

# On the Indifferentiable Hash Functions in the Multi-Stage Security Games

Yusuke Naito

Mitsubishi Electric Corporation

**Abstract.** It had been widely believed that the indifferentiability framework ensures composition in any security game. However, Ristenpart, Shacham, and Shrimpton (EUROCRYPT 2011) demonstrated that for some multi-stage security, there exists a cryptosystem which is secure in the random oracle (RO) model but is broken when some indifferentiable hash function is used. However, this does not imply that for any multi-stage security, any cryptosystem is broken when a RO is replaced with the indifferentiable hash function. They showed that the important multi-stage security: the chosen-distribution attack (CDA) security is preserved for some public key encryption (PKE) schemes when a RO is replaced with the indifferentiable hash function proposed by Dodis, Ristenpart, and Shrimpton (EUROCRYPT 2009). An open problem from their result is the multi-stage security when a RO is replaced with other indifferentiable hash functions. We show the following for the important indifferentiable hash functions, Prefix-free Merkle-Damgård, Sponge, and chop Merkle-Damgård.

- For *any* PKE scheme, the PRIV security, which is a multi-stage security, is preserved when a RO is replaced with the indifferentiable hash functions.
- *All* existing hedged PKE scheme, which is CDA-secure in the RO model, are CDA-secure when using the indifferentiable hash function.

## 1 Introduction

The indifferentiable composition theorem of Maurer, Renner, and Holenstein [23] ensures that if a functionality  $F$  (e.g., a hash function from an ideal primitive) is indifferentiable from a second functionality  $F'$  (e.g., a random oracle (RO)), the security of any cryptosystem is preserved when  $F'$  is replaced with  $F$ . The important application of this framework is the RO model security, because many practical cryptosystems e.g., RSA-OAEP [8] and RSA-PSS [9] are designed by the RO methodology. A RO is instantiated by a hash function such as SHA-1 and SHA-256 [26]. However, the Merkle-Damgård hash functions [18, 24] such as SHA-1 and SHA-256, are not indifferentiable from ROs [17]. So many indifferentiable (from a RO) hash functions have been proposed, e.g., the finalists of the SHA-3 competition [3, 11, 20, 21, 28, 1, 2, 10, 12, 17, 16, 19]. The indifferentiable security is thus an important security of hash functions.

Recently, Ristenpart, Shacham, and Shrimpton [27] showed that in some multi-stage security game a RO secure scheme is broken when some indifferentiable hash function is used. They considered the multi-stage security game called CRP. The CRP security game for the  $n$ -bit (output length) hash function  $H$  is the two stage security game. In the first stage, for a random message  $M$  of  $4n$  bits, the first stage adversary  $A_1$  derives the some state  $st$  of  $2n$  bits. In the second stage, the second stage adversary  $A_2$  receives  $st$ , and for a random  $2n$ -bit challenge value  $C$  outputs an  $n$ -bit value  $z$ . Then, the adversary wins if  $z = H(M||C)$ . Consider the chop MD hash function  $\text{chopMD}^h(M) = \text{chop}_n(h(h(IV, M_1), M_2))$  which is indifferentiable from a RO [17], where  $h : \{0, 1\}^{4n} \rightarrow \{0, 1\}^{2n}$  is a RO,  $|M_1| = |M_2| = 2n$ ,  $M = M_1||M_2$ , and  $\text{chop}_n : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n$  outputs the right  $n$ -bits of the input. Clearly, the following adversary can win with probability 1 when  $H$  is the chop MD hash function. First,  $A_1$  receives  $M$ , calculates  $st = h(h(IV, M_1), M_2)$ , and outputs  $st$ . Second,  $A_2$  receives  $st$ , and for a random challenge  $C$ , outputs  $z = \text{chop}_n(h(st, C))$  which is equal to  $\text{chopMD}(M||C)$ . On the other hand, when  $H$  is a RO, since  $A_2$  cannot receive several value of  $M$ , the probability that the adversary wins is negligible. This result implies that the indifferentiable composition theorem does not ensure any multi-stage security when a RO is replaced with indifferentiable hash functions.

The chosen-distribution attack (CDA) security game is an important multi-stage security game, which is the security goal for deterministic [4, 6, 13], hedged [5], and efficiently searchable [4] public key encryption (PKE), wherein there are several PKE schemes which are proven in the RO model [4, 5]. For the CDA secure PKE schemes EwH [4] and REwH1 [5] (in the RO model), Ristenpart *et al.* salvaged the important

indifferentiable hash function, the NMAC-type hash function [19], which was proposed by Dodis, Ristenpart, and Shrimpton, and which is employed in the SHA-3 finalist Skein [20]. They showed that these PKE schemes are non-adaptive CDA secure in the chosen-plaintext attack (CPA) case when the NMAC-type hash function is used.

The open problem from the paper of Ristenpart *et al.* is thus the CDA security when a RO replaced with other indifferentiable hash functions. Especially, it is important to consider the security when a RO is replaced with the SHA-3 finalists and the SHA-2 hash functions, because one of the SHA-3 finalists will be published as a standard hash function (FIPS) [25] and the SHA-2 hash functions are published as standard hash functions [26]. So we consider the important hash functions, Prefix-free Merkle-Damgård (PFMD) [17], Sponge [10] and chop Merkle-Damgård (chop MD) [17]. The PFMD hash function is employed in the SHA-3 finalist BLAKE [3]. The Sponge hash function is employed in the SHA-3 finalist Keccak [11]. The chop Merkle-Damgård hash function is employed in SHA-224 and SHA384 [26]. We show the following.

- The PRIV security of any PKE scheme is preserved when a RO is replaced with these hash functions.
- All existing hedged PKE schemes [5], REwH, RtD, and PtD, which are CDA secure in the RO model, is CDA secure when using these hash functions.

The above result covers both the adaptive security and the non-adaptive security and both both chosen-ciphertext attack (CCA) and CPA cases. The PRIV security [4] is the special case of the CDA security which is the security goal for the deterministic [4, 6, 13] and efficiently searchable [4] PKE schemes. To our knowledge, our results cover all PKE schemes which are CDA secure in the RO model. The advantages of our result to the result of Ristenpart *et al.* are that (1) our result ensures the *stronger* security (adaptive and CCA), and (2) our result ensures the CDA security of *all* existing PKE schemes which are CDA secure in the RO model. Since several PKE schemes in [5, 4] support the CCA case or the adaptive case, the analysis for the stronger security cases is important.

**(Reset) Indifferentiability [27].** To prove the CDA security, we use the reset indifferentiability framework of Ristenpart *et al.* The reset indifferentiability ensures composition in any security game: if a hash function  $H^P$  which uses an ideal primitive  $P$  is reset indifferentiable from another ideal primitive  $P'$ , any security of any cryptosystem is preserved when  $P'$  is replaced with  $H^P$ .

Recall the original [23] and reset [27] indifferentiability (from a RO) framework. The original indifferentiable security game from a RO for  $H^P$  is that a distinguisher  $A$  converses either with  $(H^P, P)$  or  $(RO, S^{RO})$ .  $S$  is a simulator which simulates  $P$  with the relation among  $H^P$  and  $P$ . If the probability that the distinguisher  $A$  hits the conversing world is small, then  $H^P$  is indifferentiable from a RO. In the reset indifferentiable security game, the distinguisher can reset the initial state of the simulator at arbitrary times.

To prove the original indifferentiable security, the simulator needs to record the query-response history. For a repeated query  $P(x)$  where  $z$  was returned, the value  $z$  is returned. So, for a repeated query to the simulator where  $z$  was returned, the simulator should return  $z$ . When the internal state is reseted, the simulator forgets the value and cannot return. Thus one cannot use the reset indifferentiability from a RO to prove the CDA security when a RO is replaced with the indifferentiable hash functions.

**Our Approach.** We thus use the reset indifferentiability from a variant of a RO. We propose a variant which covers many indifferentiable hash functions. We call the variant “Versatile Oracle” ( $\mathcal{VO}$ ).  $\mathcal{VO}$  consists of a RO and auxiliary oracles. The auxiliary oracles are used to record the query-response history of a simulator.  $\mathcal{VO}$  thus enables to construct a simulator which does not update the internal state and which is unaffected by the reset function. We show that the PFMD hash function, the Sponge hash function, and the chop MD hash function are reset indifferentiable from  $\mathcal{VO}$ s. Recently, Andreeva *et al.* [1] and Chang *et al.* [16] consider the indifferentiable security of the BLAKE hash function with the more concrete structure than PFMD. In the appendix E, we prove that the BLAKE hash function with the concrete structure is reset indifferentiable from  $\mathcal{VO}$ . Then, we show the following.

- For any PKE scheme, the PRIV security is preserved when a RO is replaced with  $\mathcal{VO}$ .
- The CDA security of the existing hedged PKE schemes is preserved when a RO is replaced with  $\mathcal{VO}$ .

The reset indifferentiability composition theorem ensures that the PRIV security and the CDA security are preserved when a RO is replaced with the indifferentiable hash functions. Note that this is the first time positive result for the reset indifferentiability (from  $\mathcal{VO}$ ).

$\mathcal{RO}_n(M)$ 1 if $F[M] = \perp$ , $F[M] \xleftarrow{\$} \{0, 1\}^n$ ; 2 <b>return</b> $F[M]$ ; 	$\mathcal{RO}_{w_i}^{(i)}(M)$ 1 if $F_i^*[M] \neq \perp$ then $F_i^*[M] \xleftarrow{\$} \{0, 1\}^{w_i}$ ; 2 <b>return</b> $F_i^*[M]$ ; 	$E_t(k, x)$ 1 if $E_t[k, x] = \perp$ , $y \xleftarrow{\$} \{0, 1\}^{m_t} \setminus T_t^+[k]$ ; 2 $Update_t(k, x, y)$ ; 3 <b>return</b> $E_t[k, x]$ ; 
$\mathcal{RO}_{n_j}^j(M)$ 1 If $F_j[M] \neq \perp$ , $F_j[M] \xleftarrow{\$} \{0, 1\}^{n_j}$ ; 2 <b>return</b> $F_j[M]$ ; 	$\mathcal{TO}^{(i)}(y)$ 1 if $\exists M$ s.t. $F_i^*[M] = y$ then <b>return</b> $M$ ; 3 <b>return</b> $\perp$ ; 	$D_t(y)$ 1 if $D_t[k, y] = \perp$ , $x \xleftarrow{\$} \{0, 1\}^{m_t} \setminus T_t^-[k]$ ; 2 $Update_t(k, x, y)$ ; 3 <b>return</b> $D_t[k, y]$ ; 

Fig. 1. Versatile Oracle  $\mathcal{VO}$

## 2 Preliminaries

**Notation.** For two values  $x, y$ ,  $x||y$  is the concatenated value of  $x$  and  $y$ . For some value  $y$ ,  $x \leftarrow y$  means assigning  $y$  to  $x$ . When  $X$  is a non-empty finite set, we write  $x \xleftarrow{\$} X$  to mean that a value is sampled uniformly at random from  $X$  and assign to  $x$ .  $\oplus$  is bitwise exclusive or.  $|x|$  is the bit length of  $x$ . For  $l \times r$ -bit value  $M$ ,  $div(r, M)$  divides  $M$  into  $r$ -bit values  $(M_1, \dots, M_l)$  and outputs them where  $M_1 || \dots || M_l = M$ . For a formula  $F$ , if there exists just a value  $M$  such that  $F(M)$  is true, we denote  $\exists_1 M$  s.t.  $F(M)$ .

**(Reset) Indifferentiability [23, 27].** In the reset indifferentiability [27], for a functionality  $F$ , a private interface  $F.priv$  and a public interface  $F.pub$  are considered, where adversaries have oracle access to  $F.pub$  and other parties (honest parties) have oracle access to  $F.priv$ . For example, for a cryptosystem in the  $F$  model, an output of the cryptosystem is calculated by accessing  $F.priv$  and an adversary has oracle access to  $F.pub$ . In the RO model the RO has both interfaces. Let  $H^P$  be a hash function that utilizes an ideal primitive  $P$ . The interfaces of  $H^P$  are defined by  $H^P.priv = H^P$  and  $H^P.pub = P$ .

For two functionalities  $F_1$  (e.g., hash function) and  $F_2$  (e.g. a variant of a RO), the definition of the reset indifferentiability for  $F_1$  from  $F_2$  is as follows.

$$\text{Adv}_{F_1, F_2, S}^{\text{r-indiff}}(A) = |\Pr[A^{\bar{F}_1.priv, \bar{F}_1.pub} \Rightarrow 1] - \Pr[A^{F_2.priv, \hat{S}^{F_2.pub}} \Rightarrow 1]|$$

where  $\hat{S} = (S, S.Rst)$ ,  $\bar{F}_1.priv = F_1.priv$  and  $\bar{F}_1.pub = (F_1.pub, nop)$ .  $S.Rst$  takes no input and when run reinitializes all of  $S$ .  $nop$  takes no input and does nothing. We say  $F_1$  is reset indifferentiable from  $F_2$  if there exists a simulator  $S$  such that for any distinguisher  $A$  the advantage of the reset indifferentiability is negligible. This framework ensures that if  $F_1$  is reset indifferentiable from  $F_2$  then the any stage security of any cryptosystem is preserved when  $F_2$  is replaced with  $F_1$ . Please see Theorem 6.1 in the full version of [27].

When  $S.Rst$  and  $nop$  are removed from the reset indifferentiable security game, it is equal to the original indifferentiable security game [23]. In the original indifferentiable security game, the distinguisher interacts with  $(F_1.priv, F_1.pub)$  and  $(F_2.priv, S^{F_2.pub})$ . We denote the advantage of the indifferentiable security by  $\text{Adv}_{F_1, F_2, S}^{\text{indiff}}(A)$  for a distinguisher  $A$ . We say  $F_1$  is indifferentiable from  $F_2$  if there exists a simulator  $S$  such that for any distinguisher  $A$  the advantage is negligible.

