Davies-Meyer Merkle-Damgård Revisited: Variants of Indifferentiability and Random Oracles

Yusuke Naito[1], Kazuki Yoneyama[2], Lei Wang[3], and Kazuo Ohta[3]

[1] Mitsubishi Electoric Corporation
[2] NTT Corporation
[3] The University of Electro-Communications

Abstract. In this paper, we discuss the security of cryptosystems that use hash function DM-MD^E that is Davies-Meyer Merkle-Damgård with ideal cipher E. DM-MD^E is not indifferentiable from random oracle (RO) due to the extension attack and the inverse attack. From the indifferentiability theory, there is some cryptosystem that is secure in the RO model but insecure when RO is replaced with DM-MD^E. However, this does not imply that any cryptosystem secure in the RO model is insecure when RO is replaced with DM-MD^E. Therefore, we analyze the security of cryptosystems with DM-MD^E by using two approaches.

The first approach uses weakened random oracle (WRO). Since the extension attack and the inverse attack can be applied to DM-MD^E but not to RO, we define WRO such that these attacks can be applied, and analyze the security of cryptosystems with DM-MD^E by using WRO.

We propose the *extension attack and inverse attack simulatable random oracle* (EIRO) to which these attacks can be applied. We prove that DM-MD^E is indifferentiable from EIRO. This implies that any cryptosystem secure in the EIRO model is secure when EIRO is replaced with DM-MD^E. We prove that RSA-KEM, FDH, PSS, Fiat-Shamir and so on are secure in the EIRO model. Therefore these cryptosystems are secure when using DM-MD^E. Moreover, we prove that EIRO is equivalent to DM-MD^E. Therefore, the only differences between RO and DM-MD^E lie in the extension attack and the inverse attack. We also prove that FDH, PSS, Fiat-Shamir and so on are secure when using an output length extension (OLE) algorithm (KDF1 (MGF1), KDF2 and KDF3) with DM-MD^E.

The second approach uses a variant of the theory, denoted *indifferentiability with condition*, which is proposed in this paper. While the original indifferentiability theory deals with any cryptosystem, the indifferentiability with condition deals with cryptosystems that satisfy some condition. As an example, we consider cryptosystems that satisfy the condition "prefix-free" (PF cryptosystems) (e.g. OAEP, OAEP+, SAEP, SAEP+ and so on). We show that if DM-MD^E is indifferentiable from RO with the condition "prefix-free", PF cryptosystems are secure when using DM-MD^E. By using the previous result: "the hash function (DM-MD^E with *prefix-free* padding) is indifferentiable from RO", we can prove that DM-MD^E is indifferentiable from RO with the condition "prefix-free" by a simple and clear proof. Therefore, PF cryptosystems are secure when using DM-MD^E. Similarly, PF cryptosystems are secure when using an OLE algorithm (KDF1, KDF2 and KDF3) with DM-MD^E.

Keywords: Variants of random oracle, variant of indifferentiability, Davies-Meyer Merkle-Damgård, cryptosystems with Davies-Meyer Merkle-Damgård, key-derivation functions.

1 Introduction

1.1 Background

A foundational design methodology of cryptosystems is the random oracle (RO) [1]. RO is an ideal hash function and this methodology provides full security to cryptosystems in the RO model. Many practical cryptosystems have been designed on the RO methodology such as ISO standard cryptosystems: OAEP [2], RSA-KEM [21], PSS [3] and so on. However, when instantiating these cryptosystems, RO must be replaced with practical hash functions such as SHA-256 [19]. Therefore, we must confirm the security of cryptosystems when RO is replaced with practical hash functions.

Most hash functions are constructed by iterating a compression function. For example, the famous family of hash functions that includes SHA-1 and SHA-2 uses the Merkle-Damgård (MD)

construction [9, 17]. Let $f : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a compression function. For input M, hash function MD^f, which uses the MD construction and f, calculates the output as follows: (1) calculate $c_i = f(m_i, c_{i-1})$ for $i = 1, \ldots, s$ where $M = m_1 || \cdots || m_s$, $|m_j| = k$ $(j = 1, \ldots, s)$, and c_0 is n bit initial value IV. (2) output c_s.

There is a significant gap between RO and practical hash functions due to the impossible result of RO and hash functions [6]. Standard definitions of hash functions are collision resistance, preimage resistance, and second preimage resistance. At CRYPTO 2005, Coron et al. [8] introduced a new definition of hash functions called indifferentiability from RO that uses the indifferentiability theory [16]. This definition models the ideal situation wherein a hash function behaves like RO. In this definition, a compression function is modeled by fixed input length random oracle FILRO or ideal cipher E. Let I be an ideal function such as FILRO and E and H^I be a hash function that uses I as an underlying primitive. More strictly, hash function H^I is indifferentiable from RO if there exists simulator S such that no distinguisher D can distinguish (H^I, I) from $(\mathsf{RO}, \mathsf{S})$. S can access RO and simulate I. From the indifferentiability theory, if H^I is indifferentiable from RO, any cryptosystem secure in the RO model is secure when RO is replaced by H^I. On the other hand, from the indifferentiability theory, if H^I is not indifferentiable from RO, there is some cryptosystem that is secure in the RO model but insecure when RO is replaced with H^I.

Coron et al. [8] showed that MD^f is not indifferentiable from RO even when f is FILRO. This result is obtained by the fact that the extension attack can be applied to MD^f but not to RO. In the attack, $\mathsf{MD}^f(M||m)$ is calculated by using z and m without M where $z = \mathsf{MD}^f(M)$. Namely $\mathsf{MD}^f(M||m) = f(m, z)$. On the other hand, $\mathsf{RO}(M||m) = \mathsf{S}(m, w)$ does not hold where $w = \mathsf{RO}(M)$, since no S can know M from (m, w). They proposed new constructions such as prefix-free MD and chop MD.

1.2 Rescue Original Merkle-Damgård

Let h be FILRO. Since MD^h is not indifferentiable from RO, there is some cryptosystem that is secure in the RO model but insecure when RO is replaced with MD^h. However, this result does not imply that any cryptosystem secure in the RO model is insecure when RO is replaced with MD^h. Dodis et al. proved that PSS, FDH, Fiat-Shamir and so on are secure when using MD^h[10]. Naito et al. proved that OAEP, OAEP+, RSA-KEM are secure when using MD^h[18]. The security of those cryptosystems was proven by using the weakened random oracle (WRO) approach. Since no simulator S can simulate the extension attack by using only RO, RO must be weakened in order for S to simulate the extension attack. More strictly, (1) define weakened random oracle WRO such that MD^h is indifferentiable, and (2) prove the security of cryptosystems in the WRO model. From the indifferentiability theory, any cryptosystem secure in the WRO model is secure when using MD^h.

Dodis et al. proposed public-use random oracle (pub-RO) as WRO and proved that MD^h is indifferentiable from pub-RO. They proved that FDH, PSS, Fiat-Shamir and so on are secure in the pub-RO model. pub-RO consists of RO and oracle LO that leaks the hash list of RO. Since S can know M from w by using pub-RO where $w = \mathsf{RO}(M)$, for query (m, w), S can return $w' = \mathsf{RO}(M||m)$.

Since OAEP, OAEP+, RSA-KEM and so on are insecure in the pub-RO model, these cryptosystems with MD^h have not been proven by using pub-RO. Naito et al. proposed extension attack simulatable random oracle (ERO) which does not leak information of the hash list of RO that is unnecessary to simulate the extension attack. They proved that MD^h is indifferentiable from ERO and OAEP, OAEP+, RSA-KEM are secure in the ERO model. ERO consists of RO and oracle EO that returns $w' = \mathsf{RO}(M||m)$ for query (m, w) where $w = \mathsf{RO}(M)$. S can simulate the extension attack by using ERO. They also proved that ERO is equivalent to MD^h. Since ERO is RO with the extension attack, the difference between RO and MD^h is just the extension attack.

1.3 Davies-Meyer Merkle-Damgård

The standard hash function SHA-2 family, SHA-1 and so on, have the MD construction and the underlying compression function uses Davies-Meyer (DM) mode which uses a block cipher. These hash functions are provably secure collision resistant hash functions when the underlying block cipher is ideal cipher E [4]. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ (the first element is the key element and the second element is the plaintext element) be an ideal cipher. The compression function DM^E with DM using E is $\mathsf{DM}^E(m,x) = E(m,x) \oplus x$. Previous examinations of the MD construction don't analyze the Davies-Meyer Merkle-Damgård (DM-MD) construction. Since DM^E is not indifferentiable from FILRO [8], we cannot apply the previous results [10, 18] [4] to analyses of cryptosystems with hash function $\mathsf{MD}^{\mathsf{DM}^E}$, denoted hereafter as $\mathsf{DM\text{-}MD}^E$. Therefore, analyzing the security of cryptosystems with $\mathsf{DM\text{-}MD}^E$ is an open problem. Since the SHA-2 family has been used in many cryptosystems, analyzing the security of cryptosystems with $\mathsf{DM\text{-}MD}^E$ is important in practical situations.

1.4 Our Contribution

We will prove various cryptosystems are secure when using $\mathsf{DM\text{-}MD}^E$. We will also prove other cryptosystems are secure when using an output length extension (OLE) algorithm (key derivation functions: KDF1 (MGF1), KDF2 and KDF3 [21]) with $\mathsf{DM\text{-}MD}^E$.

We adopt two approaches: the WRO approach and the indifferentiability with condition approach. By using the first approach, we will prove the following.

- RSA-KEM [21] and pub-RO cryptosystems (FDH [1], PSS [3], Fiat-Shamir [12] and so on) are secure when using $\mathsf{DM\text{-}MD}^E$. pub-RO cryptosystems are cryptosystems secure in the pub-RO model.
- pub-RO cryptosystems are secure when using an OLE algorithm (KDF1, KDF2 and KDF3) with $\mathsf{DM\text{-}MD}^E$.

By using the second approach, we will prove the following.

- FIL cryptosystems (e.g. OAEP [2], OAEP+ [22], SAEP [5], SAEP+ [5] and so on) are secure when using $\mathsf{DM\text{-}MD}^E$ or an OLE algorithm (KDF1, KDF2 and KDF3) with $\mathsf{DM\text{-}MD}^E$. FIL cryptosystems are secure cryptosystems in the RO model wherein the input length of the hash function is fixed.

WRO Approach for $\mathsf{DM\text{-}MD}^E$. We show that $\mathsf{DM\text{-}MD}^E$ is not indifferentiable from RO by using the *inverse attack*. This attack uses the property where E is invertible. More strictly, in this attack, $z_1 = E^{-1}(m, z_2 \oplus z_1)$ holds where $z_1 = \mathsf{DM\text{-}MD}^E(M)$ and $z_2 = \mathsf{DM\text{-}MD}^E(M||m)$. Let $w_1 = \mathsf{RO}(M)$ and $w_2 = \mathsf{RO}(M||m)$. Since for inverse query $(m, w_1 \oplus w_2)$ no S can know w_1, no S can simulate the inverse attack. Therefore, $\mathsf{DM\text{-}MD}^E$ is not indifferentiable from RO due to the inverse attack in addition to the extension attack. We propose a new oracle *extension attack and inverse attack simulatable random oracle* EIRO; it represents ERO with new oracle IO that returns w_1 for query $(m, w_1 \oplus w_2)$. We prove that $\mathsf{DM\text{-}MD}^E$ is indifferentiable from EIRO.

We prove that RSA-KEM and pub-RO cryptosystems are secure in the EIRO model. Since pub-RO leaks information of the hash list of RO, which is unnecessary to simulate the extension

[4] Dodis et al. [10] proved that $\mathsf{MD}^{\mathrm{FIL}_{\mathsf{pub\text{-}RO}}}$ is indifferentiable from pub-RO where FILpub-RO is the fixed input length pub-RO. However, since DM^E is not indifferentiable from FILpub-RO, this analysis cannot be applied to $\mathsf{DM\text{-}MD}^E$ ($= \mathsf{MD}^{\mathsf{DM}^E}$).

attack and the inverse attack, but EIRO does not (pub-RO is weaker than EIRO), attack scenarios in the EIRO are more restricted than those in the pub-RO model. Therefore, pub-RO cryptosystems are also secure in the EIRO model. On the other hand, since EIRO is weaker than ERO (EIRO is ERO with IO), the security of RSA-KEM in the EIRO model cannot be automatically proven by using the proof in the ERO model. We have to prove that RSA-KEM is secure in the EIRO model. Therefore, RSA-KEM and pub-RO cryptosystems are secure when using DM-MD^E.

Moreover, we prove that EIRO is equivalent to DM-MD^E. Since EIRO is RO with the extension attack and the inverse attack, the only differences between RO and DM-MD^E are these attacks.

In practical situations, since the desired output length of hash functions in cryptosystems is usually different from that of existing hash functions, cryptosystems are instantiated by using an OLE algorithm such as KDF1, KDF2 and KDF3 that expand the output length of a hash function [14]. In this paper, we prove that pub-RO cryptosystems are secure when using an OLE algorithm (KDF1, KDF2, and KDF3) with DM-MD^E. For example, the KDF1 case is as follows. Let H be the hash function where the output length is n bit. KDF1 with H where the output length is jn bits is KDF1-$H(M) = H(M||\langle 0\rangle)||H(M||\langle 1\rangle)||\cdots||H(M||\langle j-1\rangle)$ where $\langle i\rangle$ is the 32 bit binary representation value of i. Let pub-RO$_1$ be pub-RO where the output length of RO is n bits and pub-RO$_2$ be pub-RO where the output length of RO is jn bits. For the security of cryptosystems with KDF1-DM-MD^E, we prove that KDF1-pub-RO$_1$ is indifferentiable from pub-RO$_2$. Namely, secure cryptosystems with pub-RO$_2$ are secure when pub-RO$_2$ is replaced by KDF1-pub-RO$_1$. Since pub-RO is weaker than EIRO, secure cryptosystems using KDF1-pub-RO are secure when using KDF1-EIRO. Therefore, pub-RO cryptosystems are secure when using KDF1-EIRO. Since DM-MD^E is indifferentiable from EIRO, pub-RO cryptosystems are secure when pub-RO is replaced with KDF1-DM-MD^E. Similarly, pub-RO cryptosystems are also secure when pub-RO is replaced with KDF2-DM-MD^E or KDF3-DM-MD^E.

