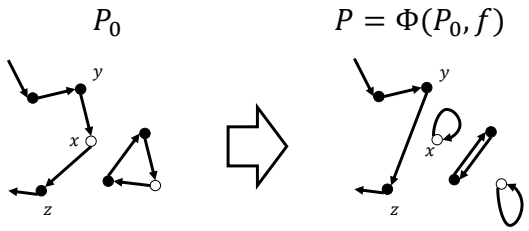

Fig. 2. How $P = \Phi(P_0, f)$ is generated. White circle are the preimages of 1 by f.

Function Φ' Φ' is a function which is defined to approximate U using U_0 and Λ similarly as Φ, but the approximation of Φ' is more rough than that of Φ. While outputs of Φ are always permutations, outputs of Φ' might not be permutations, although $\Phi(P_0, f) = \Phi'(P_0, f)$ holds with high probability when P_0 and f are sampled following U_0 and Λ. See this paper's full version [15] for more details.

Formally, function $\Phi' : \mathsf{Der}(\{0,1\}^n) \times \mathsf{Func}(\{0,1\}^n, \{0,1\}) \to \mathsf{Func}(\{0,1\}^n, \{0,1\}^n)$ is defined by the following process.

1. Take $P_0 \in \mathsf{Perm}(\{0,1\}^n), f \in \mathsf{Func}(\{0,1\}^n)$ as inputs.
2. For each $x \in \{0,1\}^n$, define $P(x)$ by:
3. If $f(x) = 1$
4. $P(x) \leftarrow x$
5. Else If $f(P_0(x)) = 1$
6. $P(x) \leftarrow P_0^2(x)$
7. Else
8. $P(x) \leftarrow P_0(x)$
9. End If
10. $\Phi'(P_0, f) \leftarrow P$

We defined not only Φ but also Φ' to achieve low simulation overhead: Suppose we are given the oracle of $f \in \mathsf{Func}(\{0,1\}^n, \{0,1\})$. Then, for any $P_0 \in \mathsf{Der}(\{0,1\}^n)$ which we choose ourselves, we can operate one evaluation of the function $\Phi'(P_0, f)$ with only two queries to f. On the other hand, we might need a lot of queries to f to evaluate $\Phi(P_0, f)$ in Step 6 of the definition of Φ (we need about 2^n queries in the worst case). This is the reason why we introduced Φ'.

For fixed P_0 and f, we define $P_2'^{\pm} : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ by

$$P_2'^{\pm}(b, x) := \begin{cases} \Phi'(P_0, f)(x) & \text{if } b = 0, \\ \Phi'(P_0^{-1}, f)(x) & \text{if } b = 1. \end{cases}$$

$P_2'^{\pm}$ can be regarded as an approximation of the function $\Phi^{\pm}(P_0, f) \in \mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$, which is defined by $\Phi^{\pm}(P_0, f)(0, x) = \Phi(P_0, f)(x)$ and $\Phi^{\pm}(P_0, f)(1, x) = \Phi(P_0^{-1}, f)(x)$.

Distribution U_1' Distribution U_1' on $\mathsf{Perm}(\{0,1\}^n)$ is an approximation of the uniform distribution U that combines U_0 with Λ. Formally, U_1' is defined by $U_1'(P) = \Pr_{P_0 \sim U_0, f \sim \Lambda}[P = \Phi(P_0, f)]$. In other words, U_1' is the distribution of the random variable that takes values in $\mathsf{Perm}(\{0,1\}^n)$ which is defined according to the following sampling:

1. $P_0 \xleftarrow{U_0} \mathsf{Perm}(\{0,1\}^n)$, $f \xleftarrow{\Lambda} \mathsf{Func}(\{0,1\}^n, \{0,1\})$
2. $P \leftarrow \Phi(P_0, f)$

Note that if P is sampled following U_1', we assume that a quantum adversary $\mathcal{A}$ is given a quantum oracle of $P^{\pm} : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ (see Section 2.1).

Distribution U_2' Distribution U_2' on $\mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$ is another approximation of U, which is more "rough" than U_1'. Below, for $F \in \mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$, the n-bit functions $F(0,\cdot), F(1,\cdot)$ are denoted by F^+ and F^-. Then, formally, U_2' is defined by $U_2'(F) = \Pr_{P_0 \sim U_0, f \sim \Lambda}[F^+ = \Phi'(P_0, f) \wedge F^- = \Phi'(P_0^{-1}, f)]$. In other words, U_2' is the distribution of the random variable that takes values in $\mathsf{Func}(\{0,1\} \times \{0,1\}^n, \{0,1\}^n)$ which is defined according to the following sampling:

1. $P_0 \xleftarrow{U_0} \mathsf{Perm}(\{0,1\}^n)$, $f \xleftarrow{\Lambda} \mathsf{Func}(\{0,1\}^n, \{0,1\})$
2. $F^+ \leftarrow \Phi'(P_0, f), F^- \leftarrow \Phi'(P_0^{-1}, f)$

Now the preparation to use the technique in Section 3 is completed. We reduce the problem of distinguishing U from U_0 to the problem of distinguishing Λ and Λ_0. Now we have the following inequalities.

$$\begin{aligned}\mathsf{Adv}^{dist}_{U^{\pm}, U_0^{\pm}}(\mathcal{A}) &\leq \mathsf{Adv}^{dist}_{U^{\pm}, U_1'^{\pm}}(\mathcal{A}) + \mathsf{Adv}^{dist}_{U_1'^{\pm}, U_2'}(\mathcal{A}) + \mathsf{Adv}^{dist}_{U_2', U_0^{\pm}}(\mathcal{A}) \\ &\leq \Delta(U^{\pm}, U_1'^{\pm}) + \Delta(U_1'^{\pm}, U_2') + \mathsf{Adv}^{dist}_{U_2', U_0{}^{\pm}}(\mathcal{A}). \qquad (16)\end{aligned}$$

Next, we show the following lemma.