## 3 Versatile Oracle

In this section, we propose a versatile oracle  $\mathcal{VO}$ .  $\mathcal{VO}$  consists of a RO  $\mathcal{RO}_n$ , ROs  $\mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ), traceable random oracles  $\mathcal{TRO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ), and ideal ciphers  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ ). The private interface is defined by  $\mathcal{VO}.priv = \mathcal{RO}_n$  and the public interface is defined by  $\mathcal{VO}.pub = (\mathcal{RO}_n, \mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ),  $\mathcal{TRO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ),  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ )).  $\mathcal{VO}$  can be implemented as Fig. 1.

$\mathcal{RO}_n$  is shown in Fig. 1 (Left) where the input length is arbitrary and the output length is  $n$  bits.  $F$  is a (initially everywhere  $\perp$ ) table.

$\text{PFMD}^h(M)$ $1 \ (M_1, \dots, M_i) \leftarrow \text{div}(m, \text{pfpad}(M))$ $2 \ x \leftarrow IV;$ $3 \ \text{For } j = 1, \dots, i, \ x \leftarrow h(x  M_j);$ $4 \ \text{Ret } x;$	$S(x, y)$ $1 \ M^* \leftarrow \mathcal{TO}^{(1)}(x);$ $2 \ \text{if } x = IV \ \text{then}$ $3 \quad \text{if } \exists M \ \text{s.t. } \text{pfpad}(M) = y \ \text{then } z \leftarrow \mathcal{RO}_n(M);$ $4 \quad \text{else } z \leftarrow \mathcal{RO}_n^{(1)}(y);$ $5 \ \text{else if } M^* \neq \perp \ \text{then}$ $6 \quad \text{if } \exists M \ \text{s.t. } \text{pfpad}(M) = M^*  y \ \text{then } z \leftarrow \mathcal{RO}_n(M);$ $7 \quad \text{else } z \leftarrow \mathcal{RO}_n^{(1)}(M^*  y);$ $8 \ \text{else } z \leftarrow \mathcal{RO}_n^1(x  y);$ $9 \ \text{return } z;$
---	--

**Fig. 2.** PFMD Hash Function (left) and Simulator  $S$  (right)

$\mathcal{RO}_{n_j}^j$  is shown in Fig. 1 (Left) where the input length is arbitrary and the output length is  $n_j$  bits, and  $F_j$  is a (initially everywhere  $\perp$ ) table. Note that  $n_j$  and  $v$  are defined in our proofs.

$\mathcal{TRCO}_{w_i}^{(i)}$  is shown in Fig. 1 (Center) which consists of a RO  $\mathcal{RO}_{w_i}^{(i)}$  and a trace oracle  $\mathcal{TO}^{(i)}$ . The output length of  $\mathcal{RO}_{w_i}^{(i)}$  and the input length of  $\mathcal{TO}^{(i)}$  are  $w_i$  bits, and  $F_i^*$  is a (initially everywhere  $\perp$ ) table. Note that  $w_i$  and  $u$  are defined in our proofs.

$\text{IC}_{k_t, m_t}^{(t)}$  can be implemented as Fig. 1 (Right) which consists of an encryption oracle  $E_t$  and a decryption oracle  $D_t$  where the first input of  $E_t$  is the key of  $k_t$  bits and the second input is the plain text of  $m_t$  bits, and the first input of  $D_t$  is the key of  $k_t$  bits and the second input is the cipher text of  $m_t$  bits.  $E_t$  and  $D_t$  are (initially everywhere  $\perp$ ) tables where for the query  $E_t(k, x)$  (resp.  $D_t(k, y)$ ) the output is recorded in  $E_t[k, x]$  (resp.  $D_t[k, y]$ ).  $T_t^+[k]$  and  $T_t^-[k]$  are (initially empty) tables which stores all values of  $E_t[k, \cdot]$  and  $D_t[k, \cdot]$ , respectively.  $\text{Update}_t(k, x, y)$  is the procedure wherein the tables  $E_t, D_t, T_t^+[k]$  and  $T_t^-[k]$  are updated,  $E_t[k, x] \leftarrow y, D_t[k, y] \leftarrow x, T_t^+[k] \leftarrow y$  and  $T_t^-[k] \leftarrow x$ . Note that the length  $k_t, m_t$  and  $s$  are defined in our proofs.

## 4 Reset Indifferentiability for Hash Functions

In this section, we consider the reset indifferentiability security of the important hash functions, prefix-free Merkle-Damgård (PFMD) [17], Sponge [10], and chop Merkle-Damgård (chop MD) [17]. We show that these hash functions are reset indifferentiable from  $\mathcal{VO}$ s.

### 4.1 Reset Indifferentiability for the PFMD Hash Function

The PFMD hash function is employed in the SHA-3 finalist BLAKE hash function [3]. In the document of [3], the indifferentiability security is proven when the compression function is a RO.

The PFMD hash function is illustrated in Fig. 2 (Left) where  $IV$  is the initial value of  $n$  bits,  $h : \{0, 1\}^d \rightarrow \{0, 1\}^n$  is a compression function,  $d = n + m$ , and  $\text{pfpad} : \{0, 1\}^* \rightarrow (\{0, 1\}^m)^*$  is an injective prefix-free padding where for any different values  $M, M'$ ,  $\text{pfpad}(M)$  is not a prefix of  $\text{pfpad}(M')$  and the inverse function of  $\text{pfpad}$  is efficiently computable.

We evaluate the reset indifferentiability security from  $\mathcal{VO}$  for the PFMD hash function where  $h$  is a RO. We define the parameter of  $\mathcal{VO}$  as  $v = 1, u = 1, n_1 = n$ , and  $w_1 = n$ . Note that in the reset indifferentiability proof ideal ciphers are not used. Thus in this case,  $\mathcal{VO}_{priv} = \mathcal{RO}_n$  and  $\mathcal{VO}_{pub} = (\mathcal{RO}_n, \mathcal{RO}_n^1, \mathcal{TRCO}_n^{(1)})$ . The following theorem shows that  $\text{PFMD}^h$  is reset indifferentiable from  $\mathcal{VO}$ .

**Theorem 1.** *There exists a simulator  $S$  such that for any distinguisher  $\mathcal{A}$ , the following holds,*

$$\text{Adv}_{\text{PFMD}^h, \mathcal{VO}, S}^{\text{r-indiff}}(\mathcal{A}) \leq \mathcal{O}\left(\frac{(lq_H + q_h)^2}{2^n}\right)$$

where  $\mathcal{A}$  can make queries to  $\text{PFMD}^h/\mathcal{RO}_n$  and  $h/S$  at most  $q_H, q_h$  times, respectively, and  $l$  is a maximum number of blocks of a query to  $\text{PFMD}^h/\mathcal{RO}_n$ .  $S$  makes at most  $2q_h$  queries and runs in time  $\mathcal{O}(q_h)$ .  $\blacklozenge$

Algorithm $Sponge^P(M)$	
1 $M' \leftarrow \text{pad}_S(M)$ ;	
2 $(M_1, \dots, M_i) \leftarrow \text{div}(n, M)$ ;	
3 $s = IV$ ;	
4 for $i = 1, \dots, i$ do $s = P(s \oplus (M_i    0^c))$ ;	
5 <b>return</b> the left most $n$ -bits of $s$ ;	
$S_-(z, w)$	
01 $M \leftarrow \mathcal{TO}^{(1)}(w)$ ;	
02 if $M \neq \perp$ and $ M  = n$ then	
03 $x \leftarrow IV_1 \oplus M$ ; $y \leftarrow IV_2$ ;	
04 if $M \neq \perp$ and $ M  > n$ then	
05 let $M = M^*    m$ ( $ m  = n$ );	
06 if $\text{unpad}_S(M^*) = M' \neq \perp$ then $x \leftarrow m \oplus \mathcal{RO}_n(M')$ ;	
07 else $x \leftarrow m \oplus \mathcal{RO}_n^1(M^*)$ ;	
08 $y \leftarrow \mathcal{RO}_c^{(1)}(M^*)$ ;	
09 else $x    y \leftarrow \mathcal{P}^{-1}(z    w)$ ;	
10 <b>return</b> $x    y$ ;	
$S_+(x, y)$	
01 $M^* \leftarrow \mathcal{TO}^{(1)}(y)$ ;	
02 if $y = IV_2$ then	
03 if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ;	
04 else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x)$ ;	
05 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1)$ ;	
06 else if $M^* \neq \perp$ then	
07 if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M')$ ;	
08 else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*)$ ;	
09 if $\text{unpad}_S(M^*    m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ;	
10 else $z \leftarrow \mathcal{RO}_n^1(M^*    m)$ ;	
11 else $z    w \leftarrow \mathcal{P}(x    y)$ ;	
12 <b>return</b> $z    w$ ;	

**Fig. 3.** Sponge Hash Function (left) and Simulator  $S$  ( $S_+$  in right and  $S_-$  in left)

**The Simulator  $S$ .** We define the simulator  $S$  in Fig. 2 which does not update the internal state to remove the attack using  $S.Rst$ . The  $S$ 's task is to simulate the compression function  $h$  such that  $\mathcal{RO}_n$  and  $S$  are consistent, that is, for a value  $M$   $\text{PFMD}^S(M) = \mathcal{RO}_n(M)$ . We explain that the simulator  $S$  succeeds in the simulation of  $h$  with the consistency. For the ordered queries  $S(IV, M_1), S(z_1, M_2)$  where  $z_1 = S(IV, M_1), z_2 = S(z_1, M_2)$ , the structure of  $S$  ensures that the responses  $z_1$  and  $z_2$  are the responses of  $\mathcal{RO}_n^{(1)}(M_1)$  and  $\mathcal{RO}_n^{(1)}(M_1 || M_2)$ , respectively, if there does not exist  $M$  such that  $\text{PFMD}(M) = M_1 || M_2$ . Thus, the Merkle-Damgård style path  $(M_1 || M_2, z_2)$  is recoded in the table  $F_1^*$  of  $\mathcal{RO}_n^{(1)}$ . Then for the query  $S(z_2, M_3)$ , the response is defined by the output of  $\mathcal{RO}_n(M)$  if there exists  $M$  such that  $\text{pfpad}(M) = M_1 || M_2 || M_3$ . Notice that  $M_1 || M_2$  can be obtained by the query  $\mathcal{TO}^{(1)}(z_2)$ . Thus the simulator  $S$  succeeds in the simulation of  $h$ . The formal proof is given in Appendix B.

*Remark 1.* The EMD hash function [7] and the MDP hash function [22] are designed from the same design spirit as the PFMD hash function, which are designed to resist the length extension attack. Thus, by the similar proof, one can prove that the EMD hash function and the MDP hash function are reset indifferentiable from  $\mathcal{VO}$ s.

## 4.2 Reset Indifferentiability for the Sponge Hash Function

The Sponge hash function is a permutation-based hash function which employed in the SHA-3 candidate Keccak [11].

Fig. 3 (left) illustrates the Sponge hash function where  $IV$  is the initial value of  $b$  bits,  $\text{pad}_S : \{0, 1\}^* \rightarrow (\{0, 1\}^n)^*$  is an injective padding function such that the final block message  $M_i \neq 0$ ,  $P : \{0, 1\}^b \rightarrow \{0, 1\}^b$  is a permutation and  $b = n + c$ . The inverse function of  $\text{pad}_S$  is denoted by  $\text{unpad}_S : (\{0, 1\}^n)^* \rightarrow \{0, 1\}^* \cup \{\perp\}$  efficiently computable.  $\text{unpad}_S(M^*)$  outputs  $M$  if there exists  $M$  such that  $\text{pad}_S(M) = M^*$ , and outputs  $\perp$  otherwise. Note that the Sponge hash function of Fig. 3 is the special case of the general Sponge hash function where the output length is variable. The output lengths of SHA-3 are 224, 256, 384 and 512 bits and in this case the Keccak hash function has the structure of Fig. 3<sup>1</sup>. We conjecture that the reset indifferentiable

<sup>1</sup> In the Keccak case,  $b = 1600$  and  $c = 576$ . So, the output length of Keccak is shorter than  $n$ . Notice that the security analysis of this case is the same as the case that the output length  $n$ -bit, because the advantage of adversaries in the shorter output length case is decreased from that of adversaries in the case that the output length is  $n$ -bit. In the shorter output length case (assume that the output length is  $n'$ -bit),  $\mathcal{VO.priv}$  is  $\text{chop}_{n-n'} \circ \mathcal{RO}_n$  and  $\mathcal{VO}$  is  $(\mathcal{RO}_n, \mathcal{RO}_c^1, \mathcal{TO}^1, \mathcal{RO}_r^2, \mathcal{P}, \mathcal{P}^{-1})$  where  $\text{chop}_{n-n'}$  is the chop function where the right most  $n - n'$ -bits of the input are chopped.

$\text{chopMD}^h(M)$ 1 $M' \leftarrow \text{pad}_c(M)$ ; 2 $(m_1, \dots, m_i) \leftarrow \text{div}(d, M')$ ; 3 $x \leftarrow IV$ ; 4 for $j = 1, \dots, i$ do $x \leftarrow h(x, m_j)$ ; 5 <b>return</b> the right $n$ -bits of $x$ ; 	$S(x, m)$ where $x = x_1    x_2$ ( $ x_1  = s,  x_2  = n$ ) 01 $M \leftarrow \mathcal{TC}^{(1)}(x_1)$ ; 02 if $x = IV$ then 03 $z \leftarrow \mathcal{RO}_n(m)$ ; 04 $w \leftarrow \mathcal{RO}_s^{(1)}(m)$ ; 05 else if $M \neq \perp$ then 06 $z \leftarrow \mathcal{RO}_n(M    m)$ ; 07 $w \leftarrow \mathcal{RO}_s^{(1)}(M    m)$ ; 08 else $w    z \leftarrow \mathcal{RO}_{n+s}^1(x, m)$ ; 09 <b>return</b> $w    z$ ; 
---	--

**Fig. 4.** chop MD (left) and  $S$  (right)

security of the general Sponge hash function can be proven by extending the following analysis of the Sponge hash function. We denote the left most  $n$ -bit value and the right most  $c$  bit value of  $IV$  by  $IV_1$  and  $IV_2$ , respectively. Namely,  $IV = IV_1 || IV_2$ .