Indifferentiability with Condition Approach. We propose a new framework called *the indifferentiability with condition*, a variant of the indifferentiability theory, and propose a new approach to analyzing the security of cryptosystems with DM-MD^E by using the theory.

Let H be a hash function that is indifferentiable from RO. In the indifferentiability from RO, since D is *any* distinguisher, *any* cryptosystem secure in the RO model is secure when RO is replaced with H. In the WRO approach, since DM-MD^E is not indifferentiable from RO, we can recognize the cryptosystems with DM-MD^E secure by choosing secure cryptosystems in the EIRO model from secure cryptosystems in the RO model. In the indifferentiability with condition approach, we can recognize the cryptosystems with DM-MD^E secure by choosing cryptosystems wherein inputs of their hash functions satisfy some condition from the secure cryptosystems in the RO model.

In the indifferentiability from RO, D interacts with (RO, S) and (DM-MD^E, E) and D can make any query. In the indifferentiability with condition, queries from D to RO and DM-MD^E are restricted by some condition. We prove that if DM-MD^E is indifferentiable from RO wherein D is restricted by condition α, cryptosystem $\mathcal{C}$ is secure when RO is replaced with DM-MD^E where $\mathcal{C}$ is secure in the RO model and inputs to hash functions in $\mathcal{C}$ are restricted by condition α.

For example, we consider cryptosystems that satisfy condition "prefix-free". This condition is that for any input values M and M' to a hash function such that $M \neq M'$, M is not the prefix of M'. The previous result [8] proved that DM-MD^E with prefix-free padding PF is indifferentiable from RO where for input M the hash function calculates DM-MD$^E(PF(M))$. By using this result, we prove that no D that is restricted by the condition "prefix-free" can distinguish (DM-MD^E, E) from (RO, S). Therefore DM-MD^E is indifferentiable from RO with the condition "prefix-free".

Next we find cryptosystems that satisfy condition "prefix-free". For example, we consider FIL cryptosystems. For any two values M and M' such that $M \neq M'$ and $|M| = |M'|$, M is not prefix of M'. Therefore, FIL cryptosystems satisfy condition "prefix-free". From the indifferentiability with condition, FIL cryptosystems are secure when using DM-MD^E. The similar discussion holds for FIL cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3).

The indifferentiability with condition approach can be applied to other MD type hash functions such that the hash functions with prefix-free padding are indifferentiable from RO. For example, hash functions using the MD construction with several PGV schemes [7]. FIL cryptosystems and FIL cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3) are secure when using the hash functions.

1.5 Related Works

In the paper of EUROCRYPT 2009 [10], Dodis et al. did not analyze the security of cryptosystems with DM-MD^E. Later, independently to our work, they analyzed the security of cryptosystems (FDH, PSS, Fiat-Shamir and so on) with DM-MD^E by using the WRO approach [11]. They use only pub-RO as WRO and prove that DM-MD^E is indifferentiable from pub-RO.

While their result is the same as a part of our results, WRO in our paper (EIRO) is different from pub-RO. Since pub-RO leaks information of the hash list of RO which EIRO does not, attack scenarios in the EIRO model are restricted more than those in the pub-RO model. Therefore, analyses of cryptosystems in the pub-RO model are more complicated than those in the EIRO model. Since EIRO is equivalent to DM-MD^E but pub-RO is not equivalent to DM-MD^E, there are cryptosystems secure in the EIRO model but insecure in the pub-RO model. For example, RSA-KEM is secure in the EIRO model (proven in this paper) but insecure in the pub-RO model [18]. Therefore, our approach of using EIRO is better than the approach of [11] that uses pub-RO from both theoretical and practical points. Since Dodis et al. [11] did not analyze them, our analyses rescure more practical cryptosystems, e.g., cryptosystems with an OLE algorithm, RSA-KEM and FIL cryptosystems, than their analyses.

Leurent and Nguyen [15] discussed the security of cryptosystems with an OLE algorithm (such as the schemes proposed in [1, 3]). While their interest is for the situation where the underlying compression function is insecure (not collision resistant), our interest is for the situation where the underlying compression function is secure (idea cipher). Our concern is different from theirs, the former is a designer's side and the latter is an attacker's side.

2 Preliminaries

2.1 Notation

For two values x, y, $x||y$ is the concatenated value of x and y. $x \leftarrow y$ means assigning y to x. $\oplus$ is bitwise exclusive or. $|x|$ is the bit length of value x. For set (list) $\mathcal{T}$ and element W, $\mathcal{T} \leftarrow W$ means to insert W into $\mathcal{T}$ (if W is already inserted in $\mathcal{T}$, W is not inserted.). For some jn bit value x, let $x[1], \ldots, x[j]$ be n bit values of each block of x (namely $x = x[1]||\cdots||x[j]$). For some value x, $x_{[w]}$ is the last w bit value of x and $x_{(w)}$ is the value excluding last w bits of x (namely $x = x_{(w)}||x_{[w]}$).

2.2 Davies-Meyer Merkle-Damgård Construction [9, 17, 20]

We first give a short description of the Merkle-Damgård (MD) construction. Hash function $MD^f : \{0,1\}^* \rightarrow \{0,1\}^n$ is built by iterating compression function $f : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ as follows.

– $MD^f(M)$:
  1. calculate $M' = pad(M)$ where pad is a padding function such that $pad : \{0,1\}^* \to (\{0,1\}^k)^*$.
  2. calculate $c_i = f(m_i, c_{i-1})$ for $i = 1, \ldots, l$ where for $i = 1, \ldots, l$, $|m_i| = k$, $M' = m_1||\cdots||m_l$ and c_0 is an initial value (s.t. $|c_0| = n$).
  3. return c_l

The Davies-Meyer Merkle-Damgård ($\mathsf{DM\text{-}MD}$) construction is the MD construction with the underlying compression function instantiated by Davies-Meyer mode (DM). The Davies-Meyer model is $\mathsf{DM}^E(m,x) = x \oplus E(m,x)$ where E is a block cipher and m is a key element of the block cipher. Hereafter E is an ideal cipher and we denote the hash function MD^{DM^E} by $\mathsf{DM\text{-}MD}^E$. In this paper we ignore the above padding function with no loss of generality, so hereafter we discuss only $\mathsf{DM\text{-}MD}^E : (\{0,1\}^t)^* \to \{0,1\}^n$.

We denote forward query (m,x) to E by $(+,m,x)$ and inverse query (m,y) to E by $(-,m,y)$.

2.3 Indifferentiability Framework for Hash Functions [16]

The indifferentiability framework generalizes the fundamental concept of the indistinguishability of two cryptosystems $\mathcal{C}(\mathcal{U})$ and $\mathcal{C}(\mathcal{V})$ where $\mathcal{C}(\mathcal{U})$ is the cryptosystem $\mathcal{C}$ that invokes underlying primitive $\mathcal{U}$ and $\mathcal{C}(\mathcal{V})$ is the cryptosystem $\mathcal{C}$ that invokes underlying primitive $\mathcal{V}$. $\mathcal{U}$ and $\mathcal{V}$ have two interfaces: public and private. Adversaries can only access the public interface and honest parties (e.g. the cryptosystem $\mathcal{C}$) can access only the private interface.

We denote the private interface of the system $\mathcal{W}$ by $\mathcal{W}^{priv}$ and the public interface of the system $\mathcal{W}$ by $\mathcal{W}^{pub}$. The definition of indifferentiability is as follows.

Definition 1. *$\mathcal{V}$ is indifferentiable from $\mathcal{U}$, denote $\mathcal{V} \sqsubset \mathcal{U}$, if for any distinguisher D with binary output (0 or 1) there is a simulator S such that the advantage $|Pr[\mathsf{D}^{\mathcal{V}^{priv},\mathcal{V}^{pub}} \Rightarrow 1] - Pr[\mathsf{D}^{\mathcal{U}^{priv},\mathsf{S}(\mathcal{U}^{pub})} \Rightarrow 1]|$ is negligible in the security parameter k.*

This definition will allow us to use construction $\mathcal{V}$ instead of $\mathcal{U}$ in *any* cryptosystem and retain the same level of provable security due to the indifferentiability theory of Maurer et al. [16]. We denote the same level of provable security by $\mathcal{C}(\mathcal{V}) \succ \mathcal{C}(\mathcal{U})$. Namely, we denote $\mathcal{C}(\mathcal{V}) \succ \mathcal{C}(\mathcal{U})$ in the case that if $\mathcal{C}(\mathcal{U})$ is secure, then $\mathcal{C}(\mathcal{U})$ is secure. More strictly, $\mathcal{V} \sqsubset \mathcal{U} \Leftrightarrow \mathcal{C}(\mathcal{V}) \succ \mathcal{C}(\mathcal{U})$ holds.

For the indifferentiability of $\mathsf{DM\text{-}MD}^E$ from RO, D interacts with $(\mathsf{RO}, \mathsf{S}(\mathsf{RO}))$ and $(\mathsf{DM\text{-}MD}^E, E)$ where S simulates E [8]. In Appendix E, the figure of the indifferentiability of $\mathsf{DM\text{-}MD}^E$ from RO is Fig.1.

2.4 Extension Attack [8]

Coron et al. showed that $\mathsf{DM\text{-}MD}^E \not\sqsubset \mathsf{RO}$ using the extension attack. The extension attack is directed toward the MD construction where we can calculate a new hash value from some hash value. $z' = \mathsf{DM\text{-}MD}^E(M||m)$ can be calculated from just z and m by $z' = E(m,z) \oplus z$ where $z = \mathsf{DM\text{-}MD}^E(M)$. Namely, z' can be calculated without knowing M. The distinguishing attack using the extension attack is as follows. Let $\mathcal{O}_1$ be $\mathsf{DM\text{-}MD}^E$ or RO and let $\mathcal{O}_2$ be E or S. First, a distinguisher poses M to $\mathcal{O}_1$ and gets z from $\mathcal{O}_1$. Second, he poses forward query $(+,m,z)$ to $\mathcal{O}_2$ and gets c from $\mathcal{O}_2$. Finally, he poses $M||m$ to $\mathcal{O}_1$ and gets z' from $\mathcal{O}_1$.

If $\mathcal{O}_1 = \mathsf{DM\text{-}MD}^E$ and $\mathcal{O}_2 = E$, then $z \oplus z' = c$, however, if $\mathcal{O}_1 = \mathsf{RO}$ and $\mathcal{O}_2 = \mathsf{S}$, then $z \oplus z' \neq c$. This is because no simulator can obtain the output value of $\mathsf{RO}(M||m)$ from just (m,z) and the output value of $\mathsf{RO}(M||m)$ is independently and randomly defined from c. Therefore, $\mathsf{DM\text{-}MD}^E \not\sqsubset \mathsf{RO}$ holds.

2.5 Weakened Random Oracle Approach [10, 18]

The weakened random oracle (WRO) approach was proposed to analyze the security of cryptosystems that use MD^h where h is the FILRO. This approach is as follows:

1. Find WRO from which MD^h is indifferentiable.
2. Prove the security of cryptosystems in the WRO model.

If WRO is found, secure cryptosystems in the WRO model are, from the indifferentiable theory, secure when using MD^h.

Dodis et al. [10] proposed public-use random oracle (pub-RO) as WRO. pub-RO consists of random oracle RO and leak oracle LO. This definition proceeds as follows: RO has initially empty list $\mathcal{L}_{\mathsf{RO}}$. For query M to RO, if $\exists(M, z) \in \mathcal{L}_{\mathsf{RO}}$, it returns z. Otherwise, it chooses an n-bit random value, z (assume that the output length of RO is n bit), $\mathcal{L}_{\mathsf{RO}} \leftarrow (M, z)$, and returns z. For a query to LO, it returns $\mathcal{L}_{\mathsf{RO}}$. They showed that FDH, PSS, Fiat-Shamir and so on are secure in the pub-RO model and that MD^h is indifferentiable from pub-RO. Therefore, cryptosystems secure in the pub-RO model are secure when using MD^h [10]. We denote cryptosystems secure in the pub-RO model by pub-RO cryptosystems.

Naito et al. [18] proposed extension attack simulatable random oracle ERO as WRO. ERO consists of RO and extension oracle EO. EO has initially empty list $\mathcal{L}$. For query (m, x) to EO: If $(m, z, z') \in \mathcal{L}$, it returns z'. Else if $z = IV$, EO poses query m to RO, receives z', $\mathcal{L}_{\mathsf{EO}} \leftarrow (m, z, z')$, and returns z'. Else if there exists only one pair $(M, z) \in \mathcal{L}_{\mathsf{RO}}$, EO poses query $M||m$ to RO, receives z', $\mathcal{L}_{\mathsf{EO}} \leftarrow (m, z, z')$, and returns z'. Else it chooses $z' \in \{0,1\}^n$ at random, $\mathcal{L}_{\mathsf{EO}} \leftarrow (m, z, z')$ and returns z'. They showed that OAEP, OAEP+, RSA-KEM and so on are secure in the ERO model and that ERO is indifferentiable from MD^h. Therefore, cryptosystems secure in the ERO model are secure when using MD^h [18].