Lemma 4.2. *For a quantum algorithm $\mathcal{A}$ to distinguish U_2' from $U_0^{\pm}$ that makes at most q quantum queries, we can construct a quantum algorithm $\mathcal{B}$ to distinguish Λ from Λ_0 that makes at most $2q$ queries and satisfies*

$$\mathsf{Adv}^{dist}_{U_2', U_0^{\pm}}(\mathcal{A}) = \mathsf{Adv}^{dist}_{\Lambda, \Lambda_0}(\mathcal{B}).$$

Proof. We give a quantum algorithm $\mathcal{B}$ that satisfies the desired properties. $\mathcal{B}$ is given a quantum oracle O_f, where f is sampled according to Λ or Λ_0. Before making queries, $\mathcal{B}$ chooses a derangement P_0 uniformly at random. Then, $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{B}$ answers to queries of $\mathcal{A}$ by calculating $\Phi'(P_0, f)$ and $\Phi'(P_0^{-1}, f)$. By definition of Φ', $\mathcal{B}$ can calculate one evaluation of $\Phi'(P_0, f)$ (and $\Phi'(P_0^{-1}, f)$) with two queries to O_f. Finally, $\mathcal{B}$ outputs what $\mathcal{A}$ outputs.

Since $\mathcal{A}$ makes at most q queries, $\mathcal{B}$ makes at most $2q$ queries. $\mathcal{B}$ perfectly simulates the distributions U_2' and $U_0{}^{\pm}$ according to which of Λ and Λ_0 is given. Thus $\mathsf{Adv}^{dist}_{U_2', U_0^{\pm}}(\mathcal{A}) = \mathsf{Adv}^{dist}_{\Lambda, \Lambda_0}(\mathcal{B})$ holds. □

From the above lemma and the inequalities (16), we have

$$\mathsf{Adv}^{dist}_{U^{\pm},U_0^{\pm}}(q) \le \Delta(U^{\pm}, {U'_1}^{\pm}) + \Delta({U'_1}^{\pm}, U'_2) + \mathsf{Adv}^{dist}_{\Lambda,\Lambda_0}(2q). \tag{17}$$

The three terms in the right hand side are upper bounded as in the following lemmas.

Lemma 4.3. $\mathsf{Adv}^{dist}_{\Lambda,\Lambda_0}(q) \le \frac{2(e+1)q}{2^{n/2}}$

Lemma 4.4. $\Delta(U^{\pm}, {U'_1}^{\pm}) \le \frac{8n^3}{2^n-2n+1} + \frac{16n^3}{2^n} + \frac{e+1}{n!}$ *for* $n \ge 32$.

Lemma 4.5. $\Delta({U'_1}^{\pm}, U'_2) \le \frac{32n^3}{2^n} + \frac{2(e+1)}{n!}$ *for* $n \ge 32$.

Thus we have

$$\mathsf{Adv}^{dist}_{U^{\pm},U_0^{\pm}}(q) \le \frac{4(e+1)q}{2^{n/2}} + \frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}.$$

Combining this inequality and inequality (15), we obtain the desired bound (14) in Theorem 4.1.

To complete the proof, we give a proof of Lemma 4.3. Proofs of Lemma 4.4 and 4.5 are given in this paper's full version [15].

Proof of Lemma 4.3. To prove the Lemma 4.3, we use Proposition 3.2. Let us define a set of functions $\mathsf{good}, \mathsf{bad} \subset \mathsf{Func}(\{0,1\}^n, \{0,1\})$ by $\mathsf{good} := \mathsf{Func}(\{0,1\}^n, \{0,1\}) \backslash \{\mathbf{0}\}$, and $\mathsf{bad} := \emptyset$. In addition, for each integer $\lambda > 0$, define $\mathsf{good}_\lambda \subset \mathsf{good}$ by $f \in \mathsf{good}_\lambda$ if and only if $|f^{-1}(1)| = \lambda$. Then, $\bigcup_\lambda \mathsf{good}_\lambda = \mathsf{good}$ and $\mathsf{good}_{\lambda_1} \cap \mathsf{good}_{\lambda_2} = \emptyset$ for $\lambda_1 \ne \lambda_2$. Moreover, the conditional probability $\Pr_{F\sim\Lambda}[F = f | F \in \mathsf{good}_\lambda]$ is independent on f due to the symmetry of the distribution Λ. Therefore we can apply Proposition 3.2.

Let $p_1^{\mathsf{good}_\lambda} := \Pr_{F\sim\Lambda}[F \in \mathsf{good}_\lambda]$ and $p_1^{f|\mathsf{good}_\lambda} := \Pr_{F\sim\Lambda}[F = f \mid F \in \mathsf{good}_\lambda]$. For each fixed x, the number of boolean function f such that $f(x) = 1 \wedge |f^{-1}(1)| = \lambda$ is exactly $\binom{2^n-1}{\lambda-1}$. Hence we have

$$\max_x |\{f \in \mathsf{good}_\lambda \mid f(x) = 1\}| = \binom{2^n-1}{\lambda-1}. \tag{18}$$

In addition,

$$p_1^{f|\mathsf{good}_\lambda} = \frac{1}{\binom{2^n}{\lambda}}. \tag{19}$$

hold.