We evaluate the reset indifferentiable security of the Sponge hash function in the random permutation model, where  $P$  is a forward oracle of the random permutation and  $P^{-1}$  is its inverse oracle<sup>2</sup>. We define the parameter of  $\mathcal{VO}$  as  $v = 1, u = 1, s = 1, n_1 = n, w_1 = c$ , and  $m_1 = b$ . We don't care the key length  $k_1$ , since in this proof we fix the key by some constant value, that is the fixed key ideal cipher is used. Since the fixed key ideal cipher is a random permutation of  $b$  bits, we use the random permutation  $(\mathcal{P}, \mathcal{P}^{-1})$  of  $b$  bits instead of the ideal cipher  $\text{IC}_{k_1, b}^{(1)}$  where  $\mathcal{P}$  is a forward oracle and  $\mathcal{P}^{-1}$  is an inverse oracle. Thus, in this case,  $\mathcal{VO}.\text{priv} = \mathcal{RO}_n$  and  $\mathcal{VO}.\text{pub} = (\mathcal{RO}_n, \mathcal{RO}_n^1, \mathcal{TRC}_c^{(1)}, \mathcal{P}, \mathcal{P}^{-1})$ . The following theorem is that the sponge hash function  $\text{Sponge}^P$  is reset indifferentiable from  $\mathcal{VO}$ .

**Theorem 2 (Sponge is reset indifferentiable from  $\mathcal{VO}$ ).** *There exists a simulator  $S = (S^+, S^-)$  such that for any distinguisher  $\mathcal{A}$ , the following holds.*

$$\text{Adv}_{\text{Sponge}^P, \mathcal{VO}, S}^{\text{r-indiff}}(\mathcal{A}) \leq \frac{(1 - 2^{-n})q^2 + (1 + 2^{-n})q}{2^{c+1}} + \frac{3q^2}{2^{b+1}} + \frac{q(3q + 1)}{2^{c-1}}$$

where  $\mathcal{A}$  can make at most  $q$  queries.  $S$  makes at most  $3q$  queries and runs in time  $\mathcal{O}(q)$ .  $\blacklozenge$

**The Simulator  $S$ .** We define the simulator  $S$  in Fig. 3 which does not update the internal state to remove the attack using  $S.\text{Rst}$ . The  $S$ 's task is to simulate the random permutation  $(P, P^{-1})$  such that  $\mathcal{RO}_n$  and  $S$  are consistent, that is, for a value  $M$ ,  $\text{Sponge}^{S^+}(M) = \mathcal{RO}_n(M)$ .  $S_+$  and  $S_-$  simulate  $P$  and  $P^{-1}$ , respectively. For the ordered queries  $S_+(x_1, IV_2), S_+(x_2, w_1)$  where  $z_1 || w_1 = S_+(x_1, IV_2), z_2 || w_2 = S_+(x_2, w_1)$ , the structure of  $S$  ensures that  $w_1 = \mathcal{RO}_c^{(1)}(M_1)$  and  $w_1 = \mathcal{RO}_c^{(1)}(M_1 || M_2)$  where  $M_1 = IV_1 \oplus x_1$  and  $M_2 = z_1 \oplus x_2$ . Thus, the path  $(M_1 || M_2, w_2)$  is recoded in the table  $F_1^*$  where  $F_1^*[M_1 || M_2] = w_2$ . Then, for the query  $S_+(x_3, w_2)$ , the response  $w_3 || z_3$  is defined as  $w_3 = \mathcal{RO}_n(M)$  and  $z_3 = \mathcal{RO}_c^{(1)}(M_1 || M_2 || M_3)$ , if  $\text{unpad}(M_1 || M_2 || M_3) = M \neq \perp$  where  $M_3 = z_2 \oplus x_3$ . Notice that  $M_1 || M_2$  can be obtained by the queries  $\mathcal{TC}^{(1)}(w_2)$  and  $z_2$  can be obtained by the query  $\mathcal{RO}_n(\text{unpad}_S(M_1 || M_2))$  or the query  $\mathcal{RO}_n^1(M_1 || M_2)$ . Thus the simulator  $S$  succeeds in the simulation of the random permutation. The formal proof is given in Appendix C.

### 4.3 Reset Indifferentiability for the Chop MD Hash Function

The chop MD hash function is employed in SHA-2 family, SHA-224 and SHA-384 [26].

Fig. 4 illustrates the chop MD hash function  $\text{chopMD}^h : \{0, 1\}^* \rightarrow \{0, 1\}^n$ .  $h : \{0, 1\}^{d+n} \rightarrow \{0, 1\}^n$  is a compression function.  $\text{pad}_c$  is an injective padding function such that the inverse function is efficiently computable.

We evaluate the reset indifferentiable security of the chop MD hash function where  $h$  is a RO. We define the parameter  $\mathcal{VO}$  as  $v = 1, u = 1, n_1 = s + n$  and  $w_1 = s$ . Note that the ideal ciphers are not used.

<sup>2</sup> The security of the Sponge hash function was evaluated in the random permutation model [10].

$\text{CDA}_{\mathcal{AE}, F}^{A_1, A_2}$	$\text{CDA}_j^{\mathcal{AE}, A_2} (j = 1, 2)$
$b \xleftarrow{\$} \{0, 1\}$	$b \xleftarrow{\$} \{0, 1\}$
$(pk, sk) \xleftarrow{\$} \mathcal{K}$	$(pk, sk) \xleftarrow{\$} \mathcal{K}$
$(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}) \leftarrow \mathcal{A}_1^{F.pub}$	$((\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}), i) \leftarrow \mathcal{A}_1^{F.pub}$
$\mathbf{c} \leftarrow \mathcal{E}^{F.priv}(pk, \mathbf{m}_b, \mathbf{r})$	$\mathbf{c} \leftarrow \mathcal{E}^{F.priv}(pk, \mathbf{m}_b, \mathbf{r})$
$b' \leftarrow \mathcal{A}_2^{F.pub}(pk, \mathbf{c})$	$b' \leftarrow \mathcal{A}_2^{F.pub}(pk, \mathbf{c})$
<b>return</b> $(b = b')$	<b>return</b> $(bit_i(\mathbf{m}_b, \mathbf{r}) = b')$

**Fig. 5.** CDA Security Game (left) and CDA $j$  Security Game ( $j = 1, 2$ ) (right)

Thus, in this case,  $\mathcal{VO} = (\mathcal{RO}_n, \mathcal{RO}_{s+n}^1, \mathcal{TRO}_s^{(1)})$ . The following theorem shows that  $\text{chopMD}^h$  is reset indistinguishable from  $\mathcal{VO}$ .

**Theorem 3.** *There exists a simulator  $S$  such that for any distinguisher  $\mathcal{A}$ , the following holds,*

$$\text{Adv}_{\text{chopMD}^h, \mathcal{VO}, S}^{r\text{-indiff}}(\mathcal{A}) \leq \frac{(3n+1)q_h + nq_H}{2^s} + \frac{(q_H + q_h)}{2^{n-1}} + \frac{(lq_H + q_h)^2}{2^{s+n+1}} + \frac{q_h^2}{2^{s-1}} + \frac{(q_h + 1)^2}{2^n}$$

where  $\mathcal{A}$  can make queries to  $\text{chopMD}^h/\mathcal{RO}_n$  and  $h/S$  at most  $q_H, q_h$  times, respectively, and  $l$  is a maximum number of blocks of a query to  $\text{chopMD}^h/\mathcal{RO}_n$ .  $S$  makes at most  $3q_h$  queries and runs in time  $\mathcal{O}(q_h)$ .  $\blacklozenge$

**The Simulator  $S$ .** We define the simulator  $S$  in Fig. 4 which does not update the internal state to remove the attack using  $S.Rst$ . In the proof of Theorem 3, the padding function  $\text{pad}_c$  is removed. Thus the queries to  $\text{chopMD}^h$  and  $\mathcal{RO}_n$  are in  $(\{0, 1\}^d)^*$ . Note that the chop Merkle-Damgård hash function with the padding function is the special case of that without the padding function. The  $S$ 's task is to simulate the compression function  $h$  such that  $\mathcal{RO}_n$  and  $S$  are consistent, that is, for a value  $M$ ,  $\text{chopMD}^S(M) = \mathcal{RO}_n(M)$ . For the ordered queries  $S(IV, M_1), S(w_1||z_1, M_2)$  where  $w_1||z_1 = S(IV, M_1), w_2||z_2 = S(w_1||z_1, M_2)$ , the structure of  $S$  ensures that  $z_1 = \mathcal{RO}_n(M_1), w_1 = \mathcal{RO}_c^{(1)}(M_1), z_2 = \mathcal{RO}_n(M_1||M_2)$ , and  $w_2 = \mathcal{RO}_c^{(1)}(M_1||M_2)$ . Thus, the path  $(M_1||M_2, w_2)$  is recoded in the table  $F_1^*$  where  $F_1^*[M_1||M_2] = w_2$ . Then, for the query  $S(w_2||z_2, M_3)$ , the response  $w_3||z_3$  is defined as  $w_3 = \mathcal{RO}_n(M_1||M_2||M_3)$  and  $z_3 = \mathcal{RO}_c^{(1)}(M_1||M_2||M_3)$ . Notice that  $M_1||M_2$  can be obtained by the queries  $\mathcal{TO}^{(1)}(w_2)$ . Thus the simulator  $S$  succeeds in the simulation of  $h$ . The formal proof is given in Appendix D.

## 5 Multi-Stage Security in the $\mathcal{VO}$ Model

We show the following which ensures both adaptive and non-adaptive cases and both CCA and CPA cases.

- For any PKE scheme, the PRIV security [4] is preserved when a RO is replaced with  $\mathcal{VO}$ .
- For all hedged PKE schemes [5], REwH, RtD, and PtD, the CDA security is preserved when a RO is replaced with  $\mathcal{VO}$ .

In this section, we use the following notations. Vectors are written in boldface, e.g.,  $\mathbf{x}$ . If  $\mathbf{x}$  is a vector then  $|\mathbf{x}|$  denotes its length and  $\mathbf{x}[i]$  denotes its  $i$ -th component for  $1 \leq i \leq |\mathbf{x}|$ .  $bit_j(\mathbf{x})$  is the left  $j$ -th bit of  $\mathbf{x}[1]||\dots||\mathbf{x}[|\mathbf{x}|]$ .

**Public Key Encryption (PKE).** Recall that a public key encryption scheme  $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  consists of three algorithms. Key generation  $\mathcal{K}$  outputs a public key, secret key pair. Encryption  $\mathcal{E}$  takes a public key  $pk$ , a message  $m$ , and randomness  $r$  and outputs a cipher text. Decryption  $\mathcal{D}$  takes a secret key, a cipher text, and outputs a plaintext or a distinguished symbol  $\perp$ . For vectors  $\mathbf{m}, \mathbf{r}$  with  $|\mathbf{m}| = |\mathbf{r}| = l$  we denote by  $\mathcal{E}(pk, \mathbf{m}; \mathbf{r})$  the vector  $(\mathcal{E}(pk, \mathbf{m}[1]; \mathbf{r}[1]), \dots, \mathcal{E}(pk, \mathbf{m}[l]; \mathbf{r}[l]))$ . We say that  $\mathcal{AE}$  is deterministic if  $\mathcal{E}$  is deterministic. (That is,  $|\mathbf{r}| = 0$ )

**CDA Security.** We explain the CDA security (we quote the explanation of the CDA security in [27]). Fig. 5 illustrates the non-adaptive CDA game in the CPA case for a PKE scheme  $\mathcal{AE}$  using a functionality  $F$ . We explain the adaptive case and the CCA case, later. This notion captures the security of a PKE scheme when the randomness  $r$  used may not be a string of uniform bits. For the remainder of this section, fix a

randomness length  $\rho \geq 0$  and a message length  $\omega > 0$ . An  $(\mu, \nu)$ -mmr-source  $\mathcal{M}$  is a randomized algorithm that outputs a triple of vector  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$  such that  $|\mathbf{m}_0| = |\mathbf{m}_1| = |\mathbf{r}| = \nu$  which is the size of vectors, all components of  $\mathbf{m}_0$  and  $\mathbf{m}_1$  are bit strings of length  $\omega$ , all components of  $\mathbf{r}$  are bit strings of length  $\rho$ , and  $(\mathbf{m}_b[i], \mathbf{r}[i]) \neq (\mathbf{m}_b[j], \mathbf{r}[j])$  for all  $1 \leq i < j \leq \nu$  and all  $b \in \{0, 1\}$ . Moreover, the source has mini-entropy  $\mu$ , meaning  $\Pr[(\mathbf{m}_b[i], \mathbf{r}[i]) = (m', r') | (\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}) \xleftarrow{\$} \mathcal{M}] \leq 2^{-\mu}$  for all  $b \in \{0, 1\}$ , all  $1 \leq i \leq \nu$ , and all  $(m', r')$ . A CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  is a pair of procedures, the first of which is a  $(\mu, \nu)$ -mmr-source. The CDA advantage for a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  against scheme  $\mathcal{AE}$  using a functionality  $F$  is defined by

$$\text{Adv}_{\mathcal{AE}, F}^{\text{cda}}(\mathcal{A}_1, \mathcal{A}_2) = 2 \cdot \Pr[\text{CDA}_{\mathcal{AE}, F}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] - 1.$$

In the adaptive case, the adversary  $\mathcal{A}_1$  can select multiple triples  $(\mathbf{m}_{0,0}, \mathbf{m}_{0,1}, \mathbf{r}_0), \dots, (\mathbf{m}_{j,0}, \mathbf{m}_{j,1}, \mathbf{r}_j)$  adaptively, where before selecting  $(\mathbf{m}_{i,0}, \mathbf{m}_{i,1}, \mathbf{r}_i)$ ,  $\mathcal{A}_1$  can know cipher texts  $\mathbf{c}_0, \dots, \mathbf{c}_{i-1}$  of  $(\mathbf{m}_{0,b}, \mathbf{r}_0), \dots, (\mathbf{m}_{i-1,b}, \mathbf{r}_{i-1})$  where  $b \in \{0, 1\}$ . The adversary  $\mathcal{A}_2$  can receive its cipher texts  $\mathbf{c}_0, \dots, \mathbf{c}_j$ . In the CCA case, the adversary  $\mathcal{A}_2$  has oracle access to the decryption oracle where the queries don't appear as a component of the cipher text(s).