2.6 KDF1, KDF2 and KDF3 [21]

The desired output length of hash functions in cryptosystems is usually different from that of existing hash functions. Therefore, the output length of hash functions is expanded by an output length extension (OLE) algorithm such as KDF1 (MGF1), KDF2 and KDF3. These algorithms are as follows. Let H be the hash function whose output length is n bits and $\langle i \rangle$ be w bit binary representation of i (usually $w = 32$). When extending from n bits to jn bits by KDF1, KDF1-$H(M)$ is defined by $H(M||\langle 0 \rangle)||H(M||\langle 1 \rangle)||\cdots||H(M||\langle j-1 \rangle)$. When extending from n bits to jn bits by KDF2, KDF2-$H(M)$ is defined by $H(M||\langle 1 \rangle)||H(M||\langle 2 \rangle)||\cdots||H(M||\langle j \rangle)$. When extending from n bits to jn bits by KDF3, KDF3-$H(M)$ is defined by $H(\langle 0 \rangle||M)||H(\langle 1 \rangle||M)||\cdots||H(\langle j-1 \rangle||M)$.

We denote the cryptosystem $\mathcal{C}$ with KDF1 by $\mathcal{C}$-KDF1, the cryptosystem $\mathcal{C}$ with KDF2 by $\mathcal{C}$-KDF2 and the cryptosystem $\mathcal{C}$ with KDF3 by $\mathcal{C}$-KDF3.

Let $\mathsf{RO}_1, \ldots \mathsf{RO}_j$ be independent random oracles. Since the output of $\mathsf{RO}_1(M)||\mathsf{RO}_2(M)||\cdots||\mathsf{RO}_j(M)$ is chosen at random, we can see that $\mathsf{RO}_1||\mathsf{RO}_2||\cdots||\mathsf{RO}_j$ is a random oracle whose output length is jn bits. In the case of KDF1, since we can see that $\mathsf{RO}_1(*||\langle 0 \rangle), \mathsf{RO}_1(*||\langle 1 \rangle), \ldots, \mathsf{RO}_1(*||\langle j-1 \rangle)$ are independent random oracles, we can see that KDF1-RO_1 is a random oracle. The same is true for the cases of KDF2 and KDF3. Therefore, the following holds.

Lemma 1. *For any cryptosystem $\mathcal{C}$ secure in the* RO *model, $\mathcal{C}$-*KDF1*, $\mathcal{C}$-*KDF2 *and $\mathcal{C}$-*KDF3 *are secure in the* RO *model.*

3 WRO Approach for DM-MD^E

In this section, by using the WRO approach, we show that RSA-KEM and pub-RO cryptosystems (FDH, PSS, Fiat-Shamir and so on) are secure when using DM-MD^E and pub-RO cryptosystems are secure when using an OLE algorithm (KDF1, KDF2, and KDF3) with DM-MD^E.

We show the inverse attack that enables D to distinguish (DM-MD$^E, E$) from (RO, S). We propose a new oracle extension attack and inverse attack simulatable random oracle EIRO as WRO, which enables S to simulate the extension attack and the inverse attack. We prove DM-MD^E is equivalent to EIRO (DM-MD$^E \sqsubset$ EIRO and EIRO $\sqsubset$ DM-MD^E). Since EIRO is RO with the extension attack and the inverse attack, the only differences between RO and DM-MD^E are these properties. We prove that RSA-KEM and pub-RO cryptosystems are secure in the EIRO model. We also prove that pub-RO cryptosystems are secure when using KDF1-EIRO, KDF2-EIRO and KDF3-EIRO.

3.1 Inverse Attack

In this subsection we show the inverse attack that enables (DM-MD$^E, E$) to be distinguished from (RO, S). This attack uses the property that block ciphers are invertible. In this attack, $z = E^{-1}(m, z \oplus z')$ holds for $z =$ DM-MD$^E(M)$ and $z' =$ DM-MD$^E(M||m)$. We show the distinguishing attack that uses this attack as follows.

In the ideal cipher scenario, on inverse query $(-, m, y)$ where $y = z \oplus z'$ such that $z =$ DM-MD$^E(M), z' =$ DM-MD$^E(M||m)$, E returns $z =$ DM-MD$^E(M)$. However, in the RO scenario, no simulator S can simulate the inverse attack. On inverse query $(-, m, y)$ where $y = z \oplus z'$ where $z =$ RO(M) and $z' =$ RO$(M||m)$, no S can return z, since no S can know z and z' from (m, y) by using just RO.

Therefore DM-MD$^E \not\sqsubset$ RO holds due to the inverse attack.

3.2 EIRO

The extension attack and the inverse attack separate RO and DM-MD^E in the indifferentiability theory. In this subsection, we propose EIRO which enables S to simulate the attacks. EIRO consists of three oracles, RO, EO and inverse oracle IO. EO is defined in [18] and enables simulation of the extension attack. Note that EO used in our analyses is slightly different from that in [18]. IO enables to simulate the inverse attack. EO and IO have list $\mathcal{L}$ that is initially empty.

- EO: For query (m, x) where $|x| = n$,
  1. If $m = \perp$, $y \leftarrow \perp$ and go to step 7.
  2. Else if $\exists(m, x, y') \in \mathcal{L}$, $y \leftarrow y'$. (if there are two or more such triples, choose a triple at random, $y \leftarrow y'$ of the triple.)
  3. Else if $x = IV$, $z \leftarrow$ RO(m) and $y \leftarrow z \oplus x$.
  4. Else if there is only one pair $(M, x) \in \mathcal{L}_{\mathsf{RO}}$, $z \leftarrow$ RO$(M||m)$ and $y \leftarrow z \oplus x$.
  5. Else choose y from $\{0,1\}^n$ at random.
  6. $\mathcal{L} \leftarrow (m, x, y)$.
  7. returns y.
- IO: For query (m, y) where $|y| = n$,
  1. If $m = \perp$, $x \leftarrow \perp$ and go to step 7.
  2. Else if $\exists(m, x', y) \in \mathcal{L}$, $x \leftarrow x'$. (if there are two or more such triples, chooses a triple at random, $x \leftarrow x'$ of the triple.)
  3. Else if $\exists(m, y \oplus IV) \in \mathcal{L}_{\mathsf{RO}}$, $x \leftarrow IV$.

4. Else if $\exists(M, z), (M||m, z \oplus y) \in \mathcal{L}_{\mathsf{RO}}$, $x \leftarrow z$.
5. Else choose x from $\{0,1\}^n$ at random.
6. $\mathcal{L} \leftarrow (m, x, y)$.
7. returns x.

Note that when we prove EIRO is equivalent to DM-MD^E, the length of first elements m of EO and IO are fixed length k, the length of the key element of E. When we prove the security of cryptosystems in EIRO model, this length is any length. Since EIRO wherein this length is fixed is stronger than EIRO wherein this length is not fixed, this restriction does not affect our security analyses.

3.3 Relationship between DM-MD^E and EIRO in the Indifferentiability Framework

In this section we prove DM-MD$^E \sqsubset$ EIRO and EIRO $\sqsubset$ DM-MD^E as follows. In theorem 1, we use statements σ_H and q_E instead of the total number of queries, q. σ_H is the total number of message blocks for RO/DM-MD^E and q_E is the total number of queries to S/E. Fig.2 in Appendix E shows the indifferentiability of DM-MD^E from EIRO.

Theorem 1. DM-MD$^E \sqsubset$ EIRO*, for any* t_D*, with* $t_S = O(q_E)$ *and* $\epsilon \leq \frac{4(q_H+\sigma_H)^2+2(q_E+\sigma_H)}{2^n}$.

This proof is given in subsection 3.4.

In theorem 2, we use statements σ_H and q_E instead of the total number of queries q. σ_H is the total number of message blocks for RO/DM-MD^E and q_E is the total number of queries to (EO, IO)/S. Fig.4 in Appendix E shows the indifferentiability of EIRO from DM-MD^E.

Theorem 2. EIRO $\sqsubset$ DM-MD^E*, for any* t_D*, with* $t_S = O(q_E)$ *and* $\epsilon \leq \frac{4(q_H+\sigma_H)^2+2(q_E+\sigma_H)}{2^n}$.

This proof is given in subsection B.

From Theorem 1 and Theorem 2, EIRO is equivalent to DM-MD^E in the indifferentiability theory.

3.4 Proof of Theorem 1

First we define simulator S as follows. We define chain triples as follows.

Definition 2 (Chain Triples). *Triples* $(m_1, x_1, y_1), \ldots, (m_i, x_i, y_i)$ *are chain triples if* $x_1 = IV$ *and* $x_{j+1} = x_j \oplus y_j$ $(j = 1, \ldots, i-1)$ *holds.*

Simulator S: On a forward query $(+, m, x)$: (1) $y \leftarrow \mathsf{EO}(m, x)$. (2) S returns y.
On an inverse query $(-, m, y)$: (1) $x \leftarrow \mathsf{IO}(m, y)$. (2) S returns x.
The running time of S is at most $O(q_E)$ time.

We need to prove that D cannot tell apart two scenarios: EIRO and DM-MD^E. In one scenario, D has oracle access to RO and S, while in the other D has access to DM-MD^E and E. The proof involves a hybrid argument starting in the EIRO scenario, and ending in the DM-MD^E scenario through a sequence of mutually indistinguishable hybrid games. Fig.3 in Appendix E shows the game structure in this proof.

Game 1: This is the EIRO model, where D has oracle access to RO and S. Let G1 denote the event that D outputs 1 after interacting with RO and S. Thus $Pr[\mathsf{G1}] = Pr[D^{\mathsf{RO},\mathsf{S}(\mathsf{EIRO})} = 1]$.

Game 2: In this game, we give the distinguisher oracle access to a dummy relay algorithm R_0 instead of direct oracle access to RO. R_0 is given oracle access to RO. On query M to R_0, the response value is $R_0(M) = \mathsf{RO}(M)$. Let $\mathsf{G2}$ denote the event that D outputs 1 in Game 2. Since the view of D remains unchanged in this game, $Pr[\mathsf{G2}] = Pr[\mathsf{G1}]$.

Game 3: In this game, we modify the relay algorithm R_0 to R_1 as follows. For hash oracle query M, R_1 applies the $\mathsf{DM\text{-}MD}$ construction to M by making forward queries to S. R_1 is essentially the same as $\mathsf{DM\text{-}MD}^{\mathsf{S}}$.

We show that Game 3 is identical to Game 2 unless the following bad events occur. For inverse query $(-, m, y)$, IO chooses response x in Step 5:

- $\mathsf{E1}$: It is the case that $x = IV$.
- $\mathsf{E2}$: There is a pair $(M, z) \in \mathcal{L}_{\mathsf{RO}}$ such that $x = z$.

For query M to RO, RO returns z:

- $\mathsf{E3}$: $z = IV$
- $\mathsf{E4}$: There is a pair $(M', z') \in \mathcal{L}_{\mathsf{RO}}$, with $M \neq M'$ such that $z = z'$.
- $\mathsf{E5}$: There is a triple $(m', x', y') \in \mathcal{L}$ such that $z = x'$ where if (m', x', y') is defined by IO, the triple is defined in Step 5 of EO or Step 5 of IO.

We demonstrate that Game 3 is identical to Game 2 unless bad events occur and the probability that bad events occur is negligible. First we give a useful property as follows.

Lemma 2. *For any chain triples $(m_1, x_1, y_1), \ldots, (m_i, x_i, y_i)$ in $\mathcal{L}$, $x_i \oplus y_i = \mathsf{RO}(m_1 || \cdots || m_i)$ holds unless bad events occur.*

Proof. On the contrary, assume that $\exists$ chain triples $(m_1, x_1, y_1), \ldots, (m_i, x_i, y_i) \in \mathcal{L}$ such that $y_i \oplus x_i \neq \mathsf{RO}(m_1 || \cdots || m_i)$.

We consider two cases: (Case 1) $\forall j \in \{1, \ldots, i\} : y_j \oplus x_j \neq \mathsf{RO}(m_1 || \cdots || m_j)$. (Case 2) $\exists j \in \{1, \ldots, i-1\}$ such that $y_j \oplus x_j = \mathsf{RO}(m_1 || \cdots || m_j)$ (Note that since $y_i \oplus x_i \neq \mathsf{RO}(m_1 || \cdots || m_i)$, $j \neq i$).

We consider Case 1. From the condition of this case, $y_1 \oplus x_1 \neq \mathsf{RO}(m_1)$ holds. (m_1, x_1, y_1) is defined by EO or IO. Since $x_1 = IV$, if (m_1, x_1, y_1) is defined by EO, the step that defines (m_1, x_1, y_1) is Step 3 of EO. Therefore, in this case $y_1 \oplus x_1 = \mathsf{RO}(m_1)$. This contradicts Case 1. If (m_1, x_1, y_1) is defined by IO, since $x_1 = IV$ and $x_1 \oplus y_1 \neq \mathsf{RO}(m_1)$, this triple is defined in Step 5 of IO. Therefore, event $\mathsf{E1}$ occurs.

We consider Case 2. We assume that j is the maximum number in $\{1, \ldots, i-1\}$ such that $y_j \oplus x_j = \mathsf{RO}(m_1 || \cdots || m_j)$ holds. We divide Case 2 into two cases: (Case 2-1) $(m_{j+1}, x_{j+1}, y_{j+1})$ is defined by RO. (Case 2-2) $(m_{j+1}, x_{j+1}, y_{j+1})$ is not defined by RO.

We consider Case 2-1. In this case, $\exists M$ such that $x_{j+1} \oplus y_{j+1} = \mathsf{RO}(M || m_{j+1})$. From the condition of j, $M \neq m_1 || \cdots || m_j$ holds. We divide Case 2-1 into two cases: (Case 2-1-1) $M = \perp$. (Case 2-1-2) $M \neq \perp$.