Next, we upper bound $p_1^{\mathsf{good}_\lambda} = \Pr_{f\sim\Lambda}[f \in \mathsf{good}_\lambda] = \Pr_{a\sim D_{num}}[a = \lambda]$. For any fixed λ, we have

$$\begin{aligned}\Pr_{a\sim D_{num}}[a = \lambda] &= \frac{\binom{2^n}{\lambda}\cdot !(2^n-\lambda)}{2^n!} = \frac{!(2^n-\lambda)}{(2^n-\lambda)!}\cdot\frac{1}{\lambda!} \le \frac{(2^n-\lambda)!/e+1}{(2^n-\lambda)!}\cdot\frac{1}{\lambda!} \\ &= \left(1 + \frac{e}{(2^n-\lambda)!}\right)\cdot\frac{1}{e}\cdot\frac{1}{\lambda!} \le \frac{1+e}{e}\cdot\frac{1}{\lambda!}\end{aligned} \tag{20}$$

(Remember that $!N$ denotes the number of derangements on a set of size N and $!N = \left\lfloor \frac{N!}{e} + \frac{1}{2} \right\rfloor$ holds. see Section 2.) Thus we have

$$p_1^{\mathsf{good}_\lambda} = \Pr_{f \sim \Lambda}[f \in \mathsf{good}_\lambda] \leq \frac{1+e}{e} \cdot \frac{1}{\lambda!}. \tag{21}$$

From Proposition 3.2, equality (18), (19), and inequality (21), since $\Pr_{f \sim \Lambda}[f \in \mathsf{bad}] = 0$ we have

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{dist}}_{\Lambda,\Lambda_0}(q) &\leq 2q \cdot \sum_{0<\lambda} p_1^{\mathsf{good}_\lambda} \sqrt{p_1^{f|\mathsf{good}_\lambda} \cdot \max_x \{|\{f \mid f(x) = 1 \wedge f \in \mathsf{good}_\lambda\}|\}} \\
&\leq 2q \cdot \sum_{0<\lambda} \frac{1+e}{e} \cdot \frac{1}{\lambda!} \sqrt{\frac{\binom{2^n-1}{\lambda-1}}{\binom{2^n}{\lambda}}} \leq \frac{2q(1+e)}{e} \cdot \sum_{0<\lambda} \frac{1}{\lambda!} \sqrt{\frac{\lambda}{2^n}} \\
&= \frac{2q(1+e)}{e} \cdot \sum_{0<\lambda} \frac{1}{\sqrt{\lambda}(\lambda-1)!} \sqrt{\frac{1}{2^n}} \\
&\leq \frac{2q(1+e)}{e} \cdot \sum_{0\leq\lambda} \frac{1}{\lambda!} \sqrt{\frac{1}{2^n}} = \frac{2(e+1)q}{\sqrt{2^n}},
\end{aligned} \tag{22}$$

which is the desired bound. Hence Lemma 4.3 follows. □

Remark 4.2. In this section we showed the non-invertibility of FF^P but did not show the one-wayness, because it seems difficult to reduce the one-wayness to the non-invertibility for the case of a permutation with feedforward. For Davies-Meyer construction, on the other hand, we can reduce its one-wayness to the non-invertibility by upper-bounding the total variation distance between the distribution of the game to break the one-wayness and that of the game to break the non-invertibility. Unfortunately, for permutations with feedforward, this strategy cannot be applied since the total variation distance between the two corresponding distributions would become very large.

5 Security of Davies-Meyer Constructions in the Quantum Ideal Cipher Model

This section gives proofs for security of Davies-Meyer constructions in the quantum ideal cipher model. We begin with showing non-invertibility, and then prove one-wayness. Our result in this section is the first proof for quantum security of functions based on public block ciphers.

5.1 Non-Invertibility of Davies-Meyer

Non-invertibility in the ideal cipher model is shown in the similar way as in the proof for non-invertibility of permutation with feedforward in Section 4. We show the following theorem.

Theorem 5.1 (Non-invertibility of Davies-Meyer). *Let $n \geq 32$. For any quantum algorithm $\mathcal{A}$ that makes at most q queries to a block cipher E,*

$$\mathsf{Adv}^{inv}_{\mathsf{DM}^E}(\mathcal{A}) \leq 4(q+1)\left(\frac{n^{1/2}}{2^{n/2}} + \frac{2^m(e+1)}{n!}\right) + 2^m\epsilon(n) \tag{23}$$

holds, where $\epsilon(n) = \frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}$. In particular, $\mathcal{A}$ cannot invert DM^E with constant probability if $\frac{2^m}{2^n} \ll 1$ and $q \ll 2^{n/2}/n^{1/2}$.

Remark 5.1. In the above theorem, security bound is valid only for the case that key length m is less than block length n. (We do not know if there exist any attacks that exploit long key lengths. The condition that key length should be shorter than the block length comes from limitation of our proof technique.) However, even if $m \geq n$, then we can achieve the same bound if we restrict key space. That is, if we are given n-bit block ciphers with m-bit key and $m \geq n$, we use only the keys of which all bits are 0 except for the first $n/2$-bits, for example. Then we can construct non-invertible functions with $3n/2$-bit input and n-bit output.

We cannot get rid of this restriction on usage of key space since there are terms of order $O(n^3 \cdot 2^{m-n})$ in our bound (23), which come from Lemma 4.4 and 4.5. The bound of Lemma 4.4 cannot be essentially improved, since $\Delta(U, U'_1) \geq \frac{1}{4e \cdot 2^n}$ holds (see this paper's full version [15] for more details). Thus, if we want to get rid of the restriction, then we have to use other proof strategies.