**PRIV Security.** The PRIV security is the special case of the CDA security when the PKE scheme  $\mathcal{AE}$  being considered has randomness length  $\rho = 0$ . Thus the PRIV security game for a PKE scheme  $\mathcal{AE}$  using a functionality  $F$  against adversary  $\mathcal{A}_1, \mathcal{A}_2$  is equal to the CDA game when  $\rho = 0$ . The PRIV advantage for a PRIV adversary  $\mathcal{A}_1, \mathcal{A}_2$  is denoted by  $\text{Adv}_{\mathcal{AE}, F}^{\text{priv}}(\mathcal{A}_1, \mathcal{A}_2)$  which is equal to the CDA advantage with  $\rho = 0$ .

**CDA1 Security.** In the following proofs, we use a new security called CDA1. The CDA1 security game is shown in Fig. 5 where  $\mathcal{A}_1$  is a  $(\mu, \nu)$ -mmr-source and outputs  $i$  in addition to  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$  and  $\mathcal{A}_2$  outputs a bit  $b'$ . Fig. 5 is a non-adaptive and CPA case. In the adaptive case,  $\mathcal{A}_1$  outputs  $(\mathbf{m}_{0,0}, \mathbf{m}_{0,1}, \mathbf{r}_0), \dots, (\mathbf{m}_{j-1,0}, \mathbf{m}_{j-1,1}, \mathbf{r}_{j-1})$  and  $\mathcal{A}_2$  obtains its cipher texts  $\mathbf{c}_0, \dots, \mathbf{c}_{j-1}$ . In the adaptive case, the CDA1 game returns  $(\text{bit}_i(\mathbf{m}_{0,b}, \dots, \mathbf{m}_{j-1,b}, \mathbf{r}_1, \dots, \mathbf{r}_{j-1}) b')$ . In the CCA case, the adversary  $\mathcal{A}_2$  has oracle access to the decryption oracle where the queries don't appear as a component of the cipher text(s). The CDA1 advantage for a CDA1 adversary  $\mathcal{A}_1, \mathcal{A}_2$  for a PKE scheme  $\mathcal{AE}$  using a functionality  $F$  is defined by

$$\text{Adv}_{\mathcal{AE}, F}^{\text{cda1}}(\mathcal{A}_1, \mathcal{A}_2) = 2 \cdot \Pr[\text{CDA1}_{\mathcal{AE}, F}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] - 1.$$

**CDA2 Security.** The CDA2 security game is the special case of the CDA1 security game. In the CDA2 security game,  $\mathcal{A}_1$  outputs  $((\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}), i)$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is a random bit, namely,  $\Pr[\text{bit}_i(\mathbf{m}_b, \mathbf{r}) = 1] = 1/2$ . The CDA2 advantage for a CDA2 adversary  $\mathcal{A}_1, \mathcal{A}_2$  for a PKE scheme  $\mathcal{AE}$  using a functionality  $F$  is defined by

$$\text{Adv}_{\mathcal{AE}, F}^{\text{cda2}}(\mathcal{A}_1, \mathcal{A}_2) = 2 \cdot \Pr[\text{CDA2}_{\mathcal{AE}, F}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] - 1.$$

Clearly the following lemma holds.

**Lemma 1.** *For any CDA2 adversary  $\mathcal{A}_1, \mathcal{A}_2$  of a PKE scheme  $\mathcal{AE}$  using a functionality  $F$ , there exists a CDA1 adversary  $\mathcal{B}_1, \mathcal{B}_2$  such that*

$$\text{Adv}_{\mathcal{AE}, F}^{\text{cda2}}(\mathcal{A}_1, \mathcal{A}_2) \leq \text{Adv}_{\mathcal{AE}, F}^{\text{cda1}}(\mathcal{B}_1, \mathcal{B}_2)$$

where the running time of  $\mathcal{B}_1, \mathcal{B}_2$  is at most that of  $\mathcal{A}_1, \mathcal{A}_2$ .  $\blacklozenge$

## 5.1 Tools of Our Security Proofs

**Removing Random Oracle.** Let  $\mathcal{RO}_n$  and  $\mathcal{RO}^*$  be ROs (in this case we don't care the lengths of domain and range spaces of  $\mathcal{RO}^*$ ). Let  $\mathcal{O}_1$  be some oracle where  $\mathcal{O}_1.\text{priv} = \mathcal{RO}_n$  and  $\mathcal{O}_1.\text{pub}$  includes  $\mathcal{RO}_n, \mathcal{RO}^*$  and other independent oracles. Let  $\mathcal{O}_2$  be an oracle which is equal to  $\mathcal{O}_1$  but excludes  $\mathcal{RO}^*$ . The following lemma ensures that the CDA security in the  $\mathcal{O}_2$  model ensures that in the  $\mathcal{O}_1$  model. Notice that the following lemma ensures both the CPA case and the CCA case and both the non-adaptive case and the adaptive case.



**Lemma 2.** For any CDA adversary  $A_1, A_2$ , making queries at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}^*}, q$  times to  $\mathcal{RO}_n, \mathcal{RO}^*$  and other oracles, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  such that

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_1}^{A_1, A_2} \Rightarrow \text{true}] \leq \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_2}^{A_1, A_2} \Rightarrow \text{true}].$$

where the running time of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  is at most that of the CDA adversary  $A_1, A_2$  and makes queries at most  $q_{\mathcal{RO}}, q$  times to  $\mathcal{RO}_n$ , and other oracles.  $\blacklozenge$

*Proof.* We consider the following three games.

- Game 0 is the CDA game in the  $\mathcal{O}_1$  model where the adversary is  $A_1, A_2$  which has oracle access to  $\mathcal{O}_1.\text{pub}$ .
- Game 1 is the CDA game in the  $\mathcal{O}_1$  model where the adversary is  $A_1, A_2$  but  $A_1, A_2$  does not have oracle access to  $\mathcal{RO}^*$ .
- Game 2 is the CDA game in the  $\mathcal{O}_2$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_2.\text{pub}$ .

Let  $G_j$  be an event that the CDA game in Game  $j$  output true. Thus

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_1}^{A_1, A_2} \Rightarrow \text{true}] - \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_2}^{A_1, A_2} \Rightarrow \text{true}] \leq \Pr[G0] - \Pr[G1] + \Pr[G1] - \Pr[G2].$$

**Game 0  $\Rightarrow$  Game 1.** We evaluate  $\Pr[G0] - \Pr[G1]$ . Since  $\mathcal{RO}^*$  does not leak one bit or more of  $(\mathbf{m}_0, \mathbf{m}_1)$ ,  $\mathcal{RO}^*$  gives no advantage to the CDA adversary. Thus  $\Pr[G0] \leq \Pr[G1]$ .

**Game 0  $\Rightarrow$  Game 1.** Clearly,  $\Pr[G1] = \Pr[G2]$ .  $\square$

**Removing Ideal Cipher.** Let  $\mathcal{RO}_n$  be a RO. Let  $\text{IC} = (E, D)$  be an ideal cipher where  $E$  is an encryption oracle and  $D$  is a decryption oracle (in this case we don't care the length of the plain text, the length of the cipher text and the length of the key). Let  $\mathcal{O}_3$  be some oracle where  $\mathcal{O}_3.\text{priv} = \mathcal{RO}_n$  and  $\mathcal{O}_3.\text{pub}$  includes  $\mathcal{RO}_n, \text{IC}$  and other oracles. Let  $\mathcal{O}_4$  be an oracle which is equal to  $\mathcal{O}_3$  but does not include  $\text{IC}$ . The following lemma ensures that the CDA security in the  $\mathcal{O}_4$  model ensures that in the  $\mathcal{O}_3$  model. Notice that the following lemma ensures both the CPA case and the CCA case and both the cases of the non-adaptive adversary and the adaptive adversary.

**Lemma 3.** For any CDA adversary  $A_1, A_2$  in the  $\mathcal{O}_3$  model, making queries at most  $q_{\mathcal{RO}}, q_{\text{IC}}, q$  times to  $\mathcal{RO}_n, \text{IC}$  and other oracles, respectively, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  such that

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_3}^{A_1, A_2} \Rightarrow \text{true}] \leq \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_4}^{A_1, A_2} \Rightarrow \text{true}].$$

$\mathcal{A}_1, \mathcal{A}_2$  can make queries at most  $q_{\mathcal{RO}}, q$  times to  $\mathcal{RO}_n$  and other oracles, respectively. The running time of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  is at most that of the CDA adversary  $A_1, A_2$ .  $\blacklozenge$

*Proof.* We consider the following three games.

- Game 0 is the CDA game in the  $\mathcal{O}_3$  model where the adversary is  $A_1, A_2$  which has oracle access to  $\mathcal{O}_3.\text{pub}$ .
- Game 1 is the CDA game in the  $\mathcal{O}_3$  model where the adversary is  $A_1, A_2$  which has oracle access to  $\mathcal{O}_3.\text{pub}$  excluding the ideal cipher  $(E, D)$ .
- Game 2 is the CDA game in the  $\mathcal{O}_4$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_4.\text{pub}$ .

Let  $G_j$  be an event that the CDA game in Game  $j$  output true. Thus

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_3}^{A_1, A_2} \Rightarrow \text{true}] - \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_4}^{A_1, A_2} \Rightarrow \text{true}] \leq \Pr[G0] - \Pr[G1] + \Pr[G1] - \Pr[G2].$$

**Game 0  $\Rightarrow$  Game 1.** Consider the difference between Game 0 and Game 1 ( $\Pr[G0] - \Pr[G1]$ ). If  $\mathcal{A}_1$  can success to give some cipher text of the ideal cipher to  $\mathcal{A}_2$  where the plain text includes one bit or more of  $(\mathbf{m}_0, \mathbf{m}_1)$ , the adversary might be obtained the advantage of the ideal cipher. However, since the length of the plain text is equal to that of the cipher text, the adversary  $\mathcal{A}_1$  can also give the plain text to  $\mathcal{A}_2$  without the ideal cipher. Thus, the ideal cipher gives no advantage to the adversary and  $\Pr[G0] \leq \Pr[G1]$ .

**Game 1  $\Rightarrow$  Game 2.** Since in Game 1 the adversary cannot make a query to the ideal cipher, Game 2 is equal to Game 1. So  $\Pr[G1] = \Pr[G2]$ .  $\square$

**Removing Traceable Random Oracles.** Let  $\mathcal{RO}_n$  be a RO. Let  $\mathcal{TRCO}_{w_i}^{(i)} = (\mathcal{RO}_{w_i}^{(i)}, \mathcal{TO}^{(i)})$  ( $i = 1, \dots, u$ ) be traceable random oracles. Let  $\mathcal{O}_5$  be some oracle where  $\mathcal{O}_5.\text{priv} = \mathcal{RO}_n$  and  $\mathcal{O}_5.\text{pub}$  includes  $\mathcal{RO}_n$ ,  $\mathcal{TRCO}_{w_i}^{(i)}$  and other independent oracles. Let  $\mathcal{O}_6$  be an oracle which is equal to  $\mathcal{O}_5$  but does not include  $\mathcal{TRCO}_{w_i}^{(i)}$ . The following lemma shows that the CDA security in the  $\mathcal{O}_6$  model and the CDA2 security in the  $\mathcal{O}_5$  model ensures CDA security in the  $\mathcal{O}_5$  model. Notice that the following lemma ensures both the CPA case and the CCA case and both the cases of the non-adaptive adversary and the adaptive adversary.

**Lemma 4.** *For any CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  in the  $\mathcal{O}_5$  model, making queries to  $\mathcal{RO}_n, \mathcal{RO}_{w_i}^{(i)}, \mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ) and other oracles at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}^*}, q_{\mathcal{TO}^*}, q$ , respectively, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  in the  $\mathcal{O}_6$  mode or a CDA1 adversary  $B_1, B_2$  in the  $\mathcal{O}_6$  model such that*

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_5}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] \leq \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_6}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] + \text{Adv}_{\mathcal{AE}, \mathcal{O}_5}^{\text{cda2}}(B_1, B_2) + \frac{q_{\mathcal{RO}^*} q_{\mathcal{TO}^*}}{2^{w-1}}.$$

where  $\mathcal{A}_1, \mathcal{A}_2$  can query to  $\mathcal{RO}_n$  and other oracles at most  $q_{\mathcal{RO}}, q$ , respectively.  $w = \min\{w_1, \dots, w_u\}$ . The running time of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  is at most that of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$ .  $\blacklozenge$

*Proof.* We consider the following four games.

- Game 0 is the CDA game in the  $\mathcal{O}_5$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_5.\text{pub}$ .
- Game 1 is the CDA game in the  $\mathcal{O}_5$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_5.\text{pub}$  excluding  $\mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ).
- Game 2 is the CDA game in the  $\mathcal{O}_5$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_5.\text{pub}$  excluding  $\mathcal{TRCO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ).
- Game 3 is the CDA game in the  $\mathcal{O}_6$  model where the adversary is  $\mathcal{A}_1, \mathcal{A}_2$  which has oracle access to  $\mathcal{O}_6.\text{pub}$ .