In Case 2-1-1, $x_{j+1} \oplus y_{j+1} = \mathsf{RO}(m_{j+1})$ holds. From the definition of EIRO, the step where $(m_{j+1}, x_{j+1}, y_{j+1})$ is defined by RO is Step 3 of EO, Step 4 of EO, Step 3 of IO or Step 4 of IO. Since $M = \perp$, this step is Step 3 of EO or Step 3 of IO. From the condition of executing Step 3 of EO or Step 3 of IO, $x_{j+1} = IV$ holds. Since $x_{j+1} = x_j \oplus y_j = \mathsf{RO}(m_1 || \cdots || m_j)$ and $x_{j+1} = IV$ hold, event $\mathsf{E3}$ occurs.

In Case 2-1-2, $M \neq \perp$ holds. From the definition of EIRO, the step where $(m_{j+1}, x_{j+1}, y_{j+1})$ is defined by RO is Step 3 of EO, Step 4 of EO, Step 3 of IO or Step 4 of IO. Since $M \neq \perp$ holds, this

step is Step 4 of EO or Step 4 of IO. From the condition of executing Step 4 of EO or Step 4 of IO, $x_{j+1} = \mathsf{RO}(M)$ holds. Since $x_{j+1} = x_j \oplus y_j = \mathsf{RO}(m_1||\cdots||m_j)$ and $x_{j+1} = \mathsf{RO}(M)$ holds, event $\mathsf{E4}$ occurs.

We consider Case 2-2. Since $(m_{j+1}, x_{j+1}, y_{j+1})$ is not defined by RO, this triple is defined in Step 5 of EO or Step 5 of IO. We consider the case that $(m_{j+1}, x_{j+1}, y_{j+1})$ is defined in Step 5 of EO. In this case, since $x_{j+1} = x_j \oplus y_j = \mathsf{RO}(m_1||\cdots||m_j)$ holds, when (m_j, x_j, y_j) is defined, $(m_{j+1}, x_{j+1}, y_{j+1})$ is already defined (If (m_j, x_j, y_j) is defined before defining $(m_{j+1}, x_{j+1}, y_{j+1})$, $x_{j+1} \oplus y_{j+1} = \mathsf{RO}(m_1||\cdots||m_{j+1})$ holds from Step 4 of EO). Therefore in this case event $\mathsf{E5}$. Finally, we consider the case that $(m_{j+1}, x_{j+1}, y_{j+1})$ is defined in Step 5 of IO. This case occurs in event $\mathsf{E2}$ or $\mathsf{E5}$.

From the above discussions, if $y_i \oplus x_i \neq \mathsf{RO}(m_1||\cdots||m_i)$ holds, then a bad event occurs. □

Next by using Lemma 2 we prove that the view of D in Game 3 is identical to that in Game 2 unless a bad event occurs. We prove this by the same technique as [13]. First, since the definition of R_1 is different from R_0, we prove that outputs of R_1 are identical with those of R_0 unless a bad event occurs. Second, since R_0 does not access S and R_1 accesses S, we prove that R_0 is consistent with S as "R_1 is consistent with S".

From Lemma 2, for any chain triples $(m_1, x_1, y_1), \ldots, (m_i, x_i, y_i) \in \mathcal{L}$, $x_i \oplus y_i = \mathsf{RO}(m_1||\cdots||m_i)$ holds. Since R_1 is the Davies-Meyer Merkle-Damgård hash function with S, for any query M $R_1(M) = \mathsf{RO}(M)$ holds unless a bad event occurs. For any query M, outputs R_0 are $\mathsf{RO}(M)$. Therefore, the outputs of R_1 are the same as those of R_0.

Second we discuss consistency. From Lemma 2, for any chain triples $(m_1, x_1, y_1), \ldots, (m_i, x_i, y_i) \in \mathcal{L}$, $x_i \oplus y_i = \mathsf{RO}(m_1||\cdots||m_i) = R_0(m_1||\cdots||m_i)$ holds. Therefore, R_0 is consistent with S as "R_1 is consistent with S".

Finally we show the probability that a bad event occurs.

Lemma 3. *$Pr[\mathsf{E1} \vee \mathsf{E2} \vee \mathsf{E3} \vee \mathsf{E4} \vee \mathsf{E5}] \leq \frac{q_2^2 + 2q_1q_2 + q_1 + q_2}{2^n}$ where q_1 is the maximum number of times the simulator is invoked and q_2 is the maximum number of times RO is invoked.*

Proof. We will examine each of the five events and determine bounds of their probability. Since event $\mathsf{E1}$ is that a random value is equal to IV, the probability that $\mathsf{E1}$ occurs is $Pr[\mathsf{E1}] \leq 1 - (\frac{2^n-1}{2^n})^{q_1} \leq \frac{q_1}{2^n}$. Since event $\mathsf{E2}$ is that a random value is equal to some output value of RO, the probability that $\mathsf{E2}$ occurs is $Pr[\mathsf{E2}] \leq 1 - (\frac{2^n-q_2}{2^n})^{q_1} \leq \frac{q_1q_2}{2^n}$. Since event $\mathsf{E3}$ is that some output of RO is equal to IV, the probability that $\mathsf{E3}$ occurs is $Pr[\mathsf{E3}] \leq \frac{q_2}{2^n}$. Since event $\mathsf{E4}$ is that a collision of RO occurs, $Pr[\mathsf{E4}] \leq 1 - \frac{2^n-1}{2^n} \cdots \frac{2^n-q_2+1}{2^n} \leq \frac{q_2^2}{2^n}$. Since event $\mathsf{E5}$ is some output of RO is equal to the second element value of some triple in $\mathcal{L}$, the probability that $\mathsf{E5}$ occurs is $Pr[\mathsf{E5}] \leq \frac{q_1q_2}{2^n}$. Therefore, $Pr[\mathsf{E1} \vee \mathsf{E2} \vee \mathsf{E3} \vee \mathsf{E4} \vee \mathsf{E5}] \leq Pr[\mathsf{E1}] + Pr[\mathsf{E2}] + Pr[\mathsf{E3}] + Pr[\mathsf{E4}] + Pr[\mathsf{E5}] \leq \frac{q_2^2 + 2q_1q_2 + q_1 + q_2}{2^n}$. □

Let $\mathsf{G3}$ denote the event that distinguisher D outputs 1 in Game 3, $\mathsf{B2}$ be the event wherein $\mathsf{E1} \vee \mathsf{E2} \vee \mathsf{E3} \vee \mathsf{E4} \vee \mathsf{E5}$ occurs in Game 2 and $\mathsf{B3}$ be the event wherein $\mathsf{E1} \vee \mathsf{E2} \vee \mathsf{E3} \vee \mathsf{E4} \vee \mathsf{E5}$ occurs in Game 3. From Lemma 3, since $q_1 \leq q_E$ and $q_2 \leq q_E + \sigma_H$ in Game 2 and $q_1 \leq q_E + \sigma_H$ and $q_2 \leq q_E + \sigma_H$ the probability that bad events occur in Game 2 is less than $\frac{(q_E+\sigma_H)^2 + 2q_E(q_E+\sigma_H) + 2q_E + \sigma_H}{2^n}$ and the probability that bad events occur in Game 3 is less than $\frac{3(q_H+\sigma_H)^2 + 2(q_E+\sigma_H)}{2^n}$. Therefore, $|Pr[\mathsf{G3}] - Pr[\mathsf{G2}]| = |Pr[\mathsf{G3} \wedge \mathsf{B3}] + Pr[\mathsf{G3} \wedge \neg\mathsf{B3}] - Pr[\mathsf{G2} \wedge \mathsf{B2}] - Pr[\mathsf{G2} \wedge \neg\mathsf{B2}]| \leq |Pr[\mathsf{G3}|\mathsf{B3}] \times Pr[\mathsf{B3}] - Pr[\mathsf{G2}|\mathsf{B2}] \times Pr[\mathsf{B2}]| \leq \max\{Pr[\mathsf{B2}], Pr[\mathsf{B3}]\} = \frac{3(q_H+\sigma_H)^2 + 2(q_E+\sigma_H)}{2^n}$.

Game 4: In this Game, we modify simulator S to S_1. RO is removed from simulator S_1 as follows. S_1 has initially empty list $\mathcal{T}$.

For forward query $(+, m, x)$,

1. If $\exists(m, x, y') \in \mathcal{T}$, $y \leftarrow y'$. (if there are two or more such triples, choose a triple at random and $y \leftarrow y'$.)
2. Else S_1 chooses y from $\{0,1\}^n$ at random.
3. $\mathcal{T} \leftarrow (m, x, y)$.
4. S_1 responds with y.

For inverse query $(-, m, y)$,

1. If $\exists(m, x', y) \in \mathcal{T}$, $x \leftarrow x'$. (if there are two or more such triple, choose a triple at random and $x \leftarrow x'$.)
2. Else S_1 chooses x from $\{0,1\}^n$ at random.
3. $\mathcal{T} \leftarrow (m, x, y)$.
4. S_1 responds with x.

An output of S is chosen at random or chosen by RO. Therefore, for any fresh query to S, the response is chosen at random. Since RO is invoked only by S, no D can access RO. Namely, no D distinguish S_1 from S, though RO is removed in S_1, so Game 4 is identical to Game 3. Let $\mathsf{G4}$ denote the event that distinguisher D outputs 1 in Game 4. $Pr[\mathsf{G4}] = Pr[\mathsf{G3}]$ holds.

Game 5. This is the final game. In this game, we replace S_1 with ideal cipher E. Let $\mathsf{G5}$ be the event that D outputs 1 in Game 5. Since the outputs of S_1 are chosen at random, if a collision of outputs of S_1 does not occur, the view of Game 5 is equal to that of Game 4. Let Coll be the event that a collision of outputs of S_1 occurs. $|Pr[\mathsf{G5}] - Pr[\mathsf{G4}]| = |Pr[\mathsf{G5}] - (Pr[\mathsf{G4} \wedge \mathsf{Coll}] + Pr[\mathsf{G4} \wedge \neg\mathsf{Coll}])| = Pr[\mathsf{G4} \wedge \mathsf{Coll}] = Pr[\mathsf{Coll}] \times Pr[\mathsf{G4}|\mathsf{Coll}] \leq Pr[\mathsf{Coll}]$. Since the maximum number times S_1 is invoked is $q_E + \sigma_H$, $Pr[\mathsf{Coll}] \leq \frac{(q_E+\sigma_H)^2}{2^n}$. Therefore, $|Pr[\mathsf{G5}] - Pr[\mathsf{G4}]| \leq \frac{(q_E+\sigma_H)^2}{2^n}$.

Now we can complete the proof of the Theorem by combining Games 1 to 5, and observing that Game 1 is the same as EIRO scenario while Game 5 is same as $\mathsf{DM\text{-}MD}^E$ scenario. Hence we can deduce that $\epsilon \leq \frac{4(q_H+\sigma_H)^2+2(q_E+\sigma_H)}{2^n}$. □

3.5 The Security of Cryptosystems in the EIRO Model

In this subsection, we show that RSA-KEM and pub-RO cryptosystems are secure in the EIRO model.

Since pub-RO leaks information that EIRO does not, pub-RO cryptosystems are explicitly secure in the EIRO model. We show this by the indifferentiable theory as follows.

Theorem 3. $\mathsf{EIRO} \sqsubset \mathsf{pub\text{-}RO}$.

Fig.6 in Appendix E shows the indifferentiability of EIRO from pub-RO. In the indifferentiability of EIRO from pub-RO, D interacts with EIRO or $(\mathsf{RO}, \mathsf{S}(\mathsf{pub\text{-}RO}))$ where S simulates EO and IO. If we can prove that no D can distinguish EIRO from $(\mathsf{RO}, \mathsf{S}(\mathsf{pub\text{-}RO}))$, then $\mathsf{pub\text{-}RO} \sqsubset \mathsf{EIRO}$ holds. Since S can obtain hash list $\mathcal{L}_{\mathsf{RO}}$, S can explicitly simulate EO and IO by using pub-RO. Therefore, Theorem 3 holds. Therefore, pub-RO cryptosystems are secure in the EIRO model from the indifferentiability theory.

Next we show that RSA-KEM is secure in the EIRO model. We can also prove the security of RSA-KEM in the EIRO model as well as in the RO model. The definition of RSA-KEM is described in Appendix D.

Theorem 4 (Security of RSA-KEM in the EIRO model). *If the RSA problem is (t', ϵ')-hard, then RSA-KEM satisfies (t, ϵ)-IND-CCA for KEM as follows:*

$$t' = t + (q_{RO} + q_{EO}) \cdot expo,$$
$$\epsilon' \geq \epsilon - \frac{q_D}{n} - \frac{q_{IO}}{|\mathbb{Z}_n|},$$

where H is modeled as the EIRO, q_{RO} is the number of hash queries to the RO of H, q_{EO} is the number of extension attack queries to the EO of H, q_{IO} is the number of inverse attack queries to the IO of H, q_D is the number of queries to the decryption oracle DO, $|\mathbb{Z}_n|$ is the number of elements of $\mathbb{Z}_n$ and expo is the computational cost of exponentiation modulo n.

The full proof of Theorem 4 is shown in Appendix D. From Theorem 1, Theorem 3 and Theorem 4, the following corollary is obtained.