Let U_E be the uniform distribution on $\mathsf{Ciph}(m,n)$, and $U_{E,0}$ be the distribution on $\mathsf{Ciph}(m,n)$ defined by $U_{E_0}(E) = \prod_k U_0(E_k)$ (i.e., when E is sampled according to $U_{E,0}$, then E_k is sampled according to U_0 for each key k.) We say that a pair (z,x) is a fixed point of a block cipher E if $E_z(x) = x$. Let us define the advantage of a quantum algorithm $\mathcal{A}$ to find a fixed point of an ideal block cipher E by

$$\mathsf{Adv}^{fixpt}_E(\mathcal{A}) := \Pr_{E \sim U_E}[\mathcal{A}^{O_{E^\pm}}() = (z,x) \wedge E_z(x) = x],$$

and

$$\mathsf{Adv}^{fixpt}_E(q) := \max_{\mathcal{A}} \left\{ \mathsf{Adv}^{fixpt}_E(\mathcal{A}) \right\},$$

where the maximum is taken over all quantum-query algorithms, each making at most q quantum queries.

Then, similarly as in the proof for permutation with feedforward, we have

$$\mathsf{Adv}^{inv}_{\mathsf{DM}^E}(q) \leq \mathsf{Adv}^{fixpt}_E(q) \leq \mathsf{Adv}^{dist}_{U_E^\pm, U_{E,0}^\pm}(q+1). \tag{24}$$

To upper bound $\mathsf{Adv}^{dist}_{U_E^\pm, U_{E,0}^\pm}$, we introduce distributions $D_{E,num}, \Lambda_E, \Lambda_{E,0}, U'_{E,1}$, $U'_{E,2}$, which are essentially product distributions of $D_{num}, \Lambda, \Lambda_0, U'_1, U'_2$, respectively.

Distribution $D_{E,num}$. Distribution $D_{E,num}$ on $([0,\dots,2^n])^{\times 2^m}$ is the product distribution $D_{num}\times\cdots\times D_{num}$, i.e. $D_{E,num}$ is defined by $D_{E,num}(\lambda_0,\dots,\lambda_{2^m-1})$ $:= D_{num}(\lambda_0)\times\cdots\times D_{num}(\lambda_{2^m-1})$. $D_{E,num}$ can be regarded as the distribution of the number of fixed points of ideal ciphers.

Distribution Λ_E. Distribution Λ_E on the set $\mathsf{Func}(\{0,1\}^m\times\{0,1\}^n,\{0,1\})$ $= (\mathsf{Func}(\{0,1\}^n,\{0,1\}))^{2^m}$ is defined as the product distribution $\Lambda\times\cdots\times\Lambda$, i.e. Λ_E is defined by $\Lambda_E(F) := \Lambda_E(F(0,\cdot))\times\Lambda_E(F(1,\cdot))\times\cdots\times\Lambda_E(F(2^m-1,\cdot))$. Λ_E can be regarded as the distribution of fixed points of ideal ciphers.

Distribution $\Lambda_{E,0}$. Distribution $\Lambda_{E,0}$ on $\mathsf{Func}(\{0,1\}^m\times\{0,1\}^n,\{0,1\})$ is the degenerate distribution with support on the zero-function $\mathbf{0}$.

Distribution $U'_{E,1}$ Distribution $U'_{E,1}$ on $\mathsf{Ciph}(m,n)$ is defined by $U'_{E,1}(E) := \prod_{k\in\{0,1\}^m} U'_1(E_k)$. That is, when E is sampled according to $U'_{E,1}$, then E_k is chosen according to U'_1 independently for each key k. Similarly as U'_1 is an approximation of U, $U'_{E,1}$ can be regarded as an approximation of U_E.

Distribution $U'_{E,2}$ Distribution $U'_{E,2}$ on $\mathsf{Func}(\{0,1\}\times\{0,1\}^m\times\{0,1\}^n,\{0,1\}^n)$ is defined by $U'_{E,2}(F) = \prod_{k\in\{0,1\}^m} U'_2(F(\cdot,k,\cdot))$. That is, $U'_{E,2}$ is the distribution of the random variable that is defined by the following sampling.

1. For each $z\in\{0,1\}^m$, do:
2. $\quad G_z \xleftarrow{U'_2} \mathsf{Func}(\{0,1\}\times\{0,1\}^n,\{0,1\}^n)$
3. $F(b,z,x)\leftarrow G_z(b,x)$ for each $b\in\{0,1\}, z\in\{0,1\}^m, x\in\{0,1\}^n$.
4. Return F

Similarly as U'_2 is a rough approximation of $U^{\pm}$, $U'_{E,2}$ can be regarded as a rough approximation of $U_E^{\pm}$.

Now we apply the technique introduced in Section 3. Similarly as inequality (17), we can show that

$$\mathsf{Adv}^{dist}_{U_E^{\pm},U_{E,0}^{\pm}}(q) \le \Delta(U_E^{\pm},U_{E,1}^{'\pm}) + \Delta(U_{E,1}^{'\pm},U'_{E,2}) + \mathsf{Adv}^{dist}_{\Lambda_E,\Lambda_{E,0}}(2q),$$

holds. In addition, since $U, U'_{E,1}, U'_{E,2}$ are essentially the product distributions of U, U'_1, U'_2, from Lemma 4.4 and Lemma 4.5 we have

$$\begin{aligned}\mathsf{Adv}^{dist}_{U_E^{\pm},U_{E,0}^{\pm}}(q) &\le 2^m\Delta(U^{\pm},U_1^{'\pm}) + 2^m\Delta(U_1^{'\pm},U'_2) + \mathsf{Adv}^{dist}_{\Lambda_E,\Lambda_{E,0}}(2q)\\ &\le 2^m\left(\frac{8n^3}{2^n-2n+1}+\frac{48n^3}{2^n}+\frac{3(e+1)}{n!}\right) + \mathsf{Adv}^{dist}_{\Lambda_E,\Lambda_{E,0}}(2q).\end{aligned} \tag{25}$$

Thus, to prove Theorem 5.1, it suffices to show the following lemma.