Let  $G_j$  be an event that the CDA game in Game  $j$  output true. Thus

$$\Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_1}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] - \Pr[\text{CDA}_{\mathcal{AE}, \mathcal{O}_2}^{\mathcal{A}_1, \mathcal{A}_2} \Rightarrow \text{true}] \leq \Pr[G_0] - \Pr[G_1] + \Pr[G_1] - \Pr[G_2] + \Pr[G_2] - \Pr[G_3].$$

**Game 0  $\Rightarrow$  Game 1.** We evaluate  $\Pr[G_0] - \Pr[G_1]$ . We consider the following events for Game 0.

- Event E1:  $\mathcal{A}_1$  makes a query  $\mathcal{RO}_{w_i}^{(i)}(M)$  such that  $M$  includes one bit or more of  $(\mathbf{m}_0, \mathbf{m}_1)$ .
  - Event E11 =  $E1 \wedge E1'$  where Event  $E1'$  is that  $\mathcal{A}_2$  makes the query  $\mathcal{TO}^{(i)}(z)$  where  $z = \mathcal{RO}_{w_i}^{(i)}(M)$ 
    - \* Event E111 =  $E11 \wedge E11'$  where Event  $E11'$  is that  $(\mathbf{m}_b, \mathbf{r})$  includes one bit or more of  $z$ .
      - Event E1111 =  $E111 \wedge E111'$  where Event  $E111'$  is that when  $\mathcal{A}_2$  makes the query  $\mathcal{TO}^{(i)}(z)$ ,  $\mathcal{A}_2$  knows one bit or more of  $z$  in  $(\mathbf{m}_b, \mathbf{r})$ .
      - Event E1112 =  $E111 \wedge \neg E112'$  where Event  $\neg E112'$  is that when  $\mathcal{A}_2$  makes the query  $\mathcal{TO}^{(i)}(z)$ ,  $\mathcal{A}_2$  know no bit of  $z$  in  $(\mathbf{m}_b, \mathbf{r})$ .
    - \* Event E112 =  $E11 \wedge \neg E11'$  where Event  $\neg E11'$  is that  $(\mathbf{m}_b, \mathbf{r})$  includes no bit of  $z$ .
  - Event E12 =  $E1 \wedge \neg E1'$  where Event  $\neg E1'$  is that  $\mathcal{A}_2$  does not make the query  $\mathcal{TO}^{(i)}(z)$ .
- Event E2 =  $\neg E1$  where Event  $\neg E1$  is that  $\mathcal{A}_1$  does not make the query  $\mathcal{RO}_{w_i}^{(i)}(M)$ .

Then

$$\begin{aligned} \Pr[G_0] - \Pr[G_1] &\leq \Pr[G_0|E1111] \Pr[E1111] + \Pr[G_0|E1112] \Pr[E1112] + \Pr[G_0|E112] \Pr[E112] \\ &\quad + \Pr[G_0|E12] \Pr[E12] + \Pr[G_0|E2] \Pr[E2] - \Pr[G_1] \\ &\leq \Pr[E1111] + \Pr[E1112] + \Pr[E112] + \Pr[G_0|E12] \Pr[E12] + \Pr[G_0|E2] \Pr[E2] - \Pr[G_1] \end{aligned}$$

$\Pr[E1111]$ : Under Event E1111,  $\mathcal{A}_2$  knows one bit or more of  $z$  in  $(\mathbf{m}_b, \mathbf{r})$  without using  $\mathcal{TO}^{(i)}$ . And  $\mathcal{RO}_{n_i}^{(i)}$  leaks no bit of  $(\mathbf{m}_b, \mathbf{r})$ . Thus  $\mathcal{A}_2$  knows the bit without using the traceable random oracles  $\mathcal{TRCO}_{w_i}^{(i)}$ . Since  $z$  is a random value, E1111 is equal to the event that in the  $\mathcal{O}_6$  model  $\mathcal{A}_1$  makes  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$  such that for some  $i$   $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is some bit of  $z$  and then  $\mathcal{A}_2$  hits the bit. This is equal to the CDA1 security game. Thus if E1111 occurs then the CDA2 advantage is 1. So there exists the CDA2 adversary  $B_1, B_2$  such that  $\Pr[E1111] \leq \text{Adv}_{\mathcal{AE}, \mathcal{O}_6}^{\text{cda2}}(B_1, B_2)$ .

Pr[E1112]: Under Event E1111, when  $A_2$  makes a query  $\mathcal{TO}^{(i)}(z)$ ,  $A_2$  knows no bit of  $(\mathbf{m}_b, \mathbf{r})$ , that is  $A_2$  knows no bit of  $z$ . Thus, Event E1111 is that  $A_2$  needs to hit the random value  $z$ . Since  $A_1$  can make such value  $z$  at most  $q_{\mathcal{RO}}$  values,  $\Pr[\text{E1112}] \leq q_{\mathcal{RO}^*} \times q_{\mathcal{TO}^*} / 2^w$ .

Pr[E112]: Since  $(\mathbf{m}_b, \mathbf{r})$  does not include  $z$ , to query  $\mathcal{TO}^{(i)}(z)$ ,  $A_2$  needs to hit the random value  $z$ . Since  $A_1$  can make such value  $z$  at most  $q_{\mathcal{RO}^*}$  values,  $\Pr[\text{E112}] \leq q_{\mathcal{RO}^*} \times q_{\mathcal{TO}^*} / 2^w$ .

Pr[G0|E12]: Since  $A_2$  makes no  $\mathcal{TO}^{(i)}$  query to obtain  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$ ,  $\mathcal{TO}^{(i)}$  gives no advantage to  $A_2$ . Thus  $\Pr[\text{G0|E12}] = \Pr[\text{G1}]$ .

Pr[G0|E2]: Since  $\mathcal{TRCO}_{w_i}^{(i)}$  gives no value of  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$  to  $A_2$  under Event E2,  $\Pr[\text{G0|E2}] = \Pr[\text{G1}]$ .

Since  $\Pr[\text{E12}] + \Pr[\text{E2}] \leq 1$ , there exists the CDA2 adversary  $B_1, B_2$  such that

$$\Pr[\text{G0}] - \Pr[\text{G1}] \leq \text{Adv}_{\mathcal{AE}, \mathcal{O}_6}^{\text{cda2}}(B_1, B_2) + q_{\mathcal{RO}^*} \times q_{\mathcal{TO}^*} / 2^{w-1}.$$

Note that the above discussion is in the case of the non-adaptive adversary, but clearly one can apply the discussion to the case of the adaptive adversary by changing the  $A_1$ 's output and the cipher text from  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$  and  $\mathbf{c}$  to  $(\mathbf{m}_{0,0}, \mathbf{m}_{0,1}, \mathbf{r}_0), \dots, (\mathbf{m}_{i-1,0}, \mathbf{m}_{i-1,1}, \mathbf{r}_{i-1})$  and  $(\mathbf{c}_0, \dots, \mathbf{c}_j)$

**Game 1  $\Rightarrow$  Game 2.** In Game 2  $\mathcal{RO}_{w_i}^{(i)}$  queries are removed. From Lemma 2,  $\Pr[\text{G1}] \leq \Pr[\text{G2}]$ .

**Game 2  $\Rightarrow$  Game 3.** Clearly Game 3 is equal to Game 2. Thus  $\Pr[\text{G2}] = \Pr[\text{G3}]$ .  $\square$

## 5.2 PRIV Security

Lemmas 2 and 3 ensure that for any PKE scheme the PRIV security is preserved when  $\mathcal{O}_7$  is replaced with  $\mathcal{VO}$ , where  $\mathcal{O}_{7.\text{priv}} = \mathcal{RO}_n$  and  $\mathcal{O}_{7.\text{pub}} = (\mathcal{RO}_n, \mathcal{TRCO}_{w_i}^{(i)})$  for  $i = 1, \dots, u$ . To use Lemma 4, we evaluate the CDA1 advantage in the  $\mathcal{RO}_n$  model. Note that CDA2 advantage is bounded by the CDA1 advantage from Lemma 1. Winning the CDA1 game implies that the second stage adversary in the PRIV game obtains one bit or more of  $\mathbf{m}_b$ . Thus, in this case, the CDA1 adversary can win the PRIV game by generating  $\mathbf{m}_b$  such that the obtained bit is  $b$ . Namely, the CDA1 advantage is bounded by the PRIV advantage in the RO model. The formal evaluation of the bound of the CDA1 advantage is given in Appendix F. We thus obtain the following theorem. Notice that the theorem ensures both the CPA case and the CCA case and both the non-adaptive cases and the adaptive case.

**Theorem 4.** *For any PRIV adversary  $A_1, A_2$  in the  $\mathcal{VO}$  model, making queries at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}'}, q_{\mathcal{IC}}, q_{\mathcal{RO}^*}$  and  $q_{\mathcal{TO}^*}$  times to  $\mathcal{RO}_n, \mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ),  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ ),  $\mathcal{RO}_{w_i}^{(i)}$  and  $\mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ), respectively, there exists a PRIV adversary  $A_1, A_2$  such that*

$$\text{Adv}_{\mathcal{AE}, \mathcal{O}^*}^{\text{priv}}(A_1, A_2) \leq 3 \cdot \text{Adv}_{\mathcal{AE}, \mathcal{RO}_n}^{\text{priv}}(A_1, A_2) + \frac{q_{\mathcal{RO}^*} q_{\mathcal{TO}^*}}{2^{w-2}}.$$

$w = \min\{w_1, \dots, w_u\}$ .  $A_1, A_2$  can make queries at most  $q_{\mathcal{RO}}$  times to  $\mathcal{RO}_n$ . The running time of the PRIV adversary  $A_1, A_2$  is at most that of the PRIV adversary  $A_1, A_2$ .  $\blacklozenge$

## 5.3 The CDA Security of Hedged PKE Schemes

In the CDA security game with randomness, one cannot use Lemma 4 for some PKE scheme, since there exists a PKE scheme which is CDA secure in the RO model but the CDA2 advantage is not negligible. For example, such PKE scheme is that the encryption is defined as  $\mathcal{E}(pk, \mathbf{m}; \mathbf{r}) || \text{bit}_1(\mathbf{r})$ . We thus prove all hedged PKE schemes, REwH, RtD and PtD [5]. The theorem ensures both the non-adaptive cases and the adaptive case. Note that the CCA case of REwH, RtD and PtD have not been proved.

Lemmas 2 and 3 ensure that the CDA security of these PKE schemes is preserved when  $\mathcal{O}_7$  is replaced with  $\mathcal{VO}$  where  $\mathcal{O}_{7.\text{priv}} = \mathcal{RO}_n$  and  $\mathcal{O}_{7.\text{pub}} = (\mathcal{RO}_n, \mathcal{TRCO}_{w_i}^{(i)})$  for  $i = 1, \dots, u$ . We thus consider the CDA2

security of these PKE schemes in the  $\mathcal{RO}_n$ . Then Lemma 4 ensures that the CDA security of these PKE schemes is preserved when  $\mathcal{RO}$  is replaced with  $\mathcal{O}_7$ .

Let  $\mathcal{AE}_r = (\mathcal{K}_r, \mathcal{E}_r, \mathcal{D}_r)$  be a (randomized) PKE scheme with randomness length  $\rho_r > 0$ . Let  $\mathcal{AE}_d = (\mathcal{K}_d, \mathcal{E}_d, \mathcal{D}_d)$  be a (deterministic) PKE scheme with randomness length always 0.

**The CDA Security of REwH.** Let  $\text{REwH}[\mathcal{AE}_r] = (\mathcal{K}_{\text{REwH}}, \mathcal{E}_{\text{REwH}}, \mathcal{D}_{\text{REwH}})$  be the PKE scheme. The encryption is defined as  $\mathcal{E}_{\text{REwH}}(pk, m; r) = \mathcal{E}_r(pk, m; \mathcal{RO}_n(pk||m||r))$ . We evaluate the CDA2 advantage of REwH in the  $\mathcal{RO}_n$  model. The message  $\mathbf{m}_b$  is hidden by  $\mathcal{E}_r$  and the randomness  $\mathbf{r}$  is hidden by  $\mathcal{RO}_n$ . When the first stage CDA2 adversary selects  $i$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is some bit of  $\mathbf{m}_b$  and a random bit, if the second stage CDA2 adversary hits the bit, then the adversary can break the CDA security by setting  $b$  in the obtained bit via the CDA1 adversary (Lemma 1). Thus in this case the CDA2 advantage is bounded by the CDA advantage. When the first stage CDA2 adversary selects  $i$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is some bit of  $\mathbf{r}$  and a random bit, the probability that the second stage CDA2 adversary hits the random bit is  $1/2$ . Thus in this case the CDA2 advantage is 0. The formal evaluation is given in Appendix G. We thus have the following theorem.

**Theorem 5.** *For any CDA adversary  $A_1, A_2$  in the  $\mathcal{VO}$  model, making queries at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}'}, q_{\text{IC}}, q_{\mathcal{RO}^*}$  and  $q_{\mathcal{TO}^*}$  times to  $\mathcal{RO}_n, \mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ),  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ ),  $\mathcal{RO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ) and  $\mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ), respectively, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  such that*

$$\text{Adv}_{\text{REwH}, \mathcal{O}^*}^{\text{cda}}(A_1, A_2) \leq 3 \cdot \text{Adv}_{\text{REwH}, \mathcal{RO}_n}^{\text{cda}}(\mathcal{A}_1, \mathcal{A}_2) + \frac{q_{\mathcal{RO}^*} q_{\mathcal{TO}^*}}{2^{w-2}}$$

$A_1, A_2$  can make queries at most  $q_{\mathcal{RO}}$  times to  $\mathcal{RO}_n$ . The running time of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  is at most that of the CDA adversary  $A_1, A_2$ .  $\blacklozenge$

**The CDA Security of PtD.** Let  $\text{PtD}[\mathcal{AE}_r] = (\mathcal{K}_{\text{PtD}}, \mathcal{E}_{\text{PtD}}, \mathcal{D}_{\text{PtD}})$  be the PKE scheme. The encryption is defined as  $\mathcal{E}_{\text{PtD}}(pk_d, m; r) = \mathcal{E}_d(pk_d, r||m)$ . For the CDA1 advantage of PtD, the deterministic encryption  $\mathcal{E}_d$  ensures that the PRIV security of  $\mathcal{E}_d$  ensure the CDA1 security of PtD. The same is hold for the CDA2 security from Lemma 1. The formal evaluation is given in Appendix H. We have the following theorem.