Corollary 1. *$\forall$ cryptosystem $\mathcal{C} \in \{$RSA-KEM and $\mathsf{pub\text{-}RO}$ cryptosystems$\}$, $\mathcal{C}(\mathsf{DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$.*

3.6 Security of Cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3)

In this subsection, we prove that $\mathsf{pub\text{-}RO}$ cryptosystems are secure when using an OLE algorithm (KDF1, KDF2 and KDF3) with $\mathsf{DM\text{-}MD}^E$. Let H be $\mathsf{pub\text{-}RO}$, H_{RO} be RO of H whose output length is jn bits and H_{LO} be LO of H. Let $\mathcal{L}_{H_{\mathsf{RO}}}$ be the hash list of H_{RO}. Let F be EIRO, F_{RO} be RO of F whose output length is n bits, F_{EO} be EO of F, and F_{IO} be IO of F. Let $\mathcal{L}_{F_{\mathsf{RO}}}$ be the hash list of F_{RO} and $\mathcal{L}_F$ be the list of EO and IO. We prove these cryptosystems by proving $\mathsf{KDF1}$-$F \sqsubset H$, $\mathsf{KDF2}$-$F \sqsubset H$ and $\mathsf{KDF3}$-$F \sqsubset H$. If above points are proven, since $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{EIRO}$ and $\mathsf{EIRO} \sqsubset \mathsf{pub\text{-}RO}$ hold, cryptosystems secure in the $\mathsf{pub\text{-}RO}$ model are also secure when using $\mathsf{KDF1\text{-}DM\text{-}MD}^E$, $\mathsf{KDF2\text{-}DM\text{-}MD}^E$ and $\mathsf{KDF3\text{-}DM\text{-}MD}^E$. For example, we discuss the KDF1 case. The same discussion can be applied to KDF2 and KDF3.

In theorem 5, we use statements σ, q_{RO}, q_{EO} and q_{IO} instead of the total number of queries, q. σ is the total number of message blocks for $\mathsf{KDF1}$-$F_{\mathsf{RO}}/H_{\mathsf{RO}}$, q_{RO} is the total number of queries for $F_{\mathsf{RO}}/\mathsf{S}$ of RO q_{EO} is the total number of queries for $F_{\mathsf{EO}}/\mathsf{S}$ of EO, q_{IO} is the total number of queries for $F_{\mathsf{IO}}/\mathsf{S}$ of IO.

Theorem 5. *$\mathsf{KDF1}$-$F \sqsubset H$ for any t_D, with $t_S = O((q_{\mathsf{RO}}+\sigma)(q_{\mathsf{EO}}+q_{\mathsf{IO}}))$ and $\epsilon \leq \frac{j(\sigma+q_{\mathsf{RO}}+q_{\mathsf{EO}}+q_{\mathsf{IO}})(q_{\mathsf{EO}}+q_{\mathsf{IO}})}{2^n}$.*

This proof is given in Appendix C. Fig.7 in Appendix E shows the indifferentiability of $\mathsf{KDF1}$-F from H.

Similarly, the following theorem can be proven.

Theorem 6. *$\mathsf{KDF2}$-$F \sqsubset H$ and $\mathsf{KDF3}$-$F \sqsubset H$ for any t_D, with $t_S = O((q_{\mathsf{RO}} + \sigma)(q_{\mathsf{EO}} + q_{\mathsf{IO}}))$ and $\epsilon \leq \frac{j(\sigma+q_{\mathsf{RO}}+q_{\mathsf{EO}}+q_{\mathsf{IO}})(q_{\mathsf{EO}}+q_{\mathsf{IO}})}{2^n}$.*

Therefore we can obtain the following corollary.

Corollary 2. *$\forall \mathcal{C} \in \{\mathsf{pub\text{-}RO}$ cryptosystems$\}$, $\mathcal{C}(\mathsf{KDF1\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO}), \mathcal{C}(\mathsf{KDF2\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$ and $\mathcal{C}(\mathsf{KDF3\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$.*

4 Indifferentiability with Condition Approach

In this section, we propose a variant of the indifferentiability theory called *indifferentiability with condition*. By using this theory, we prove that cryptosystems secure in the RO model wherein input length from cryptosystems to hash functions are fixed, denote FIL cryptosystems, (e.g. OAEP, OAEP+, SAEP, SAEP+ and so on) are secure when using $\mathsf{DM\text{-}MD}^E$ or an OLE algorithm (KDF1, KDF2 and KDF3) with $\mathsf{DM\text{-}MD}^E$ by a simple and clear proof.

4.1 Indifferentiability with Condition

In this subsection, we propose the indifferentiability with condition and reveal the relationship between the theory and the security of cryptosystems.

In the indifferentiability from RO, D is *any* distinguisher. Therefore, if hash function H is indifferentiable from RO, *any* cryptosystem secure in the RO model is secure when RO is replaced with H. However, when D is any distinguisher, MD type hash functions are not indifferentiable from RO due to the extension attack. Therefore, we cannot analyze the security of cryptosystems that use the MD type hash function such as Davies-Meyer Merkle-Damgård and so on.

In the indifferentiability with condition, we restrict the behavior of the distinguishers by some condition. More strictly, the definition of the indifferentiability with condition is as follows. Let I be ideal primitive such as FILRO and ideal cipher and H^I a hash function with I.

Definition 3. *Hash function H^I is indifferentiable from RO with condition α, denote $H^I \sqsubset \mathsf{RO}$ with condition α, if for any distinguisher D with binary output (0 or 1) whose queries to H^I and RO are restricted within condition α, there is a simulator, S, such that the advantage $|Pr[\mathsf{D}^{H^I,I} \Rightarrow 1] - Pr[\mathsf{D}^{\mathsf{RO},S(\mathsf{RO})} \Rightarrow 1]|$ is negligible in the security parameter k.*

Fig.9 in Appendix E shows the figure of this definition. In this figure, queries of dotted lines are satisfied with condition α and queries of other lines are not restricted by condition α. By using this definition, we can analyze the security of cryptosystems wherein all inputs from the cryptosystems to hash functions satisfy condition α. More strictly, the following theorem is obtained.

Theorem 7. *Let $\mathcal{C}$ be any cryptosystem whose queries to a hash function are restricted to condition α. Then, $H^I \sqsubset \mathsf{RO}$ with condition $\alpha \Leftrightarrow \mathcal{C}(H^I) \succ \mathcal{C}(\mathsf{RO})$.*

This proof is obtained in a similar way to the proof of Theorem 1 of [16].

Proof. Before starting the proof, we define $\mathcal{C}(H^I) \succ \mathcal{C}(\mathsf{RO})$. We use the same definition as the definition 1 of [16]. Let $\mathcal{C}$ be a cryptosystem wherein queries to hash functions are restricted within condition α and Env is a random system with binary output, called environment.

Definition 4. *$\mathcal{C}(H^I) \succ \mathcal{C}(\mathsf{RO})$ holds if for all environments Env (distinguisher for $\mathcal{C}$) the following holds: For any attacker $\mathcal{A}$ accessing $\mathcal{C}(H^I)$ and I there is another attacker $\mathcal{A}'$ accessing $\mathcal{C}(\mathsf{RO})$ and RO such that the difference between the probability distributions of the binary outputs of $Env^{\mathcal{C}(H^I),\mathcal{A}}$ and $Env^{\mathcal{C}(\mathsf{RO}),\mathcal{A}'}$, $|Pr[Env^{\mathcal{C}(H^I),\mathcal{A}} \Rightarrow 1] - Pr[Env^{\mathcal{C}(\mathsf{RO}),\mathcal{A}'} \Rightarrow 1]|$ is negligible in the security parameter k.*

Fig.10 in Appendix E shows the figure of this definition. In this figure, queries of dotted lines are satisfied with condition α and queries of other lines are not restricted by condition α.

Let us start with the first implication ("$\Rightarrow$"). Fig.11 in Appendix E shows the figure of this proof. Assume that $\forall \mathsf{D}, \exists \mathsf{S}$ such that $|Pr[\mathsf{D}^{H^I,I} \Rightarrow 1] - Pr[\mathsf{D}^{\mathsf{RO},\mathsf{S}(\mathsf{RO})} \Rightarrow 1]|$ is neglitible. We show that $\forall Env, \forall \mathcal{A}, \exists \mathcal{A}'$ such that $|Pr[Env^{\mathcal{C}(H^I),\mathcal{A}} \Rightarrow 1] - Pr[Env^{\mathcal{C}(\mathsf{RO}),\mathcal{A}'} \Rightarrow 1]|$ is negligible. Since for $\forall \mathsf{D}\ \exists \mathsf{S}$, $|Pr[\mathsf{D}^{H^I,I} \Rightarrow 1] - Pr[\mathsf{D}^{\mathsf{RO},S(\mathsf{RO})} \Rightarrow 1]|$ is negligible, for D that is restricted by $\mathsf{D} = Env^{\mathcal{C},\mathcal{A}}$, $|Pr[\mathsf{D}^{H^I,I} \Rightarrow 1] - Pr[\mathsf{D}^{\mathsf{RO},\mathsf{S}(\mathsf{RO})} \Rightarrow 1]|$ is also negligible. We define $\mathcal{A}'$ by combining any attacker $\mathcal{A}$ and S. Then, $|Pr[Env^{\mathcal{C}(H^I),\mathcal{A}} \Rightarrow 1] - Pr[Env^{\mathcal{C}(\mathsf{RO}),\mathcal{A}'} \Rightarrow 1]|$ is negligible.

The second implication ("$\Leftarrow$") is proven similarly. Since we do not use this result, we omit its proof (follows the proof of Theorem 1 of [16]). □

The generalized version of indifferentiability with condition is discussed in Appendix A.

4.2 Confirm the Security of Cryptosystems using Indifferentiability with Condition

We prove the security of cryptosystems with $\mathsf{DM\text{-}MD}^E$ by the following approach. We start by discussing hash function H^I (e.g. $\mathsf{DM\text{-}MD}^E$) where I is the underlying primitive of the hash function (e.g. ideal cipher E).

1. Find condition α such that H^I is indifferentiable from RO with condition α.
2. Find cryptosystem $\mathcal{C}$ whose queries to a hash function are restricted within condition α and which is secure in the RO model.

If the above approach works for some condition α, cryptosystem $\mathcal{C}(H^I)$ is secure from indifferentiability with condition.

We discuss the case that condition α is "prefix-free". By using this condition, we prove that FIL cryptosystems are secure when using $\mathsf{DM\text{-}MD}^E$ or an OLE algorithm (KDF1, KDF2 and KDF3) with $\mathsf{DM\text{-}MD}^E$.

First, we show that $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ with condition "prefix-free". Condition "prefix-free" is that for any different queries M, M' from D to $\mathsf{DM\text{-}MD}^E$ and RO, M is not the prefix of M'. This can be easily and simply proven by using the previous result of prefix-free $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ [8]. Let PF be the prefix-free padding where for any different two values, M' and M, $PF(M)$ is not the prefix of $PF(M')$. The prefix-free $\mathsf{DM\text{-}MD}^E$ is that for input M prefix-free $\mathsf{DM\text{-}MD}^E(M) = \mathsf{DM\text{-}MD}^E(PF(M))$. Note that prefix-free $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ holds for any prefix-free padding.

Theorem 8. $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ *with condition "prefix-free".*

Proof. Since prefix-free $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ [8], no distinguisher D can distinguish (prefix-free $\mathsf{DM\text{-}MD}^E, E$) from $(\mathsf{RO}, \mathsf{S})$. Therefore, no D that is restricted by condition "prefix-free" can distinguish (prefix-free $\mathsf{DM\text{-}MD}^E, E$) from $(\mathsf{RO}, \mathsf{S})$.

Since D is restricted by condition "prefix-free", even when the prefix-free padding is removed, inputs to $\mathsf{DM\text{-}MD}^E$ satisfy "prefix-free". Therefore, no D that is restricted by condition "prefix-free" can distinguish $(\mathsf{DM\text{-}MD}^E, E)$ from $(\mathsf{RO}, \mathsf{S})$. Therefore, $\mathsf{DM\text{-}MD}^E \sqsubset \mathsf{RO}$ with condition "prefix-free" holds. □

Finally, we find cryptosystems that satisfy condition "prefix-free". We pick up FIL cryptosystems and explain that these cryptosystems satisfy this condition. For any M, M' such that $|M| = |M'|$ and $M \neq M'$, M is not the prefix of M'. Therefore, FIL cryptosystems satisfy condition "prefix-free".

From above discussions, the following corollary is obtained.

Corollary 3. $\forall \mathcal{C} \in \{$*FIL cryptosystems*$\}$, $\mathcal{C}(\mathsf{DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$.

From Lemma 1, FIL cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3) are also secure in the RO model. Since the input length of hash functions in FIL cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3) is fixed, the following corollary obtained.

Corollary 4. $\forall \mathcal{C} \in \{$*FIL cryptosystems*$\}$, $\mathcal{C}(\mathsf{KDF1\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$, $\mathcal{C}(\mathsf{KDF2\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$, *and* $\mathcal{C}(\mathsf{KDF3\text{-}DM\text{-}MD}^E) \succ \mathcal{C}(\mathsf{RO})$.

Remark 1. Let H be one of MD type hash functions such that H with the prefix-free padding $\sqsubset \mathsf{RO}$ holds [7]. Then FIL cryptosystems and FIL cryptosystems with an OLE algorithm (KDF1, KDF2 and KDF3) are also secure when using H from the same discussion as the above discussion.