Lemma 5.1.

$$\mathsf{Adv}^{dist}_{\Lambda_E,\Lambda_{E,0}}(q) \le 2q\left(\frac{n^{1/2}}{2^{n/2}} + \frac{2^m(e+1)}{n!}\right)$$

Proof. To prove the Lemma 5.1, again we use our tool in Section 3. Let us define a set of functions $\mathsf{good} \subset \mathsf{Func}(\{0,1\}^m \times \{0,1\}^n, \{0,1\})$ by $f \in \mathsf{good}$ if and only if $f \neq \mathbf{0}$ and $\lambda_z = |f_z^{-1}(1)| < n$ for all $z \in \{0,1\}^m$, where $f_z(\cdot) = f(z,\cdot)$. Let $\mathsf{bad} := \mathsf{Func}(\{0,1\}^m \times \{0,1\}^n, \{0,1\}) \backslash (\mathsf{good} \cup \{\mathbf{0}\})$. In addition, for each sequence of integers $\lambda_S = (\lambda_0, \lambda_1, \ldots, \lambda_{2^m-1})$, define $\mathsf{good}_{\lambda_S} \subset \mathsf{good}$ by $f \in \mathsf{good}_{\lambda_S}$ if and only if $f_z^{-1}(1) = \lambda_z$ for all $0 \le z \le 2^m - 1$. For simplicity, we write $\lambda_S < n$ if and only if $\lambda_z < n$ for all $0 \le z \le 2^m - 1$. Similarly, we write $0 < \lambda_S$ if and only if $\lambda_z > 0$ for all $0 \le z \le 2^m - 1$. Then, $\bigcup_{0<\lambda_S<n} \mathsf{good}_{\lambda_S} = \mathsf{good}$ and $\mathsf{good}_{\lambda_S} \cap \mathsf{good}_{\lambda_{S'}} = \emptyset$ for $\lambda_S \neq \lambda_{S'}$. The conditional probability $\Pr_{F\sim\Lambda_E}[F = f | f \in \mathsf{good}_{\lambda_S}]$ is independent on f due to the symmetry of the distribution Λ_E. Therefore we can apply Proposition 3.2 with $D_1 = \Lambda_E$ and $D_2 = \Lambda_{E,0}$.

Define

$$p_1^{\mathsf{good}_{\lambda_S}} := \Pr_{f\sim\Lambda_E}\left[f \in \mathsf{good}_{\lambda_S}\right] \tag{26}$$

and

$$p_1^{f|\mathsf{good}_{\lambda_S}} := \Pr_{F\sim\Lambda_E}\left[F = f \mid F \in \mathsf{good}_{\lambda_S}\right]. \tag{27}$$

Now we upper bound $\Pr_{f\sim\Lambda_E}[f \in \mathsf{bad}]$. Note that $\Pr_{f\sim\Lambda_E}[f \in \mathsf{bad}] \le 2^m \Pr_{f\sim\Lambda}[|f^{-1}(1)| \ge n]$ holds since Λ_E is product distribution of Λ. In addition, from inequality (21) we have

$$\Pr_{f\sim\Lambda}[|f^{-1}(1)| \ge \lambda_0] \le \frac{e+1}{e}\sum_{\lambda\ge\lambda_0}\frac{1}{\lambda!} \le \frac{e+1}{e}\frac{e}{\lambda_0!} = \frac{e+1}{\lambda_0!}, \tag{28}$$

where we used the fact $\sum_{\lambda\ge\lambda_0}\frac{1}{\lambda!} \le \frac{e}{\lambda_0!}$. Thus we have

$$\Pr_{f\sim\Lambda_E}[f \in \mathsf{bad}] \le \frac{2^m(1+e)}{n!}. \tag{29}$$

Next, we upper bound $p_1^{f|\mathsf{good}_{\lambda_S}} \cdot \max_{(z,x)} \left|\left\{f \in \mathsf{good}_{\lambda_S} \mid f(z,x) = f_z(x) = 1\right\}\right|$. For each fixed $w \in \{0,1\}^m, x \in \{0,1\}^n$ and $\lambda_S = (\lambda_0, \ldots, \lambda_{2^m-1})$, the number of boolean function $f \in \mathsf{good}_{\lambda_S}$ such that $f_w(x) = 1$ is equal to

$$\binom{2^n-1}{\lambda_w - 1} \cdot \prod_{z\neq w\in\{0,1\}^m}\binom{2^n}{\lambda_z} = \frac{\lambda_w}{2^n}\cdot\prod_{z\in\{0,1\}^m}\binom{2^n}{\lambda_z}. \tag{30}$$

Thus for each sequence $\lambda_S < n$ we have

$$\begin{aligned}\max_{(z,x)}\left|\left\{f \in \mathsf{good}_{\lambda_S} \mid f(z,x) = f_z(x) = 1\right\}\right| &= \max_{(z,x)}\left\{\frac{\lambda_z}{2^n}\cdot\prod_{z\in\{0,1\}^m}\binom{2^n}{\lambda_z}\right\} \\ &\le \frac{n}{2^n}\cdot\prod_{z\in\{0,1\}^m}\binom{2^n}{\lambda_z}\end{aligned} \tag{31}$$

Hence, for each sequence $\lambda_S < n$ we have

$$p_{\Delta}^{f|\mathsf{good}_{\lambda_S}} \cdot \max_{(z,x)} \left|\left\{f \in \mathsf{good}_{\lambda_S} \mid f(z,x) = f_z(x) = 1\right\}\right| \\ \leq \frac{1}{\prod_{z\in\{0,1\}^m} \binom{2^n}{\lambda_z}} \cdot \frac{n}{2^n} \cdot \prod_{z\in\{0,1\}^m} \binom{2^n}{\lambda_z} = \frac{n}{2^n}. \tag{32}$$