**Theorem 6.** *For any CDA adversary  $A_1, A_2$  in the  $\mathcal{VO}$  model, making queries at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}'}, q_{\text{IC}}, q_{\mathcal{RO}^*}$  and  $q_{\mathcal{TO}^*}$  times to  $\mathcal{RO}_n, \mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ),  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ ),  $\mathcal{RO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ) and  $\mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ), respectively, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  or a PRIV adversary  $B_1, B_2$  such that*

$$\text{Adv}_{\text{PtD}, \mathcal{O}^*}^{\text{cda}}(A_1, A_2) \leq 2 \cdot \text{Adv}_{\text{PtD}, \mathcal{RO}_n}^{\text{cda}}(\mathcal{A}_1, \mathcal{A}_2) + 2 \cdot \text{Adv}_{\mathcal{AE}_d, \mathcal{RO}_n}^{\text{priv}}(B_1, B_2) + \frac{q_{\mathcal{RO}^*} q_{\mathcal{TO}^*}}{2^{w-2}}$$

$A_1, A_2$  and  $B_1, B_2$  can make queries at most  $q_{\mathcal{RO}}$  times to  $\mathcal{RO}_n$ . The running times of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  and the PRIV adversary  $B_1, B_2$  are at most that of the CDA adversary  $A_1, A_2$ .  $\blacklozenge$

**The CDA Security of RtD.** Let  $\text{RtD}[\mathcal{AE}_r] = (\mathcal{K}_{\text{RtD}}, \mathcal{E}_{\text{RtD}}, \mathcal{D}_{\text{RtD}})$  be the PKE scheme. The encryption is defined as  $\mathcal{E}_{\text{RtD}}((pk_r, pk_d), m; r) = \mathcal{E}_d(pk_d, \mathcal{E}_r(pk_r, m; r)||10^l)$  where the randomized encryption  $\mathcal{E}_r$  preserves the mini-entropy of its inputs. Thus, RtD is the special case of PtD. Namely, the CDA security of PtD ensures that of RtD. We thus have the following theorem.

**Theorem 7.** *For any CDA adversary  $A_1, A_2$  in the  $\mathcal{VO}$  model, making queries at most  $q_{\mathcal{RO}}, q_{\mathcal{RO}'}, q_{\text{IC}}, q_{\mathcal{RO}^*}$  and  $q_{\mathcal{TO}^*}$  times to  $\mathcal{RO}_n, \mathcal{RO}_{n_j}^j$  ( $j = 1, \dots, v$ ),  $\text{IC}_{k_t, m_t}^{(t)}$  ( $t = 1, \dots, s$ ),  $\mathcal{RO}_{w_i}^{(i)}$  ( $i = 1, \dots, u$ ) and  $\mathcal{TO}^{(i)}$  ( $i = 1, \dots, u$ ), respectively, there exists a CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  or a PRIV adversary  $B_1, B_2$  such that*

$$\text{Adv}_{\text{RtD}, \mathcal{O}^*}^{\text{cda}}(A_1, A_2) \leq 2 \cdot \text{Adv}_{\text{RtD}, \mathcal{RO}_n}^{\text{cda}}(\mathcal{A}_1, \mathcal{A}_2) + 2 \cdot \text{Adv}_{\mathcal{AE}_d, \mathcal{RO}_n}^{\text{priv}}(B_1, B_2) + \frac{q_{\mathcal{RO}^*} q_{\mathcal{TO}^*}}{2^{w-2}}$$

$A_1, A_2$  and  $B_1, B_2$  can make queries at most  $q_{\mathcal{RO}}$  times to  $\mathcal{RO}_n$ . The running times of the CDA adversary  $\mathcal{A}_1, \mathcal{A}_2$  and the PRIV adversary  $B_1, B_2$  are at most that of the CDA adversary  $A_1, A_2$ .  $\blacklozenge$

## 6 Conclusion and Future Works

We proved that for any PKE scheme being PRIV secure in the RO model and all hedged PKE schemes REwH, RtD and PtD, the adaptive CDA security and the non-adaptive CDA security in both CPA and CCA cases are preserved when a RO is replaced with the indiffereniable hash functions, PFMD, Sponge, and chop MD. First, we proposed the Versatile Oracle  $\mathcal{VO}$ , and showed that the PFMD hash function, the Sponge hash function, and the chop MD hash function are reset indiffereniable from  $\mathcal{VO}$ s. Second, we proved that for the PKE schemes the CDA security are preserved when a RO is replaced with  $\mathcal{VO}$ . The reset indiffereniable composition theorem ensures the CDA security when a RO is replaced with the indiffereniable hash functions. So far, there is no positive result for the reset indiffereniable. So, our result is the first time positive result.

For other indiffereniable hash functions, e.g., the SHA-3 finalists JH [28] and Grøstl [21], the CDA security is still open. We conjecture that our approach can be applied to the CDA security proof for these indiffereniable hash functions.

### Acknowledgements

The author would like to thank the anonymous Eurocrypt 2012 referees for very useful comments that helped to improve the paper.

### References

1. Elena Andreeva, Atul Luykx, and Bart Mennink. Provable security of blake with non-ideal compression function, eprint 2011/620. 2011.
2. Elena Andreeva, Bart Mennink, and Bart Preneel. On the Indiffereniable of the Grøstl Hash Function. In *SCN*, volume 6280 of *LNCS*, pages 88–105. Springer, 2010.
3. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan. SHA-3 proposal BLAKE. Submission to NIST (Round 3). 2010.
4. Mihir Bellare, Alexandra Boldyreva, and Adam O’Neill. Deterministic and Efficiently Searchable Encryption. In *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 535–552. Springer, 2007.
5. Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged public-key encryption: How to protect against bad randomness. In *ASIACRYPT*, volume 5912 of *LNCS*, pages 232–249. Springer, 2009.
6. Mihir Bellare, Marc Fischlin, Adam O’Neill, and Thomas Ristenpart. Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. In *CRYPTO*, volume 5157 of *LNCS*, pages 360–378. Springer, 2008.
7. Mihir Bellare and Thomas Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 299–314. Springer, 2006.
8. Mihir Bellare and Phillip Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer, 1994.
9. 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.
10. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the Indiffereniable of the Sponge Construction. In *EUROCRYPT*, pages 181–197, 2008.
11. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak SHA-3 submission. Submission to NIST (Round 3). 2011.
12. Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi. Security Analysis of the Mode of JH Hash Function. In *FSE*, volume 6147 of *LNCS*, pages 168–191. Springer, 2010.
13. Alexandra Boldyreva, Serge Fehr, and Adam O’Neill. On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles. In *CRYPTO*, volume 5157 of *LNCS*, pages 335–359. Springer, 2008.
14. Donghoon Chang, Sangjin Lee, Mridul Nandi, and Moti Yung. Indiffereniable 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.
15. Donghoon Chang and Mridul Nandi. Improved Indiffereniable Security Analysis of chopMD Hash Function. In *FSE*, pages 429–443, 2008.
16. Donghoon Chang, Mridul Nandi, and Moti Yung. Indiffereniable of the Hash Algorithm BLAKE, ePrint 2011/623. 2011.

17. 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.
18. Ivan Damgård. A Design Principle for Hash Functions. In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 416–427. Springer, 1989.
19. Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *EUROCRYPT (Full Version in ePrint 2009/177)*, volume 5479 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2009.
20. Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. Submission to NIST (Round 3). 2010.
21. Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen. Grøstl – a SHA-3 candidate. Submission to NIST (Round 3). 2011.
22. Shoichi Hirose, Je Hong Park, and Aaram Yun. A Simple Variant of the Merkle-Damgård Scheme with a Permutation. In *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 113–129. Springer, 2007.
23. 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.
24. Ralph C. Merkle. One Way Hash Functions and DES. In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 428–446. Springer, 1989.
25. National Institute of Standards and Technology. Cryptographic Hash Algorithm Competition.
26. National Institute of Standards and Technology. FIPS PUB 180-3 Secure Hash Standard. In *FIPS PUB*, 2008.
27. Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with Composition: Limitations of the Indifferentiability Framework. In *EUROCRYPT (Full Version: ePrint 2011/339)*, volume 6632 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2011.
28. Hongjun Wu. The Hash Function JH. Submission to NIST (Round 3). 2011.

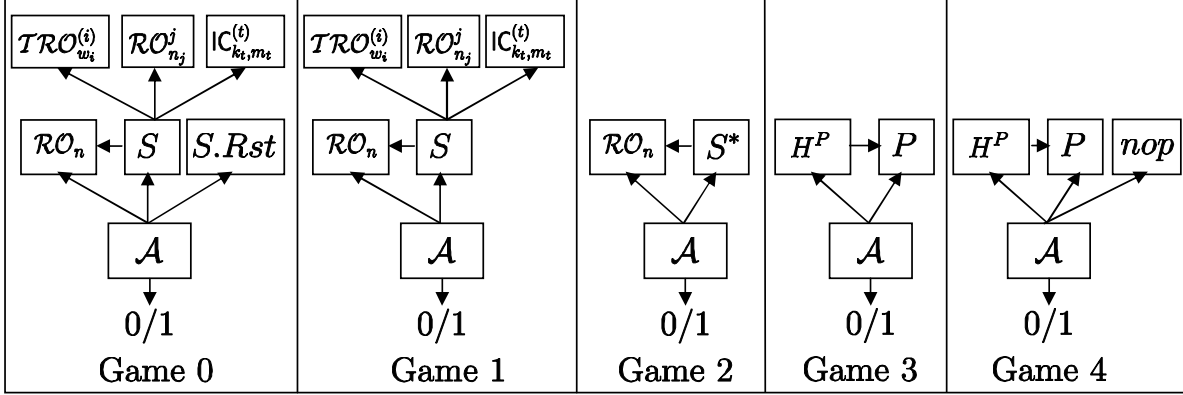


Fig. 6. Games of Reset Indifferentiable Security Proof

## A The Strategy of Reset Indifferentiable Security Proofs

We prove the reset indifferentiable security by using the following strategy which enables to modularly incorporate the previous original indifferentiable security result into our proof.

Let  $P$  be some ideal primitive. Let  $H^P : \{0, 1\}^* \rightarrow \{0, 1\}^n$  be a hash function using  $P$ . In the reset indifferentiable game, in the  $H^P$  world the distinguisher interacts with  $(\mathcal{R}\mathcal{O}_n, \hat{S})$  ( $\mathcal{V}\mathcal{O}$  scenario) and  $(H^P, P)$  ( $H^P$  scenario) where  $\hat{S} = (S, S.Rst)$  and the simulator  $S$  simulates  $P$ . The simulator  $S$  has oracle access to  $\mathcal{V}\mathcal{O}.pub$ . Let  $S^*$  be the simulator of the original indifferentiable security from  $\mathcal{R}\mathcal{O}_n$  for  $H^P$  where the simulator  $S^*$  has oracle access to  $\mathcal{R}\mathcal{O}_n$ .

To evaluate the reset indifferentiable advantage, we employ the following strategy which consists of the five games.

- Game 0. This is the  $\mathcal{V}\mathcal{O}$  scenario. Thus  $\mathcal{A}$  has oracle access to  $(\mathcal{R}\mathcal{O}_n, \hat{S})$ .
- Game 1. This game is equal to Game 0 but  $S.Rst$  is removed. Thus  $\mathcal{A}$  has oracle access to  $(\mathcal{R}\mathcal{O}_n, S)$ .
- Game 2. This game is the RO scenario of the original indifferentiable security game of  $H^P$ . Thus  $\mathcal{A}$  has oracle access to  $(\mathcal{R}\mathcal{O}_n, S^*)$ .
- Game 3. This game is the  $H^P$  scenario of the original indifferentiable security game. Thus  $\mathcal{A}$  has oracle access to  $(H^P, P)$ .
- Game 4. This game is the  $H^P$  scenario of the reset indifferentiable security game. Thus  $\mathcal{A}$  has oracle access to  $(H^P, P, nop)$ .

Let  $G_i$  be an event that  $\mathcal{A}$  outputs 1 in Game  $i$ . Then,

$$\begin{aligned} \text{Adv}_{H^P, \mathcal{V}\mathcal{O}, S}^{r\text{-indiff}}(\mathcal{A}) &\leq \Pr[G0] - \Pr[G4] \\ &\leq (\Pr[G0] - \Pr[G1]) + (\Pr[G1] - \Pr[G2]) + (\Pr[G2] - \Pr[G3]) + (\Pr[G3] - \Pr[G4]) \end{aligned}$$

The difference  $(\Pr[G2] - \Pr[G3])$  is equal to the advantage of the original indifferentiable security of  $H^P$  from a RO. We denote the bound of the advantage by  $p^*$ . Since  $nop$  takes no input and does not nothing,  $\Pr[G3] = \Pr[G4]$ . Thus for any distinguisher  $\mathcal{A}$ , the following holds.

$$\text{Adv}_{H^P, \mathcal{V}\mathcal{O}, S}^{r\text{-indiff}}(\mathcal{A}) \leq (\Pr[G0] - \Pr[G1]) + (\Pr[G1] - \Pr[G2]) + p^*.$$

So the remaining work is to define the simulator  $S$  such that the simulator does not update the internal state and the difference  $(\Pr[G1] - \Pr[G2])$  is small. If the simulator does not update the internal state,  $S.Rst$  gives no advantage to  $\mathcal{A}$ , that is,  $\Pr[G0] = \Pr[G1]$ .