References

1. Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
2. Mihir Bellare and Phillip Rogaway. Optimal Asymmetric Encryption. In *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer, 1994.
3. Mihir Bellare and Phillip Rogaway. The Exact Security of Digital Signatures - How to Sign with RSA and Rabin. In *EUROCRYPT*, volume 1070 of *Lecture Notes in Computer Science*, pages 399–416. Springer, 1996.
4. John Black, Phillip Rogaway, and Thomas Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Functions Constructions from PGV. In *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 103–118. Springer, 2002.
5. Dan Boneh. Simplified OAEP for the RSA and Rabin functions. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 275–291. Springer, 2001.
6. Ran Canetti, Oded Goldreich, and Shai Halevi. The Random Oracle Methodology, Revisited (Preliminary Version). In *STOC*, pages 209–218, 1998.
7. Donghoon Chang, Sangjin Lee, Mridul Nandi, and Moti Yung. Indifferentiable Security Analysis of Popular Hash Functions with Prefix-Free Padding. In *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 283–298. Springer, 2006.
8. Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-Damgård Revisited: How to Construct a Hash Function. In *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 430–448. Springer, 2005.
9. Ivan Damgård. A Design Principle for Hash Functions. In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 416–427. Springer, 1989.
10. Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2009.
11. Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *ePrint 2009/177*, 2009.
12. Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems.
13. Jonathan J. Hoch and Adi Shamir. On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak. In *ICALP*, Lecture Notes in Computer Science, pages 616–630. Springer, 2008.
14. RSA Laboratories. PKCS-1: RSA Cryptography Standard. 2002.
15. Gaëtan Leurent and Phong Q. Nguyen. How Risky Is the Random-Oracle Model? In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2009.
16. Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.
17. Ralph C. Merkle. One Way Hash Functions and DES. In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 428–446. Springer, 1989.
18. Yusuke Naito, Kazuki Yoneyama, Lei Wang, and Kazuo Ohta. How to Confirm Cryptosystems Security: the Original Merkle-Damgård is Still Alive! In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*. Springer, 2009.
19. National Institute of Standards and Technoloty. FIPS PUB 180-3 Secure Hash Standard. In *FIPS PUB*, 2008.
20. Bart Preneel, René Govaerts, and Joos Vandewalle. Hash Functions Based on Block Ciphers: A Synthetic Approach. In *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer, 1993.
21. Victor Shoup. A Proposal for an ISO Standard for Public Key Encryption (version 2.1). 2001.
22. Victor Shoup. OAEP Reconsidered. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer, 2001.

A Generalization of Indifferentiability with Condition

The indifferentiability with condition extends the standard idea of indifferentiability by considering the addition of condition α of queries to private interfaces. The definition of this framework is as follows.

Definition 5. *$\mathcal{V}$ is $(t_D, t_{\mathsf{S}}, q, \epsilon)$ indifferentiable from $\mathcal{U}$ with condition α, denote $\mathcal{V} \sqsubset \mathcal{U}$ with condition α, if for any distinguisher D with binary output (0 or 1) such that queries to a private interface are restricted by condition α there is a simulator S such that $|Pr[\mathsf{D}^{\mathcal{V}^{\mathsf{priv}},\mathcal{V}^{\mathsf{pub}}} \Rightarrow 1] - Pr[\mathsf{D}^{\mathcal{U}^{\mathsf{priv}},\mathsf{S}(\mathcal{U}^{\mathsf{pub}})} \Rightarrow 1]| < \epsilon$. ϵ is negligible in security parameter k.*

Let x be any query from D to a private interface. Then, for any cryptosystem $\mathcal{C}$ such that queries of $\mathcal{C}$ to a private interface are restricted by condition α, $\mathcal{V} \sqsubset \mathcal{U}$ with condition $\alpha \Leftrightarrow \mathcal{C}(\mathcal{V}^{\mathsf{priv}}) \succ \mathcal{C}(\mathcal{U}^{\mathsf{priv}})$ holds. This result is easily proved by extending the proof of Theorem 1 of [16].

B Proof of Theorem 2

We define simulator S as follows.
Simulator S:
On forward query $(+, m, x)$, $y \leftarrow E(m, x)$ and S returns y.
On inverse query $(-, m, y)$, $x \leftarrow E^{-1}(m, y)$ and S returns x.
The running time of S is at most $O(q_E)$ time.

This proof utilizes the proof of Theorem 1. The proof involves a hybrid argument starting in the EIRO scenario, and ending in the $\mathsf{DM\text{-}MD}^E$ scenario through a sequence of mutually indistinguishable hybrid games. Fig.5 in Appendix E shows the game structure in this proof.

Game 1. This game is the same as the EIRO scenario. Let $\mathsf{G1}$ be the event that D outputs 1 in this game. $Pr[\mathsf{G1}] = Pr[D^{\mathsf{EIRO}} \Rightarrow 1]$ holds.

Game 2. In this game, D interacts with $(\mathsf{DM\text{-}MD}^E, E)$. In the proof of Theorem 1, for forward query $(+, m, x)$, S returns the output of $\mathsf{EO}(m, x)$, and for inverse query $(-, m, y)$, S returns the output of $\mathsf{IO}(m, y)$. Therefore, the view of D in Game 1 is identical with that of D in Game 1 of the proof of Theorem 1. Game 2 is identical with Game 5 in the proof of Theorem 1. Let $\mathsf{G2}$ be the event that D outputs 1 in this game. From the proof of Theorem 1, $|Pr[\mathsf{G2}] - Pr[\mathsf{G1}]| \leq \frac{4(q_H+\sigma_H)^2+2(q_E+\sigma_H)}{2^n}$.

Game 3. This is the final game. In this game, D interacts with $(\mathsf{DM\text{-}MD}^E, \mathsf{S})$. Let $\mathsf{G3}$ be the event that D outputs 1 in this game. Since for any query S simply returns the output of E, $Pr[\mathsf{G3}] = Pr[\mathsf{G2}]$.

Now we can complete the proof of Theorem 2 by combining Games 1 to 3, and observing that Game 1 is the same as EIRO scenario while Game 3 is same as $\mathsf{DM\text{-}MD}^E$ scenario. Hence we can deduce that $\epsilon \leq \frac{4(q_H+\sigma_H)^2+2(q_E+\sigma_H)}{2^n}$. □

C Proof of Theorem 5

In indifferentiability for $\mathsf{KDF1}$-F from H, D interacts with $(\mathsf{KDF1}\text{-}F_{\mathsf{RO}}, F)$ and $(H_{\mathsf{RO}}, \mathsf{S}(H))$. We define S that simulates F and show that no D can distinguish $(\mathsf{KDF1}\text{-}F_{\mathsf{RO}}, F)$ from $(H_{\mathsf{RO}}, \mathsf{S}(H))$. S has initially empty list $\mathcal{T}_{\mathsf{RO}}$ and $\mathcal{T}$.

- S of F_{RO}, denote S_{RO}: On query M,
  1. If $(M, z') \in \mathcal{T}_{\mathsf{RO}}$, $z \leftarrow z'$.
  2. Else if $\exists i \in \{0, \ldots, j-1\}$ such that $M_{[w]} = \langle i \rangle$, $z^* \leftarrow H_{\mathsf{RO}}(M_{(w)})$ and $z \leftarrow z^*[i+1]$.
  3. Else, z is chosen from $\{0,1\}^n$ at random.
  4. $\mathcal{T}_{\mathsf{RO}} \leftarrow (M, z)$.
  5. Return z.
- S of F_{EO}, denote S_{EO}: On query (m, x),
  1. Make a leak query to H_{LO} and receive lists $\mathcal{T}_{H_{\mathsf{RO}}}$.
  2. For $\forall (M, z) \in \mathcal{L}_{H_{\mathsf{RO}}}$, for $i = 0, \ldots, j-1$, $\mathcal{T}_{\mathsf{RO}} \leftarrow (M || \langle i \rangle), z[i+1])$.

3. If $m = \perp$, $y \leftarrow \perp$ and goto Step 9.
4. Else if $\exists(m, x, y') \in \mathcal{T}$, $y \leftarrow y'$ (if there are two or more such triples, choose a triple at random, $y \leftarrow y'$ of the triple and go to step 9.).
5. Else if $x = IV$, $z \leftarrow \mathsf{S}_{\mathsf{RO}}(m)$ and $y \leftarrow z \oplus x$.
6. Else if there is only one pair $(M, x) \in \mathcal{T}_{\mathsf{RO}}$, $z \leftarrow \mathsf{S}_{\mathsf{RO}}(M||m)$ and $y \leftarrow z \oplus x$.
7. Else y is chosen from $\{0,1\}^n$ at random.
8. $\mathcal{T} \leftarrow (m, x, y)$.
9. return y.

– S of F_{IO}, denote S_{IO}: On query (m, y),
1. Make a leak query to H_{LO} and receive lists $\mathcal{L}_{H_{\mathsf{RO}}}$.
2. For $\forall(M, z) \in \mathcal{L}_{H_{\mathsf{RO}}}$, for $i = 0, \ldots, j-1$, $\mathcal{T}_{\mathsf{RO}} \leftarrow (M||\langle i \rangle), z[i+1])$.
3. If $m = \perp$, $y \leftarrow \perp$ and goto Step 9.
4. Else if $\exists(m, x', y) \in \mathcal{T}$, $x \leftarrow x'$ (if there are two or more such triples, choose a triple at random, $x \leftarrow x'$ of the triple and go to step 9.).
5. Else if $\exists(m, y \oplus IV) \in \mathcal{T}_{\mathsf{RO}}$, $x \leftarrow IV$.
6. Else if $\exists(M, z), (M||m, z \oplus y) \in \mathcal{T}_{\mathsf{RO}}$, $x \leftarrow z$.
7. Else, x is chosen from $\{0,1\}^n$ at random.
8. $\mathcal{T} \leftarrow (m, x, y)$.
9. return x.

The proof involves a hybrid argument starting in the H scenario, and ending in the $\mathsf{KDF1}$-F scenario through a sequence of mutually indistinguishable hybrid games. Fig.8 in Appendix E shows the figure of games of this proof.

Game 1. In this game, D interacts with $(H_{\mathsf{RO}}, \mathsf{S}(H))$. Let $\mathsf{G1}$ be the event that D outputs 1 in this game. $Pr[\mathsf{D}^{H_{\mathsf{RO}}, \mathsf{S}(H)} \Rightarrow 1] = Pr[\mathsf{G1}]$.

Game 2. In this game, we replace H_{RO} with $\mathsf{KDF1}$-S_{RO}. Namely, for query M, $\mathsf{KDF1}$-S_{RO} returns $\mathsf{S}_{\mathsf{RO}}(M||\langle 0 \rangle)||\cdots||\,\mathsf{S}_{\mathsf{RO}}(M||\langle j-1 \rangle)$. From the definition of S_{RO}, for query $M||\langle i-1 \rangle$ $(i \in \{1, \ldots, j\})$, S_{RO} returns $z[i]$ where $z = H_{\mathsf{RO}}(M)$. Therefore, $\mathsf{KDF1}$-$\mathsf{S}_{\mathsf{RO}}(M) = H_{\mathsf{RO}}(M)$ holds. Let $\mathsf{G2}$ be the event that D outputs 1 in this game. $Pr[\mathsf{G1}] = Pr[\mathsf{G2}]$ holds.

Game 3. This is the final game. In this game, we replace S with F and remove H. Namely this game is the $\mathsf{KDF1}$-F scenario. In Game 2, S is identical with F except for Step 1 and 2 of S_{EO} and Step 1 and 2 of S_{IO}. From the steps, there is the event that there is (M, z) in $\mathcal{T}_{\mathsf{RO}}$ where M is not queried to S_{RO}. This event occurs when M is queried to S_{RO} such that for some $i \in \{0, \ldots, j-1\}$ $M_{[w]} = \langle i \rangle$ and S_{EO} or S_{IO} is invoked, since $(M||\langle 0 \rangle, z[1]), \ldots, (M||\langle i-1 \rangle, z[i]), (M||\langle i+1 \rangle, z[i+2]), \ldots, (M||\langle j-1 \rangle, z[j])$ are inserted in $\mathcal{T}_{\mathsf{RO}}$ where $z = H_{\mathsf{RO}}(M)$ when S_{EO} or S_{IO} is invoked. However, since $z[1], \ldots, z[i], z[i+2], \ldots, z[j]$ are chosen at random and D cannot see $\mathcal{T}_{\mathsf{RO}}$, D cannot know these pairs. If for some $s \in \{0, \ldots, i-1, i+1, \ldots, j-1\}$ $M||\langle s \rangle$ is queried to S_{RO}, since $z[s+1]$ is chosen at random, this query is not helpful for D to distinguish Game 3 from Game 2. However, if for some $s \in \{1, \ldots, i, i+2, \ldots, j\}$ a query corresponding with $z[s]$ is queried to S_{EO} or S_{IO}, D can distinguish Game 3 from Game 2. For example, if $(m, z[s])$ is queried to EO, Step 6 is executed. On the other hand, in EIRO, since $M||\langle 0 \rangle, \ldots, M||\langle i-1 \rangle, M||\langle i+1 \rangle, \ldots, M||\langle j-1 \rangle$ are not inserted in $\mathcal{L}_{H_{\mathsf{RO}}}$, the same event as S does not occurs. Therefore, in Game 2, if for some $s \in \{1, \ldots, i, i+2, \ldots, j\}$ $(M||\langle s-1 \rangle, z[s])$ is queried to S_{RO}, D can distinguish Game 3 from Game 2. However, since no D can know $\mathcal{T}_{\mathsf{RO}}$ and $z[1], \ldots, z[i], z[i+2], \ldots, z[j]$ is chosen from $\{0,1\}^n$ at random, the probability that for some $s \in \{0, \ldots, i-1, i+1, \ldots, j-1\}$ a query corresponding

with $z[s]$ to $\mathsf{S_{EO}}$ or $\mathsf{S_{IO}}$ is made is negligible. More strictly, since the maximum numbre of invoking H_{RO} is $\sigma + q_{\mathsf{RO}} + q_{\mathsf{EO}} + q_{\mathsf{IO}}$ and the maximum number of invoking $\mathsf{S_{EO}}$ and $\mathsf{S_{IO}}$ is $q_{\mathsf{EO}} + q_{\mathsf{IO}}$, the probability is less than $\frac{j(\sigma+q_{\mathsf{RO}}+q_{\mathsf{EO}}+q_{\mathsf{IO}})(q_{\mathsf{EO}}+q_{\mathsf{IO}})}{2^n}$. Let $\mathsf{G3}$ be the event that D outputs 1 in this game and Bad the event that for some $s \in \{1, \ldots, i, i+2, \ldots, j\}$ a query corresponding with $z[s]$ to $\mathsf{S_{EO}}$ or $\mathsf{S_{IO}}$ is made. $|Pr[\mathsf{G3}] - Pr[\mathsf{G2}]| = |Pr[\mathsf{G2} \wedge \mathsf{Bad}] + Pr[\mathsf{G2} \wedge \neg\mathsf{Bad}] - Pr[\mathsf{G3}]| = Pr[\mathsf{G2} \wedge \mathsf{Bad}] \leq Pr[\mathsf{Bad}] \times Pr[\mathsf{G2}|\mathsf{Bad}] \leq Pr[\mathsf{Bad}] \leq \frac{j(\sigma+q_{\mathsf{RO}}+q_{\mathsf{EO}}+q_{\mathsf{IO}})(q_{\mathsf{EO}}+q_{\mathsf{IO}})}{2^n}$ holds.