From Proposition 3.2, and inequalities (29) and (32), $\mathsf{Adv}^{\mathsf{dist}}_{\Lambda,\Lambda_0}(q)$ is upper bounded by

$$2q \cdot \sum_{\lambda_S<n} p_1^{\mathsf{good}_{\lambda_S}} \sqrt{p_1^{f|\mathsf{good}_{\lambda_S}} \cdot \max_{(z,x)} \left|\left\{f \in \mathsf{good}_{\lambda_S} \mid f_z(x) = 1\right\}\right|} \\ + 2q \cdot \Pr_{f\sim\Lambda_E}[f \in \mathsf{bad}] \\ \leq 2q \cdot \sum_{\lambda_S<n} p_1^{\mathsf{good}_{\lambda_S}} \sqrt{\frac{n}{2^n}} + 2q \cdot \frac{2^m(e+1)}{n!} \leq 2q\left(\sqrt{\frac{n}{2^n}} + \frac{2^m(e+1)}{n!}\right), \tag{33}$$

which completes the proof. □

5.2 One-Wayness of Davies-Meyer

Next, we show that Davies-Meyer constructions are also quantum one-way in the quantum ideal cipher model.

Theorem 5.2 (One-wayness of Davies-Meyer). *Let $n \geq 32$ and $m \leq n^2$. For any quantum algorithm $\mathcal{A}$ that makes at most q queries to a block cipher E,*

$$\mathsf{Adv}^{ow}_{\mathsf{DM}^E}(\mathcal{A}) \leq 4(q+1)\left(\frac{n^{1/2}}{2^{n/2}} + \frac{2^m(e+1)}{n!}\right) + 2^m\epsilon(n) + \frac{2n+1}{2^{m/3+1}} + \frac{n^2}{2^{m-2}} \tag{34}$$

holds, where $\epsilon(n) = \frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}$. In particular, $\mathcal{A}$ cannot find a preimage of DM^E with constant probability if $\frac{2^m}{2^n} \ll 1$ and $q \ll 2^{n/2}/n^{1/2}$.

Remark 5.2. Here we need an additional condition $m \leq n^2$ for technical reasons. This assumption is reasonable since usual block ciphers satisfy it.

Proof. Let U_n be the uniform distribution on $\{0,1\}^n$ and V be the distribution on $\mathsf{Ciph}(m,n) \times \{0,1\}^n$ which is defined by $V(E,y) = \Pr_{e\sim U_E,(z,x)\sim U_{m+n}}[e = E \wedge \mathsf{DM}^E(z,x) = y]$. That is, V is the distribution of the random variable which is defined by the following sampling:

1. $E \xleftarrow{U_E} \mathsf{Ciph}(m,n)$, $z \xleftarrow{\$} \{0,1\}^m, x \xleftarrow{\$} \{0,1\}^n$
2. $y \leftarrow \mathsf{DM}^E(z,x)$
3. Return (E,y)

Then $\mathsf{Adv}^{ow}_{\mathsf{DM}^E}(\mathcal{A}) = \Pr_{(E,y)\sim V}[\mathcal{A}^{O_{E^\pm}}(y) = (z', x') \wedge \mathsf{DM}^E(z', x') = y]$ is upper bounded by

$$\begin{aligned}
&\Pr_{E\sim U_E, y\sim U_n}[\mathcal{A}^{O_{E^\pm}}(y) = (z', x') \wedge \mathsf{DM}^E(z', x') = y] \\
&\quad + \Big| \Pr_{(E,y)\sim V}[\mathcal{A}^{O_{E^\pm}}(y) = (z', x') \wedge \mathsf{DM}^E(z', x') = y] \\
&\qquad\qquad - \Pr_{E\sim U_E, y\sim U_n}[\mathcal{A}^{O_{E^\pm}}(y) = (z', x') \wedge \mathsf{DM}^E(z', x') = y]\Big| \\
&\leq \mathsf{Adv}^{inv}_{\mathsf{DM}^E}(\mathcal{A}) + \Delta(V, (U_E, U_n)). \qquad (35)
\end{aligned}$$

Hence Theorem 5.2 follows from Theorem 5.1 and the following lemma.

Lemma 5.2. *$\Delta(V, (U_E, U_n)) \leq \frac{2n+1}{2^{m/3+1}} + \frac{n^2}{2^{m-2}}$ for $n \geq 32$ and $m \leq n^2$.*

A proof of this lemma is given in this paper's full version [15]. □

6 Security of Merkle-Damgård with Davies-Meyer Constructions

This section shows that the combination of Davies-Meyer constructions with the Merkle-Damgård constructions are optimally non-invertible and one-way in the quantum ideal cipher model.

Merkle-Damgård construction is the most basic construction to convert compression functions, which have fixed input length, to a function with (variable) long input lengths. In particular, lots of popular hash functions like SHA-2 [22] are based on the Merkle-Damgård constructions, and use Davies-Meyer constructions as compression functions. Merkle-Damgård construction with MD-compliant padding is proven to be collision resistant hash function when underlying compression function is collision-resistant [12]. However, there is no guarantee that Merkle-Damgård constructions (with MD-compliant padding) become one-way (preimage resistant) or second preimage resistant hash functions even if underlying compression functions are one-way (preimage resistant) or second preimage resistant. Actually there is an attack that finds a second preimage with complexity less than 2^n [18].

Since usual Merkle-Damgård constructions do not guarantee one-wayness even in classical settings, in this paper we fix input length. Input length can be very long (actually we will construct functions of which input bit length are exponential of n), but must be fixed.