$\overline{S^*(x, y)}$ 01 if $T_{S^*}[x, y] \neq \perp$ then <b>return</b> $T_{S^*}[x, y]$ ; 02 if $x = IV$ then 03   if $\exists M$ s.t. $\text{pfpad}(M) = y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 04   else 05 $z \leftarrow \{0, 1\}^n$ ; 06     if $\text{Path}[z] = \perp$ then $\text{Path}[z] \leftarrow y$ ; 07 else if $\text{Path}[x] = M^* \neq \perp$ then 08   if $\exists M$ s.t. $\text{pfpad}(M) = M^*    y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 09   else 10 $z \leftarrow \{0, 1\}^n$ ; 11     if $\text{Path}[z] = \perp$ then $\text{Path}[z] \leftarrow M^*    y$ ; 12 else $z \xleftarrow{\$} \{0, 1\}^n$ ; 13 $T_{S^*}[x, y] \leftarrow z$ ; 14 <b>return</b> $T_{S^*}[x, y]$ ; 	$\overline{\mathcal{O}(x, y)}$ 1 $M^* \leftarrow \mathcal{TO}^{(1)}(x)$ ; 2 if $x = IV$ then 3   if $\exists M$ s.t. $\text{pfpad}(M) = y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 4   else $z \leftarrow \mathcal{RO}_n^{(1)}(y)$ ; 5 else if $M^* \neq \perp$ then 6   if $\exists M$ s.t. $\text{pfpad}(M) = M^*    y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 7   else $z \leftarrow \mathcal{RO}_n^{(1)}(M^*    y)$ ; 8 else $z \leftarrow \mathcal{RO}_n^1(x    y)$ ; 9 <b>return</b> $z$ ; 
---	---

**Fig. 7.** Simulator  $S^*$  (Left) and Game PF1 (Right)

$\overline{\mathcal{O}(x, y)}$ 01 if $x = IV$ then 02   if $\exists M$ s.t. $\text{pfpad}(M) = y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 03   else 04     if $F_1^*[y] = \perp$ then $F_1^*[y] \xleftarrow{\$} \{0, 1\}^n$ ; 05 $z \leftarrow F_1^*[y]$ ; 06 else if $\exists M^*$ s.t. $F_1^*[M^*] = x$ then 07   if $\exists M$ s.t. $\text{pfpad}(M) = M^*    y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 08   else 09     if $F_1^*[M^*    y] = \perp$ then $F_1^*[M^*    y] \xleftarrow{\$} \{0, 1\}^n$ ; 10 $z \leftarrow F_1^*[M^*    y]$ ; 11 else 12   if $F_1[x    y] = \perp$ then $F_1[x    y] \xleftarrow{\$} \{0, 1\}^n$ ; 13 $z \leftarrow F_1[x    y]$ ; 14 $T_{S^*}[x, y] \leftarrow z$ ; 15 <b>return</b> $T_{S^*}[x, y]$ ; 	$\overline{\mathcal{O}(x, y)}$ 01 if $T_{S^*}[x, y] \neq \perp$ then <b>return</b> $T_{S^*}[x, y]$ ; 02 if $x = IV$ then 03   if $\exists M$ s.t. $\text{pfpad}(M) = y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 04   else 05     if $F_1^*[y] = \perp$ then $F_1^*[y] \xleftarrow{\$} \{0, 1\}^n$ ; 06 $z \leftarrow F_1^*[y]$ ; 07 else if $\exists M^*$ s.t. $F_1^*[M^*] = x$ then 08   if $\exists M$ s.t. $\text{pfpad}(M) = M^*    y$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 09   else 10     if $F_1^*[M^*    y] = \perp$ then $F_1^*[M^*    y] \xleftarrow{\$} \{0, 1\}^n$ ; 11 $z \leftarrow F_1^*[M^*    y]$ ; 12 else 13   if $F_1[x    y] = \perp$ then $F_1[x    y] \xleftarrow{\$} \{0, 1\}^n$ ; 14 $z \leftarrow F_1[x    y]$ ; 15 $T_{S^*}[x, y] \leftarrow z$ ; 16 <b>return</b> $T_{S^*}[x, y]$ ; 
---	--

**Fig. 8.** Game PF2 (left), and Game PF3 (right)

## B Proof of Theorem 1

We prove Theorem 1 by using the strategy in Appendix A.

Since the simulator  $S$  does not update the internal state,  $\Pr[G0] - \Pr[G1] = 0$ .

We use the result of the indistinguishable security by Chang *et al.* [14]. They defined a simulator  $S^*$  which is shown in Fig. 7.  $T_{S^*}$  is a (initially everywhere  $\perp$ ) table which records query-response values of  $S^*$ . For the query  $S^*(x, y)$ , the response is recorded in  $T_{S^*}[x, y]$ .  $\text{Path}$  is a (initially everywhere  $\perp$ ) table which records all paths with the Merkle-Damgård style. If triples  $(z_0, y_1, z_1), (z_1, y_2, z_2), (z_2, y_3, z_3)$  are recoded in  $T_{S^*}$  where  $T_{S^*}[z_{j-1}, y_j] = z_j$  and  $z_0 = IV$ ,  $y_1 || y_2 || y_3$  is recoded in  $\text{Path}[z_3]$ <sup>3</sup>. The task of the simulator  $S^*$  is to simulate  $h$  so that  $\mathcal{RO}_n$  and  $S^*$  are consistent. So the response of  $S^*(x, y)$  is defined by the output of  $\mathcal{RO}_n(M)$  if there exists  $M^*$  such that  $\text{Path}[x] = M^*$  and there exists  $M$  such that  $\text{pfpad}(M) = M^* || y$ . They show that the advantage  $p^*$  of the indistinguishable security is bounded by  $\mathcal{O}((lq_H + q_n)^2 / 2^n)$ .

We evaluate the difference  $\Pr[G1] - \Pr[G2]$  where the distinguisher interacts with  $(\mathcal{RO}_n, S)$  in Game 1 and  $(\mathcal{RO}_n, S^*)$  in Game 2. Since the difference between Game 1 and Game 2 is a simulator, we consider

<sup>3</sup> Note that in [14], the paths are recorded by using another formula, which is a relation  $\mathcal{R}$ , but the table  $\text{Path}$  realizes the same role as the relation.



<pre> <math>\mathcal{O}(x, y)</math> 01 if <math>T_{S^*}[x, y] \neq \perp</math> then <b>return</b> <math>T_{S^*}[x, y]</math>; 02 if <math>x = IV</math> then 03   if <math>\exists M</math> s.t. <math>\text{pfpad}(M) = y</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 04   else 05     <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 06     <math>F_1^*[y] \leftarrow z</math>; 07 else if <math>\exists M^*</math> s.t. <math>F_1^*[M^*] = x</math> then 08   if <math>\exists M</math> s.t. <math>\text{pfpad}(M) = M^*  y</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 09   else 10     <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 11     <math>F_1^*[M^*  y] \leftarrow z</math>; 12 else 13   <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 14   <math>F_1[x  y] \leftarrow z</math>; 15 <math>T_{S^*}[x, y] \leftarrow z</math>; 16 <b>return</b> <math>T_{S^*}[x, y]</math>; </pre>	<pre> <math>\mathcal{O}(x, y)</math> 01 if <math>T_{S^*}[x, y] \neq \perp</math> then <b>return</b> <math>T_{S^*}[x, y]</math>; 02 if <math>x = IV</math> then 03   if <math>\exists M</math> s.t. <math>\text{pfpad}(M) = y</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 04   else 05     <math>z \leftarrow \{0, 1\}^n</math>; 06     if <math>\text{Path}[z] = \perp</math> then <math>\text{Path}[z] \leftarrow y</math>; 07 else if <math>\text{Path}[x] = M^* \neq \perp</math> then 08   if <math>\exists M</math> s.t. <math>\text{pfpad}(M) = M^*  y</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 09   else 10     <math>z \leftarrow \{0, 1\}^n</math>; 11     if <math>\text{Path}[z] = \perp</math> then <math>\text{Path}[z] \leftarrow M^*  y</math>; 12 else <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 13 <math>T_{S^*}[x, y] \leftarrow z</math>; 14 <b>return</b> <math>T_{S^*}[x, y]</math>; </pre>
---	---

**Fig. 9.** Game PF4 (left), and Game PF5 (right)

the distinguishing game between  $S$  and  $S^*$ . We evaluate the difference  $\Pr[A_1^S \Rightarrow 1] - \Pr[A_1^{S^*} \Rightarrow 1]$  for any distinguisher  $A_1$  which outputs a bit.

We consider the five games, Game PF1, Game PF2, Game PF3, Game PF4, and Game PF5. In each game, the distinguisher  $A_1$  interacts with  $\mathcal{O}$  which is shown in Figs. 7, 8, and 9.  $\mathcal{O}$  in Game PF1 is equal to  $S$  and  $\mathcal{O}$  in Game PF5 is equal to  $S^*$ . Let  $GPFj$  be an event that in Game PF $j$   $A_1$  outputs 1. Thus

$$\begin{aligned} \Pr[G1] - \Pr[G2] &= \Pr[GPF1] - \Pr[GPF5] \\ &= \sum_{j=1}^4 \Pr[GPFj] - \Pr[GPF(j+1)] \end{aligned}$$

First we evaluate the difference  $\Pr[GPF1] - \Pr[GPF2]$ . In Game PF2, the procedures of  $\mathcal{TR}\mathcal{O}_n^{(1)}$  and  $\mathcal{R}\mathcal{O}_n^1$  are hard-coded. Thus this modification does not affect the distinguisher's view and  $\Pr[GPF1] = \Pr[GPF2]$ .

We evaluate the difference  $\Pr[GPF2] - \Pr[GPF3]$ . In Game PF3, for a repeated query to  $\mathcal{O}$ , the value which was previously defined is returned due to the step 01. In Game PF2, due to the condition of the step 06, the following cases might differentiate Game PF2 from Game PF3, where for a repeated query, the value which was previously defined may not be returned.

- Case 1: A collision for  $F_1^*$  occurs in Game PF2.
- Case 2: In Game PF2, first, for a query  $\mathcal{O}(x, y)$ , the output  $z$  is defined in the steps 12-14. Second, a value  $M^*$  is defined such that  $F_1^*[M^*] = x$ . Then, for a repeated query,  $\mathcal{O}(x, y)$ , the output  $z$  is defined in the steps 07-11.

The collision probability is bounded by  $q_h^2/2^{n+1}$  from a birthday analysis and the probability of Case 2 is bounded by  $q_h^2/2^n$ , since the number of such  $M^*$  is at most  $q_h$ . We thus have

$$\Pr[GPF2] - \Pr[GPF3] \leq \frac{3q_h^2}{2^{n+1}}.$$

We evaluate the difference  $\Pr[GPF3] - \Pr[GPF4]$ . In Game PF4, “if” in the steps 05, 10, and 13 is removed. So some value of the tables  $F_1^*$  and  $F_1$  might be redefined. However, the table  $T_{S^*}$  prevents the redefinition. Thus this modification does not affect the distinguisher's view and  $\Pr[GPF3] = \Pr[GPF4]$ .

Finally, we evaluate the difference  $\Pr[GPF4] - \Pr[GPF5]$ . In Game PF4, the table  $F_1^*$  is replaced with the table  $\text{Path}$  and  $F_1$  is removed.  $F_1$  is not used in Game PF4. For a pair  $(M, z)$ , if  $F_1^*[M] = z$  in Game PF4 then  $\text{Path}[z] = M$  in Game PF5. Thus if no collision for the table  $F_1^*$  occurs, this modification does not

affects the distinguisher's view. The collision probability is at most  $q_h^2/2^{n+1}$  from a birthday analysis. We thus have

$$\Pr[GPF4] - \Pr[GPF5] \leq \frac{q_h^2}{2^{n+1}}.$$

□

<pre> <math>S_+^*(x, y)</math> 01 if <math>T_{S_+^*}[x, y] \neq \perp</math> then <b>return</b> <math>T_{S_+^*}[x, y]</math>; 02 if <math>y = IV_2</math> then 03   if <math>\text{unpad}_S(IV_1 \oplus x) = M \neq \perp</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 04   else <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 05 else if <math>\text{Path}[y] \neq \perp</math> then 06   let <math>\text{Path}[y] = (M^*, z^*)</math>; 07   if <math>\text{unpad}_S(M^*    (z^* \oplus x)) = M \neq \perp</math> then <math>z \leftarrow \mathcal{R}\mathcal{O}_n(M)</math>; 08   else <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 09 else <math>z \xleftarrow{\\$} \{0, 1\}^n</math>; 10 <math>w \xleftarrow{\\$} \{0, 1\}^c \setminus T_F[z]</math>; 11 <math>\text{Update}_{S^*}(x, y, z, w)</math>; 12 <b>return</b> <math>z    w</math>; </pre>	<pre> <math>S_-^*(z, w)</math> 1 if <math>T_{S_-^*}[z, w] \neq \perp</math> then <math>T_{S_-^*}[z, w]</math>; 2 <math>x \xleftarrow{\\$} \{0, 1\}^n</math>; <math>y \xleftarrow{\\$} \{0, 1\}^c \setminus T_I[x]</math>; 3 <math>\text{Update}_{S^*}(x, y, z, w)</math>; 4 <b>return</b> <math>x    y</math>; </pre>
--	---

Fig. 10. Simulator  $S^*$

## C Proof of Theorem 2

We prove Theorem 2 by using the strategy in Appendix A.

Since the simulator  $S$  does not update the internal state,  $\Pr[G0] - \Pr[G1] = 0$ .