Therefore $|Pr[\mathsf{D}^{\mathsf{KDF1}\text{-}F,F} \Rightarrow 1] - Pr[\mathsf{D}^{H_{\mathsf{RO}},\mathsf{S}(H)} \Rightarrow 1]| \leq \frac{j(\sigma+q_{\mathsf{RO}}+q_{\mathsf{EO}}+q_{\mathsf{IO}})(q_{\mathsf{EO}}+q_{\mathsf{IO}})}{2^n}$. □

D Security of RSA-KEM

D.1 Security Notion of KEM

First, we briefly review the model and the security notion of KEM schemes.

Definition 6 (Model for KEM Schemes).
A KEM scheme consists of the following 3-tuple (**KEM.Gen**, **KEM.Enc**, **KEM.Dec**)*:*

- **KEM.Gen** *: a key generation algorithm which on input 1^k, where k is the security parameter, outputs a pair of keys (ek, dk). ek and dk are called encryption key and decryption key, respectively.*
- **KEM.Enc** *: an encryption algorithm which takes as input encryption key ek, outputs key K and ciphertext c.*
- **KEM.Dec** *: a decryption algorithm which takes as input decryption key dk and ciphertext c, outputs key K.*

In particular, a scheme which cannot even satisfy one-wayness under chosen plaintext attacks (OW-CPA) cannot be called a KEM scheme. In general, indistinguishability under chosen ciphertext attacks (IND-CCA) is recognized as the strongest security notion. Here, we recall definitions of OW-CPA and IND-CCA for KEM as follows.

Definition 7 (OW-CPA for KEM).
A KEM scheme is (t, ϵ)-OW-CPA for KEM if the following property holds for security parameter k;

For any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, $\Pr[\ (ek, dk) \leftarrow \mathbf{KEM.Gen}(1^k); (state) \leftarrow \mathcal{A}_1(ek); (K^*, c^*) \leftarrow \mathbf{KEM.Enc}(ek); K' \leftarrow \mathcal{A}_2(c^*, state); K' = K^*] \leq \epsilon$, where state is state information which $\mathcal{A}$ wants to preserve from $\mathcal{A}_1$ to $\mathcal{A}_2$ and $\mathcal{A}$ runs in at most t steps.

Definition 8 (IND-CCA for KEM). *A KEM scheme is (t, ϵ)-IND-CCA for KEM if the following property holds for security parameter k; For any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, $|\Pr[\ (ek, dk) \leftarrow \mathbf{KEM.Gen}(1^k); (state) \leftarrow \mathcal{A}_1^{\mathcal{DO}(dk,\cdot)}(ek); b \xleftarrow{R} \{0,1\}; (K_0^*, c_0^*) \leftarrow \mathbf{KEM.Enc}(ek); K_1^* \xleftarrow{R} \mathcal{K}; b' \leftarrow \mathcal{A}_2^{\mathcal{DO}(dk,\cdot)}(ek, (K_b^*, c_0^*), state); b' = b] - 1/2| \leq \epsilon$, where $\mathcal{DO}$ is the decryption oracle, $\mathcal{K}$ is the key space, state is state information which $\mathcal{A}$ wants to preserve from $\mathcal{A}_1$ to $\mathcal{A}_2$ and $\mathcal{A}$ runs in at most t steps. $\mathcal{A}$ cannot submit the ciphertext $c = c_0^*$ to $\mathcal{DO}$.*

D.2 RSA-KEM

The security of RSA-KEM is based on the RSA assumption.

Definition 9 (RSA assumption). *Let n be an RSA modulus that is the product of two large primes (p, q) for security parameter k and e be an exponent such that gcd$(e, \phi(n)) = 1$. We say that the RSA problem is (t, ϵ)-hard if for any adversary Alg,* $\Pr[y \leftarrow \mathbb{Z}_n; Alg(n, e, y) = x; y \equiv x^e \pmod{n}] \leq \epsilon$, *where Alg runs in at most t steps.*

The description of RSA-KEM is as follows:

Key generation : For input k, output encryption key $(ek = (n, e))$ and decryption key $(dk = d)$ such that n is an RSA modulus that is the product of two large primes (p, q) for security parameter k, $\gcd(e, \phi(n)) = 1$ and $ed \equiv 1 \pmod{\phi(n)}$.

Encryption : Generate randomness $r \xleftarrow{R} \mathbb{Z}_n$, compute $c = r^e \mod n$ and $K = H(r)$, and output ciphertext c and key K where $H : \mathbb{Z}_n \to \{0, 1\}^k$ is a hash function.

Decryption : Upon input of ciphertext c, compute $r = c^d \mod n$ and output $K = H(r)$.

In [21], security of RSA-KEM in the RO model is proved as follows;

Lemma 4 (Security of RSA-KEM in the RO model [21]). *If the RSA problem is hard, then RSA-KEM satisfies IND-CCA for KEM where H is modeled as the* RO.

D.3 Insecurity of RSA-KEM in pub-RO Model

Though RSA-KEM is secure in the RO model, it is insecure in the pub-RO model. More specifically, we can show RSA-KEM does not satisfy even OW-CPA for KEM in the pub-RO model.

Theorem 9 (Insecurity of RSA-KEM in the pub-RO model). *Even if the RSA problem is hard, RSA-KEM does not satisfy OW-CPA for KEM where H is modeled as* pub-RO.

Proof. We construct an adversary $\mathcal{A}$ which successfully plays the OW-CPA game by using pub-RO H. The construction of $\mathcal{A}$ is as follows;

Input : (n, e) as the public key

Output : K'

Step 1 : Return *state* and receive c^* as the challenge ciphertext. Pose the leak query to LO of H, obtain the hash list $\{(r, K)\}$.

Step 2 : For all r in $\{(r, K)\}$, check whether $r^e \stackrel{?}{\equiv} c^* \pmod{n}$. If there is r^* that satisfies the relation, output K' which is the tally of (r^*, K').

We estimate the success probability of $\mathcal{A}$. When the challenge ciphertext c^* is generated, r^* such that $K^* = H(r^*)$ is certainly posed to H because c^* is generated in accordance with the protocol description. Thus, $\mathcal{L}_H$ contains (r^*, K^*) where $\mathcal{L}_H$ is the local hash list of H. Therefore, $\mathcal{A}$ can successfully play the OW-CPA game.

□

D.4 Intuition of Proof of Theorem 4

The difference between the proof in the EIRO model and that in the RO model consists in whether or not the adversary can use EO and IO queries. To obtain some information about bit b by an EO query, the adversary has to pose the randomness r^* which was used to generate the challenge ciphertext to RO previously because of the definition of EIRO. However, if the adversary posed r^* to RO, then he has already obtained key K^* and can decide bit b. Thus, the probability that the adversary obtains some information about bit b by an EO query is negligible. Then, using EO queries gives no advantage to the adversary beside RO queries. Also, to obtain some information about bit b by an IO query, the adversary has to pose both the hash query $r^*||r$ to RO and the inverse attack query $(r, H(r^*||r) \oplus K^*)$ to IO for some r because of the definition of EIRO. However, the probability that the adversary poses $r^*||r$ to RO before obtaining information about r^* is negligible. Thus, as in the case of EO, the probability that the adversary obtains some information about bit b by an IO query is negligible. Therefore, we have succeeded in proving that RSA-KEM is secure by way of a proof similar to that used in [21].

D.5 Proof of Theorem 4

First, we transform the experiment of IND-CCA for RSA-KEM into the experiment where queries to DO, EO and IO do not give any advantage to the adversary.

Let Exp0 be the initial experiment and Succ0 be the probability that adversary $\mathcal{A}$ succeeds in guessing bit b in Exp0. $\mathcal{A}$ receives (K_b^*, c_0^*) as the challenge such that $c_0^* = r^{*e}$ for r^*.

Let Exp1 be the same experiment as Exp0 except the case that $\mathcal{A}$ is queried c_0^* to DO before receiving c_0^* as the challenge ciphertext. Exp1 aborts in the above case. Let Succ1 be the probability that $\mathcal{A}$ succeeds in guessing bit b in Exp1 and E_1 be the event that the experiment aborts. Then, the probability that event E_1 occurs is equal or lower than q_D/n because $\mathcal{A}$ has no information about the challenge. Thus, we obtain that $|\mathsf{Succ1} - \mathsf{Succ0}| \leq q_D/n$.

Let Exp2 be the same experiment as Exp1 except the case that the challenge (K_b^*, c_0^*) is generated at the beginning of the experiment. Let Succ2 be the probability that $\mathcal{A}$ succeeds in guessing bit b in Exp2. Then, we trivially obtain that $|\mathsf{Succ2} - \mathsf{Succ1}| = 0$ because the challenge is determined independently from the behavior of $\mathcal{A}$.

Let Exp3 be the same experiment as Exp2 except the case that $\mathcal{A}$ does not pose either the hash query $r^*||r$ to RO or the inverse attack query $(m, H(r^*||r) \oplus K_b^*)$ to IO for some r before posing the hash query r^* to RO. Let Succ3 be the probability that $\mathcal{A}$ succeeds in guessing bit b in Exp3 and E_3 be the event that $\mathcal{A}$ poses both the hash query $r^*||r$ to RO and the inverse attack query $(r, H(r^*||r) \oplus K_b^*)$ to IO for some r before posing the hash query r^* to RO. Also, let AskH be the event that $\mathcal{A}$ poses the hash query $r^*||r$ to RO before posing the hash query r^* to RO. Then, the probability that event E_4 occurs is equal or lower than the probability that event AskH occurs. Moreover, the probability that event AskH occurs is equal or lower than $q_{IO}/|\mathbb{Z}_n|$ because $\mathcal{A}$ has not posed r^* to RO yet and so r^* is unknown for $\mathcal{A}$ because H is RO. Thus, we obtain $|\mathsf{Succ3} - \mathsf{Succ2}| \leq q_{IO}/|\mathbb{Z}_n|$.

Let Exp4 be the same experiment as Exp3 except the case that $\mathcal{A}$ is queried r^* to RO. Exp4 aborts in the above case. Let Succ4 be the probability that $\mathcal{A}$ succeeds in guessing bit b in Exp4 and E_4 be the event that the experiment aborts by this case. Then, to evaluate the probability that event E_4 occurs, $\Pr[E_4]$, we show that $\Pr[E_4]$ is equal or lower than the probability that the RSA problem is broken as follows.

Lemma 5. *If event E_4 occurs with probability ϵ'' in time t'', we can construct an inverter $\mathcal{I}$ that breaks the RSA problem with probability ϵ' in time t' as follows:*

$$t' = t'' + (q_{RO} + q_{EO}) \cdot expo,$$
$$\epsilon' = \epsilon''.$$

Proof. We assume that $\mathcal{A}$ does not repeat previous hash queries to the EIRO H or previous decryption queries to the DO. Let $\mathcal{L}_H$ be the local hash list of H. $\mathcal{L}_H$ consists of tuples (r_i, c_i, h_i) $(0 \leq i \leq q_{RO} + q_D + q_{EO})$. Let $\mathcal{L}$ be the local EO and IO list of H. $\mathcal{L}$ consists of tuples (r_i, a_i, h_i) $(0 \leq i \leq q_{EO} + q_{IO})$. The concrete construction of $\mathcal{I}$ is as follows.

Input : (n, e, y^*) s.t. n is RSA modulus, e is the exponent where $\gcd(e, \phi(n)) = 1$ and $y^* \stackrel{R}{\leftarrow} \mathbb{Z}_n$

Output : x^* s.t. $x^* \equiv y^{*d} \pmod{n}$

Input public key : Send (n, e) to $\mathcal{A}$ in Exp4 as the input public key.

DO **simulation :** When $\mathcal{A}$ poses decryption query c_i to DO, then behave as follows:
Find (r_i, c_i, h_i) from $\mathcal{L}_H$ such that $c_i = r_i^e$. If there is a tuple (r_i, c_i, h_i) satisfying the condition, then return h_i as the answer. Otherwise, generate $h_i \in \{0,1\}^k$, add $(\emptyset, c_i, h_i)$ to $\mathcal{L}_H$ and return h_i as the answer.

RO **simulation :** When $\mathcal{A}$ poses query r_i to RO, then behave as follows:
<If $c_i = y^*$ s.t. $c_i = r_i^e \mod n$ >
Output r_i as x^* and halt.
<If $(r_i, *, h_i) \in \mathcal{L}_H$ >
Return h_i to $\mathcal{A}$ as the answer.
<If $(r_i, *, *) \notin \mathcal{L}_H$ and $(\emptyset, c_i, h_i) \in \mathcal{L}_H$ s.t. $c_i = r_i^e \mod n$ >
Replace $(\emptyset, c_i, h_i)$ to (r_i, c_i, h_i) in $\mathcal{L}_H$ and return h_i to $\mathcal{A}$ as the answer.
<If $(r_i, *, *) \notin \mathcal{L}_H$ and $(\emptyset, c, h) \notin \mathcal{L}_H$ s.t. $c = r_i^e \mod n$ >
Compute $c_i = r_i^e \mod n$, generate $h_i \in \{0,1\}^k$, add (r_i, c_i, h_i) to $\mathcal{L}_H$ and return h_i to $\mathcal{A}$ as the answer.