This section assumes that we are given an ideal block cipher $E \in \mathsf{Ciph}(m, n)$ with $m \leq n^2$. For a positive number r (r means "rate") with $1 < r < n$ and $\ell \geq 1$, define a padding function $\mathsf{pad}_{r,\ell} : \{0,1\}^n \times \{0,1\}^{\frac{n}{r}\cdot\ell} \to \{0,1\}^n \times \{0,1\}^{m\ell}$ by

$$\mathsf{pad}_{r,\ell} : x\|z_1\|\cdots\|z_\ell \mapsto x\|z_1\|0\|\cdots\|z_i\|(i-1)\|\cdots z_\ell\|(\ell-1),$$

where $z_i \in \{0,1\}^{\frac{n}{r}}$ and we assume that each integer i is expressed as an $(m-n/r)$-bit string. Let us define a function $H^E_{r,\ell} : \{0,1\}^{n+\frac{n}{r}\cdot\ell} \to \{0,1\}^n$ by

$$H^E_{r,\ell}(M) := \mathsf{MD}^{\mathsf{DM}^E}_\ell(\mathsf{pad}_{r,\ell}(M)).$$

The following theorem claims that $H^E_{r,\ell}$ has both non-invertibility and one-wayness.

Theorem 6.1 (Security of Merkle-Damgård with Davies-Meyer). *Let $n \geq 32$ and $m \leq n^2$. Assume $E \in \mathsf{Ciph}(m,n)$ is an ideal cipher. For any quantum adversary $\mathcal{A}$ that makes at most q queries to E,*

$$\mathsf{Adv}^{inv}_{H^E_{r,\ell}}(\mathcal{A}) \leq 4(q+1)\left(\frac{n^{1/2}}{2^{n/2}} + \frac{2^{n/r}(e+1)}{n!}\right) + \epsilon(r,n) \tag{36}$$

and

$$\mathsf{Adv}^{ow}_{H^E_{r,\ell}}(\mathcal{A}) \leq 4(q+1)\left(\frac{n^{1/2}}{2^{n/2}} + \frac{2^{n/r}(e+1)}{n!}\right) + \epsilon(r,n) + \delta(r,\ell,n) \tag{37}$$

holds, where $\epsilon(r,n) = 2^{n/r}\left(\frac{8n^3}{2^n-2n+1} + \frac{48n^3}{2^n} + \frac{3(e+1)}{n!}\right)$ and $\delta(r,\ell,n) = \ell\cdot\left(\frac{2n+1}{2^{n/3r+1}} + \frac{n^2}{2^{n/r-2}}\right)$. In particular, if $\ell \ll 2^{\frac{n}{3r}}$, then $\mathcal{A}$ cannot find a preimage of $H^E_{r,\ell}$ with constant probability for $q \ll 2^{n/2}/n^{1/2}$.

Remark 6.1. We need padding function $\mathsf{pad}_{r,\ell}$ to restrict key space for each message block (see Remark 5.1). Our padding function pads different numbers for different message blocks so that the i-th compression function and the j-th compression function become essentially independent for $i \neq j$.

Proof. Firstly we show non-invertibility, i.e. inequality (36). Non-invertibility of $H^E_{r,\ell}$ is reduced to non-invertibility of the Davies-Meyer construction of the last block. By using an adversary $\mathcal{A}$ to invert $H^E_{r,\ell}$, we construct an adversary $\mathcal{B}$ to invert a Davies-Meyer construction $\mathsf{DM}^{E'}$, where $E' \in \mathsf{Ciph}(n/r,n)$.

At the beginning of a game, $\mathcal{B}$ receives randomly chosen $y \in \{0,1\}^n$ as an input. In addition, $\mathcal{B}$ has oracle access to an ideal cipher $E' \in \mathsf{Ciph}(n/r,n)$. $\mathcal{B}$ simulates an oracle of ideal cipher $E \in \mathsf{Ciph}(m,n)$ as follows. $\mathcal{B}$ chooses $\tilde{E} \in \mathsf{Ciph}(m,n)$ uniformly at random, and define $E \in \mathsf{Ciph}(m,n)$ by

$$E(k,x) = \begin{cases} E'(z,x) \text{ if } k = z\|\ell \text{ for some } z \in \mathsf{Ciph}(n/r,n), \\ \tilde{E}(k,x) \text{ otherwise.} \end{cases} \tag{38}$$

The distribution of E equals to the uniform distribution. $\mathcal{B}$ runs $\mathcal{A}$, giving y as the target image. $\mathcal{B}$ answers queries of $\mathcal{A}$ by using E. After $\mathcal{A}$ outputs a message $M = x\|z_1\|\cdots\|z_\ell \in \{0,1\}^{n+\frac{n}{r}\cdot\ell}$, $\mathcal{B}$ calculates $x_{\ell-1} := H^E_{r,\ell-1}(x\|z_1\|\cdots\|z_{\ell-1})$ and outputs $(z_\ell, x_{\ell-1})$. Note that calculation of $x_{\ell-1}$ does not need any query to E'. Since $\mathsf{DM}^{E'}(z_\ell\|\ell, H^E_{r,\ell-1}(x\|z_1\|\cdots\|z_{\ell-1})) = H^E_{r,\ell}(M) = y$ holds, we have $\mathsf{Adv}^{inv}_{H^E_{r,\ell}}(\mathcal{A}) = \mathsf{Adv}^{inv}_{\mathsf{DM}^{E'}}(\mathcal{B})$, and we obtain the desired bound (36) from Theorem 5.1.

Next we show one-wayness, i.e. inequality (37). Similarly as in Section 5, we reduce one-wayness to non-invertibility. Again, let U_n be the uniform distribution on $\{0,1\}^n$. Let V_1 be the distribution of the random variable which takes values in $\mathsf{Ciph}(m,n) \times \{0,1\}^n$ and is defined by the following sampling:

1. $E \xleftarrow{U_E} \mathsf{Ciph}(m,n)$, $M \xleftarrow{\$} \{0,1\}^{n+\frac{n}{r}\cdot\ell}$
2. $y \leftarrow H^E_{r,\ell}(M)$
3. return (E,y)

Then we have

$$\mathsf{Adv}^{ow}_{H^E_{r,\ell}}(\mathcal{A}) \leq \mathsf{Adv}^{inv}_{H^E_{r,\ell}}(\mathcal{A}) + \Delta(V_1,(U_E,U_n)). \tag{39}$$

Below we upper bound $\Delta(V_1,(U_E,U_n))$ by using intermediate distributions V_2, $\ldots, V_\ell$. For $2 \leq i \leq \ell$, let V_i be the distribution of the random variable which takes values in $\{0,1\}^n$ and is defined by the following sampling:

1. $x\|z_i\|\cdots\|z_\ell \xleftarrow{\$} \{0,1\}^{n+\frac{n}{r}(\ell-i+1)}$
2. $h_{i-1} \leftarrow x$
3. For $j = i,\ldots,\ell$, do:
4. $\quad h_j \leftarrow \mathsf{DM}^E((z_i\|i),h_{j-1})$
5. $y \leftarrow h_\ell$

Note that the above definition is valid even for $i = 1$, and the resulting distribution is equal to V_1. By definition of our padding function pad, function distributions of the compression functions which process the i-th block and j-th block are essentially independent for $i \neq j$. Thus, by Lemma 5.2 we have

$$\Delta(V_i,V_{i+1}), \Delta(V_\ell,(U_E,U_n)) \leq \frac{2n+1}{2^{n/3r+1}} + \frac{n^2}{2^{n/r-2}} \tag{40}$$

for $1 \leq i \leq \ell-1$. Hence $\Delta(V_1,(U_E,U_n))$ is upper bounded by

$$\sum_{i=1}^{\ell-1} \Delta(V_i,V_{i+1}) + \Delta(V_\ell,(U_E,U_n)) \leq \ell \cdot \left(\frac{2n+1}{2^{n/3r+1}} + \frac{n}{2^{n/r-2}}\right). \tag{41}$$

Thus inequality (37) follows from inequality (39) and (41). □

References

1. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III. pp. 65–93 (2017)
2. Ambainis, A., Rosmanis, A., Unruh, D.: 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. pp. 474–483 (2014)
3. Ambainis, A., Rosmanis, A., Unruh, D.: 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. pp. 474–483 (2014)

4. Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. pp. 44–63 (2016)
5. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. In: 39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA. pp. 352–361 (1998)
6. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: Strengths and weaknesses of quantum computing. SIAM J. Comput. **26**(5), 1510–1523 (1997)
7. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. pp. 41–69 (2011)
8. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings. pp. 592–608 (2013)
9. Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. Fortsch. Phys. **46**(4-5), 493–505 (June 1998)
10. Carstens, T.V., Ebrahimi, E., Tabia, G.N., Unruh, D.: On quantum indifferentiability. IACR Cryptology ePrint Archive, Report 2018/257 (2018)
11. Czajkowski, J., Bruinderink, L.G., Hülsing, A., Schaffner, C., Unruh, D.: Post-quantum security of the sponge construction. In: Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. pp. 185–204 (2018)
12. Goldwasser, S., Bellare, M.: Lecture notes on cryptography. Summer course Cryptography and computer security at MIT (1996-2008)
13. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996. pp. 212–219 (1996)
14. Hassani, M.: Derangements and applications. Journal of Integer Sequences **6**(2) (2003)
15. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. IACR Cryptology ePrint Archive (2018)
16. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: 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. pp. 387–416 (2016)
17. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 207–237. Springer (2016)
18. Kelsey, J., Schneier, B.: Second preimages on n-bit hash functions for much less than 2^n work. In: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. pp. 474–490 (2005)
19. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings. pp. 2682–2685 (2010)

20. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012. pp. 312–316 (2012)
21. Mennink, B., Szepieniec, A.: XOR of PRPs in a quantum world. In: Lange, T., Takagi, T. (eds.) PQCrypto 2017. LNCS, vol. 10346, pp. 367–383. Springer (2017)
22. NIST: Fips pub 180-2. National Institute of Standards and Technology (2002)
23. NIST: Fips pub 202. National Institute of Standards and Technology (2014)
24. Patarin, J.: The "coefficients H" technique. In: Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers. pp. 328–345 (2008)
25. Rogaway, P., Shrimpton, T.: Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. pp. 371–388 (2004)
26. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
27. Song, F.: A note on quantum security for post-quantum cryptography. In: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. pp. 246–265 (2014)
28. Song, F., Yun, A.: Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In: Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II. pp. 283–309 (2017)
29. Unruh, D.: Quantum position verification in the random oracle model. In: Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II. pp. 1–18 (2014)
30. Unruh, D.: Revocable quantum timed-release encryption. In: Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. pp. 129–146 (2014)
31. Unruh, D.: Collapse-binding quantum commitments without random oracles. In: 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. pp. 166–195 (2016)
32. Unruh, D.: Computationally binding quantum commitments. In: 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. pp. 497–527 (2016)
33. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. IACR Cryptology ePrint Archive, Report 2018/276 (2018)
34. Zhandry, M.: How to construct quantum random functions. In: 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012. pp. 679–687 (2012)
35. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. pp. 758–775 (2012)
36. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Info. Comput. **15**(7-8), 557–567 (May 2015)