EO **simulation :** When $\mathcal{A}$ poses extension attack query (r_i, a_i) to EO, then behave as follows:
Find $(r_i, a_i, *)$ from $\mathcal{L}$. If $a_i = K_b^*$, then return randomly chosen value $h_i \in \{0,1\}^k$ and add (r_i, a_i, h_i). If there is tuple (r_i, a_i, h_i), then return $r_i \oplus h_i$. Else if $h_i = IV$, then obey the RO simulation by input r_i and return $r_i \oplus h_i$ where h_i is the output of the RO simulation. Else if there is only one tuple $(r', *, a_i)$ in $\mathcal{L}_H$, then obey the RO simulation by input $r'||r_i$ and return $r_i \oplus h_i$ where h_i is the output of the RO simulation. Otherwise, generate $h_i \in \{0,1\}^k$ add (r_i, a_i, h_i) to $\mathcal{L}$, and return $r_i \oplus h_i$.

IO **simulation :** When $\mathcal{A}$ poses an inverse attack query, (r_i, b_i), to IO, then behave as follows:
If there is tuple (r_i, a_i, b_i) in $\mathcal{L}$, then return a_i. Else if there is $(r_i, *, IV \oplus b_i)$ in $\mathcal{L}_H$, then return IV. Else if there are tuples $(r', *, h')$ and $(r'||r_i, *, h' \oplus b_i)$ in $\mathcal{L}_H$, then add (r_i, h', b_i) to $\mathcal{L}$, and return h'. Otherwise, generate $h_i \in \{0,1\}^k$ add (r_i, h_i, b_i) to $\mathcal{L}$, and return h_i.

Challenge ciphertext : When $\mathcal{A}$ outputs $(state)$, then compute (K^*, y') by the encryption procedure and return (K^*, y^*) as the challenge.

We determine the success probability of $\mathcal{I}$. In the RO simulation, if $c_i = y^*$ such that $c_i = r_i^e \bmod n$ holds, $\mathcal{I}$ can successfully break the RSA problem. This event is the same as E_4 in Exp4. In the EO simulation, if $\mathcal{A}$ poses query (r, K_b^*) for some r, $\mathcal{I}$ returns a randomly chosen value instead of returning $H(r^*||r)$. However, this simulation is indistinguishable from the real interface of EO as follows. Here, we consider distinguisher $\mathcal{D}$ which tries to distinguish the simulation from the real EO.

Lemma 6. *If the output of* RO H *is independently chosen from the input,* $\mathcal{D}$ *cannot distinguish the simulation from the real* EO*.*

Proof. We show that we can construct an algorithm $\mathcal{ALG}$ which can distinguish an output of RO H from a random value if there exists $\mathcal{D}$ which can distinguish the simulation from the real EO. The concrete construction of $\mathcal{ALG}$ is as follows.

Step 1 : Simulate Exp4 for $\mathcal{D}$, as the adversary, except when $\mathcal{D}$ poses query (r, K_b^*) for some r to EO.

Step 2 : On receiving query (r, K_b^*) for some r to EO, forward $r^*||r$ to RO H, receive h as the output where h is $H(r^*||r)$ or a random value $rand$, and return h to $\mathcal{D}$.

Step 3 : If $\mathcal{D}$ decides that he is interacting with the real EO, decide that h is $H(r^*||r)$. Otherwise, decide that h is $rand$.

The interface of $\mathcal{D}$ is identical with the real EO when h is $H(r^*||r)$. Also, the interface of $\mathcal{D}$ is identical with the simulation when h is $rand$. Therefore, if $\mathcal{D}$ succeeds, then $\mathcal{ALG}$ also succeeds. □

Thus, it is clear that $\mathcal{I}$ perfectly simulates Exp4 for $\mathcal{A}$. Therefore, we obtain

$$\epsilon' = \epsilon''.$$

$\mathcal{I}$ computes at most $q_{RO} + q_{EO}$ exponentiations modulo n. Thus, we obtain

$$t' = t'' + (q_{RO} + q_{EO}) \cdot expo.$$

□

Exp3 and Exp4 are identical until E_4 occurs. Thus, $|\mathsf{Succ4} - \mathsf{Succ3}| = \epsilon'$.

$\mathcal{A}$ can obtain no information about random bit b because key K_b^* is independent from information which $\mathcal{A}$ can obtain in Exp4. Therefore, $\mathsf{Succ4} = 1/2$. Since $\mathsf{Succ0} \leq |\mathsf{Succ1} - \mathsf{Succ0}| + |\mathsf{Succ2} - \mathsf{Succ1}| + |\mathsf{Succ3} - \mathsf{Succ2}| + |\mathsf{Succ4} - \mathsf{Succ3}| + \mathsf{Succ4}$, $\mathsf{Succ0} \leq \epsilon' + \frac{q_D}{n} + \frac{q_{IO}}{|\mathbb{Z}_n|} + 1/2$. Hence, $\epsilon' \geq \epsilon - \frac{q_D}{n} - \frac{q_{IO}}{|\mathbb{Z}_n|}$. □

E Figures

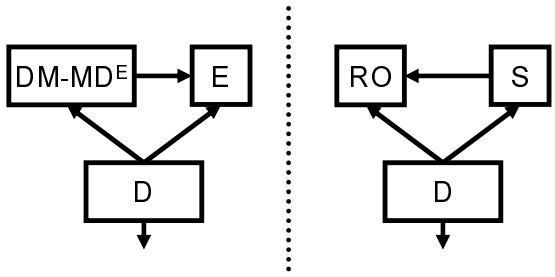

Fig. 1. Indifferentiability of DM-MD^E from RO

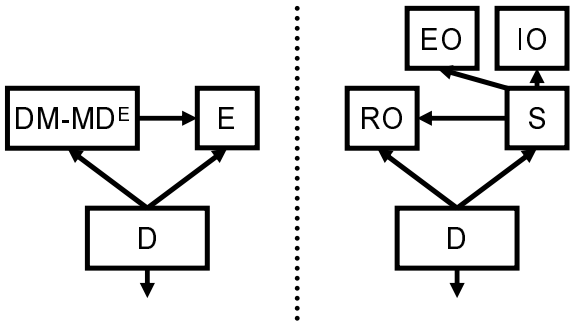

Fig. 2. Indifferentiability for Theorem 1

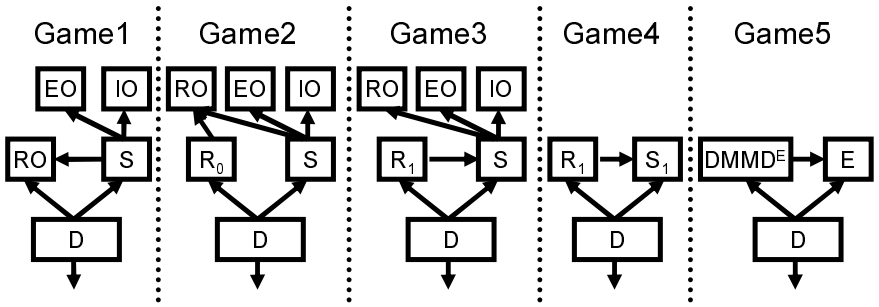

Fig. 3. Indifferentiable Games in Theorem 1

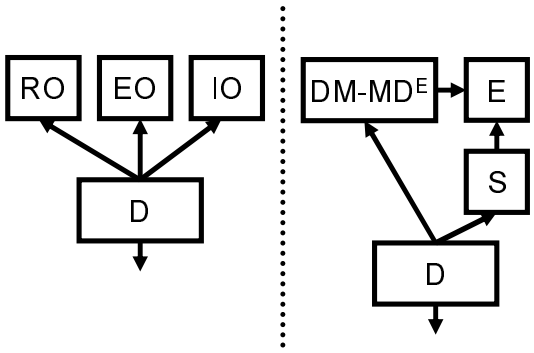

Fig. 4. Indifferentiability for Theorem 2

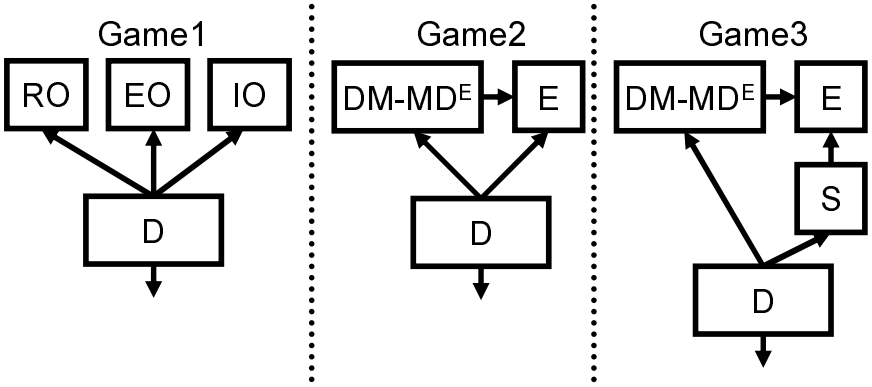

Fig. 5. Indifferentiable Games in Theorem 2

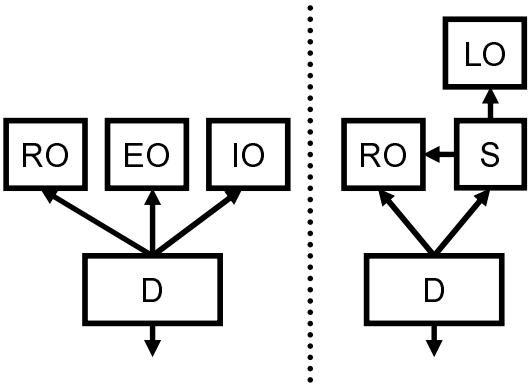

Fig. 6. Indifferentiability for Theorem 3

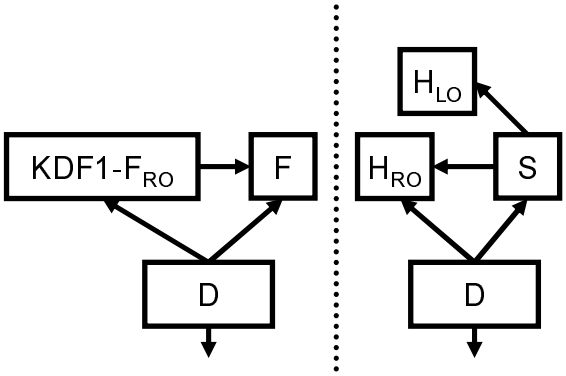

Fig. 7. Indifferentiability for Theorem 5

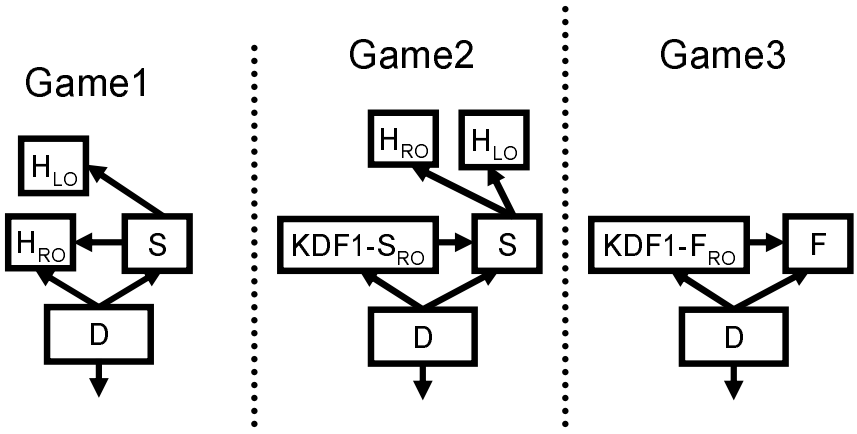

Fig. 8. Indifferentiable Games in Theorem 5

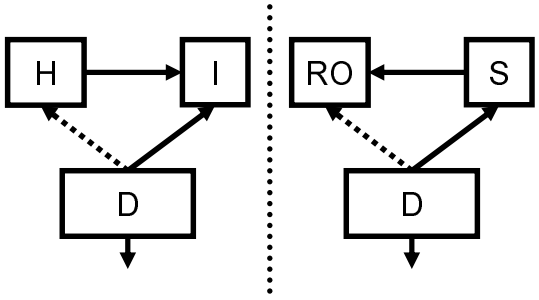

Fig. 9. Definition 3

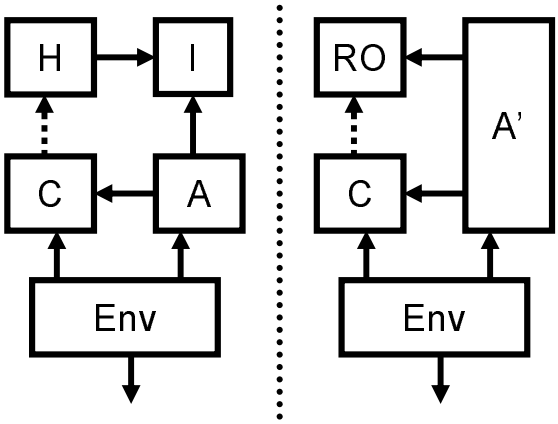

Fig. 10. Definition 4

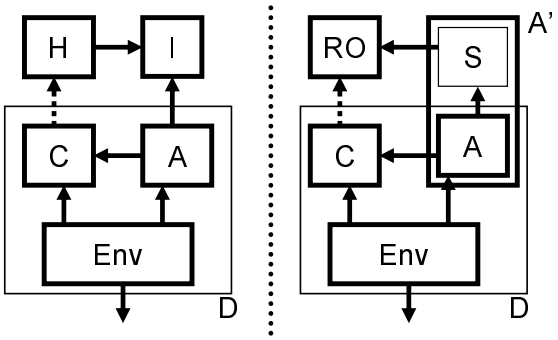

Fig. 11. Proof of "⇒" of Theorem 7