We use the result of the indifferentiable security by Bertoni *et al.* [10]. They define a simulator  $S^* = (S_+^*, S_-^*)$  which is shown in Fig. 10.  $S_+^*$  and  $S_-^*$  simulate the random permutation  $P$  and its inverse  $P^{-1}$ , respectively.  $T_{S_+^*}$  and  $T_{S_-^*}$  are (initially everywhere  $\perp$ ) tables which records query-response values of  $S_+^*$  and  $S_-^*$ . For the query  $S_+^*(x, y)$ , the response  $z || w$  is recorded in  $T_{S_+^*}[x, y]$  and  $x || y$  is recoded in  $T_{S_-^*}[z, w]$ . Similarly, the response  $z || w$  of the query  $S_-^*(x, y)$  and  $x || y$  are recoded in these tables.  $\text{Path}$  is a (initially everywhere  $\perp$ ) table which records all paths with the Sponge style. If triples  $(x_1, w_0, z_1, w_1), (x_2, w_1, z_2, w_2), (x_3, w_2, z_3, w_3)$  are the query-response values where  $T_{S_+^*}[x_j, w_{j-1}] = z_j || w_j$  ( $j = 1, 2, 3$ ) and  $w_0 = IV_2$ , then  $(x_1 \oplus IV_1) || ((x_2 \oplus z_1) || (x_3 \oplus z_2))$  and  $z_3$  is recoded in  $\text{Path}[w_3]$ .  $T_F$  and  $T_I$  are (initially everywhere  $\perp$ ) tables.  $T_F[z]$  includes values which are all  $y'$  such that  $T_{S_+^*}[y', z] \neq \perp$ ,  $IV_2$ , all  $y''$  such that  $\text{Path}[y''] \neq \perp$ , and all  $w'$  such that  $T_{S_-^*}[z || w'] \neq \perp$ .  $T_I[x]$  includes values which are  $IV_2$ , all  $y'$  such that  $\text{Path}[y'] \neq \perp$ , and all  $y''$  such that  $T_{S_+^*}[x, y'']$ .  $\text{Update}_{S^*}(x, y, z, w)$  is a procedure that the tables  $T_{S_+^*}, T_{S_-^*}$ , and  $\text{Path}$  are updated by using  $(x, y, z, w)$ , namely,  $T_{S_+^*}[x, y] \leftarrow z || w$ ,  $T_{S_-^*}[z, w] \leftarrow x || y$ , and if  $\text{Path}[y] = (M, z^*) \neq \perp$  then  $\text{Path}[w] \leftarrow (M || (x \oplus z^*), z)$ <sup>4</sup>. Notice that the tables  $T_F$  and  $T_I$  are used to avoid that a multi-path is defined in  $\text{Path}$ . They show that the advantage  $p^*$  of the indifferentiable security is bounded by  $((1 - 2^{-n})q^2 + (1 + 2^{-n}q))/2^n$ .

We evaluate the difference  $\Pr[G1] - \Pr[G2]$  where a distinguisher interacts with  $(\mathcal{R}\mathcal{O}_n, S)$  in Game 1 and  $(\mathcal{R}\mathcal{O}_n, S^*)$  in Game 2. Since the difference between Game 1 and Game 2 is a simulator, we consider the distinguishing game between  $S$  and  $S^*$ . We evaluate the difference  $\Pr[A_1^S \Rightarrow 1] - \Pr[A_1^{S^*} \Rightarrow 1]$  for any distinguisher  $A_1$  which outputs a bit.

We consider the seven games Game S1, Game S2, Game S3, Game S4, Game S5, Game S6, and Game S7. In each game, the distinguisher interacts with  $(\mathcal{O}_+, \mathcal{O}_-)$  shown in Figs. 11, 12, 13 14, 15, 16, and 17. Game S1 is equal to Game 1 and Game S7 is equal to Game 2. Let  $GSj$  be an event that  $A_1$  output 1 in Game Sj. Thus

$$\begin{aligned}
\Pr[G1] - \Pr[G2] &= \Pr[GS1] - \Pr[GS7] \\
&= \sum_{j=1}^6 (\Pr[GSj] - \Pr[GS(j+1)]).
\end{aligned}$$

In the following, we evaluate each difference  $\Pr[GSj] - \Pr[GS(j+1)]$ .

<sup>4</sup> Note that in [10], the paths and the query-response values are recorded by using a graph representation, but the table  $\text{Path}$  and the tables  $T_{S_+^*}, T_{S_-^*}$  realizes the same role as the graph.

$\mathcal{O}_+(x, y)$ 01 $M^* \leftarrow \mathcal{TO}^{(1)}(y);$ 02 if $y = IV_2$ then 03   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M);$ 04   else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x);$ 05 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1);$ 06 else if $M^* \neq \perp$ then 07   if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M');$ 08   else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*);$ 08   if $\text{unpad}_S(M^*    m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M);$ 09   else $z \leftarrow \mathcal{RO}_n^1(M^*    m);$ 10 $w \leftarrow \mathcal{RO}_c^{(1)}(M^*    m);$ 11 else $z    w \leftarrow \mathcal{P}(x    y);$ 12 <b>return</b> $z    w;$	$\mathcal{O}_-(z, w)$ 01 $M \leftarrow \mathcal{TO}^{(1)}(w);$ 02 if $M \neq \perp$ and $ M  = n$ then 03 $x \leftarrow IV_1 \oplus M; y \leftarrow IV_2;$ 04 if $M \neq \perp$ and $ M  > n$ then 05   let $M = M^*    m$ ( $ m  = n$ ); 06   if $\text{unpad}_S(M^*) = M' \neq \perp$ then $x \leftarrow m \oplus \mathcal{RO}_n(M');$ 07   else $x \leftarrow m \oplus \mathcal{RO}_n^1(M^*);$ 08 $y \leftarrow \mathcal{RO}_c^{(1)}(M^*);$ 09 else $x    y \leftarrow \mathcal{P}^{-1}(z    w);$ 10 <b>return</b> $x    y;$
---	---

Fig. 11. Game S1

$\mathcal{O}_+(x, y)$ 01 $M^* \leftarrow \mathcal{TO}^{(1)}(y);$ 02 if $y = IV_2$ then 03   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M);$ 04   else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x);$ 05 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1);$ 06 else if $M^* \neq \perp$ then 07   if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M');$ 08   else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*);$ 09   if $\text{unpad}_S(M^*    m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M);$ 10   else $z \leftarrow \mathcal{RO}_n^1(M^*    m);$ 11 $w \leftarrow \mathcal{RO}_c^{(1)}(M^*    m);$ 12 else $z    w \leftarrow \mathcal{P}_1(x    y);$ 13 <b>return</b> $z    w;$	$\mathcal{O}_-(z, w)$ 01 $M \leftarrow \mathcal{TO}^{(1)}(w);$ 02 if $M \neq \perp$ and $ M  = n$ then 03 $x \leftarrow IV_1 \oplus M; y \leftarrow IV_2;$ 04 else if $M \neq \perp$ and $ M  > n$ then 05   let $M = M^*    m$ ( $ m  = n$ ); 06   if $\text{unpad}_S(M^*) = M' \neq \perp$ then $x \leftarrow m \oplus \mathcal{RO}_n(M');$ 07   else $x \leftarrow m \oplus \mathcal{RO}_n^1(M^*);$ 08 $y \leftarrow \mathcal{RO}_c^{(1)}(M^*);$ 09 else $x    y \leftarrow \mathcal{P}_1^{-1}(z    w);$ 10 <b>return</b> $x    y;$
$\mathcal{P}_1(x)$ 1 if $F^+[x] = \perp$ , ret $F^+[x];$ 2 $y \xleftarrow{\$} \{0, 1\}^b;$ 3 $\text{Update}_P(x, y);$ 4 <b>return</b> $F^+[x];$	$\mathcal{P}_1^{-1}(y)$ 1 if $F^-[y] = \perp$ , ret $F^-[y];$ 2 $x \xleftarrow{\$} \{0, 1\}^b;$ 3 $\text{Update}_P(x, y);$ 4 <b>return</b> $F^-[y];$

Fig. 12. Game S2

**Game S2.** In this game, a random permutation  $(\mathcal{P}, \mathcal{P}^{-1})$  is replaced with a new function  $(\mathcal{P}_1, \mathcal{P}_1^{-1})$ .  $F^+$  and  $F^-$  are (initially everywhere  $\perp$ ) tables.  $\text{Update}_P(x, y)$  updates the tables  $F^+$  and  $F^-$ :  $F^+[x] \leftarrow y$  and  $F^-[y] \leftarrow x$ . An output of  $(\mathcal{P}_1, \mathcal{P}_1^{-1})$  is randomly chosen from  $\{0, 1\}^b$ . Thus if in Game GS2 no collision occurs for the outputs of  $(\mathcal{P}_1, \mathcal{P}_1^{-1})$ , Game GS2 is equal to Game GS1. We thus have via a birthday analysis that

$$\Pr[GS1] - \Pr[GS2] \leq \frac{q^2}{2^{b+1}}.$$

**Game S3.** In this game, tables  $T_{S^+}$  and  $T_{S^-}$  are used which record the outputs of  $\mathcal{O}_+$  and  $\mathcal{O}_-$ . Note that the procedure  $\text{Update}_{S^*}$  updates tables  $T_{S^+}$ ,  $T_{S^-}$ , and  $\text{Path}$ . In Game S3, for a repeated query, the value, which was previously returned, is returned if no collision for the outputs of  $\mathcal{O}_+$  or the outputs of  $\mathcal{O}_-$  occurs. In Game S2, due to the condition 07, for a repeated query, the value, which was previously returned, is returned if the following cases don't occur.

- A collision of  $\mathcal{RO}_c^{(1)}$  occurs.

$\mathcal{O}_+(x, y)$ 01 if $T_{S_+^*}[x, y] \neq \perp$ then <b>return</b> $T_{S_+^*}[x, y]$ ; 02 $M^* \leftarrow \mathcal{TO}^{(1)}(y)$ ; 03 if $y = IV_2$ then 04   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 05   else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x)$ ; 06 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1)$ ; 07 else if $M^* \neq \perp$ then 08   if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M')$ ; 09   else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*)$ ; 10   if $\text{unpad}_S(M^*  m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 11   else $z \leftarrow \mathcal{RO}_n^1(M^*  m)$ ; 12 $w \leftarrow \mathcal{RO}_c^{(1)}(M^*  m)$ ; 13 else $z  w \leftarrow \mathcal{P}_1(x  y)$ ; 14 $Update_{S^*}(x, y, z, w)$ ; 15 <b>return</b> $z  w$ ;	$\mathcal{O}_-(z, w)$ 01 if $T_{S_-^*}[z, w] \neq \perp$ then $T_{S_-^*}[z, w]$ ; 02 $M \leftarrow \mathcal{TO}^{(1)}(w)$ ; 03 if $M \neq \perp$ and $ M  = n$ then 04 $x \leftarrow IV_1 \oplus M$ ; $y \leftarrow IV_2$ ; 05 else if $M \neq \perp$ and $ M  > n$ then 06   let $M = M^*  m$ ( $ m  = n$ ); 07   if $\text{unpad}_S(M^*) = M_1 \neq \perp$ then $x \leftarrow m \oplus \mathcal{RO}_n(M_1)$ ; 08   else $x \leftarrow m \oplus \mathcal{RO}_n^1(M^*)$ ; 09 $y \leftarrow \mathcal{RO}_c^{(1)}(M^*)$ ; 10 else $x  y \leftarrow \mathcal{P}_1^{-1}(z  w)$ ; 11 $Update_{S^*}(x, y, z, w)$ ; 12 <b>return</b> $x  y$ ;
--	--

Fig. 13. Game S3

- First, for a query  $\mathcal{O}_+(x, y)$ , the output  $z||w$  is defined in the step 12, or for a query  $\mathcal{O}_-(z, w)$ , the output  $z||w$  is defined in the step 09. Second, the query  $\mathcal{RO}_c^{(1)}(M^*)$  is made where  $y = \mathcal{RO}_c^{(1)}(M^*)$ . Then, in this case, for a query  $\mathcal{O}_+(x, y)$ , the output  $z^*||w^*$  which is not equal to  $z||w$  is defined in the steps 06-11.

Thus if the following cases do not occurs, then the modification does not affect the distinguisher's view.

- Case 1: A collision of  $\mathcal{RO}_c^{(1)}$  occurs in both games.
- Case 2: In Game S2, first, for a query  $\mathcal{O}_+(x, y)$ , the output  $z||w$  is defined in the step 12, or for a query  $\mathcal{O}_-(z, w)$ , the output  $z||w$  is defined in the step 09. Second, the query  $\mathcal{RO}_c^{(1)}(M^*)$  is made where  $y = \mathcal{RO}_c^{(1)}(M^*)$ . Then, in this case, for a query  $\mathcal{O}_+(x, y)$ , the output  $z^*||w^*$  which is not equal to  $z||w$  is defined in the steps 06-11.

From a birthday analysis, the collision probability for Case1 is at most  $q^2/2^{c+1}$ . For Case 2,  $y$  is a random value of  $c$  bits and the number of such  $M^*$  is at most  $q$ . Thus the probability that Case 2 occurs is at most  $q^2/2^c$ . We thus have that

$$\Pr[GS2] - \Pr[GS3] \leq \frac{3q^2}{2^{c+1}}.$$

**Game S4.** In this game, the steps 02-09 of  $\mathcal{O}_-$  are removed. Since for the query  $\mathcal{O}_-(z, w)$ , “ $M (= \mathcal{TO}^{(1)}(w)) \neq \perp$ ” implies that the query  $\mathcal{RO}_c^{(1)}(M)$  was made by the query  $\mathcal{O}_+(x, y)$  and thus when the query  $\mathcal{O}_-(z, w)$  is made, the response  $T_{S_-^*}[z, w]$  ( $= x||y$ ) has been defined. The steps of  $\mathcal{O}_-$  corresponding with  $M (= \mathcal{TO}^{(1)}(w))$  are the steps 02-09. Note that if a collision for the outputs of  $\mathcal{O}_+$  or the outputs of  $\mathcal{O}_-$  occurs, then the table  $T_{S_+^*}$  or  $T_{S_-^*}$  is redefined. Thus the modification does not affect the distinguisher's view if no collision for the outputs of  $\mathcal{O}_+$  or the outputs of  $\mathcal{O}_-$  occurs. We thus have via a birthday analysis that

$$\Pr[GS3] - \Pr[GS4] \leq \frac{q^2}{2^{b+1}}.$$

**Game S5.** In this game, the table  $Path$  is used instead of  $\mathcal{TO}^{(1)}$ . In Game S5, if  $M^* (= \mathcal{TO}^{(1)}(y)) \neq \perp$ , then  $Path[y] = (M^*, z^*)$ . And if  $Path[y] = (M^*, z^*) \neq \perp$  and no collision of  $\mathcal{RO}_c^{(1)}$  occurs, then  $M^* \neq \perp$  where  $M^* = \mathcal{TO}^{(1)}(y)$ . Thus in both games if no collision for  $\mathcal{RO}_c^{(1)}$  occurs, then Game S5 is equal to Game S4. We thus have via a birthday analysis

$$\Pr[GS4] - \Pr[GS5] \leq \frac{q^2}{2^{c+1}}.$$

$\overline{\mathcal{O}_+(x, y)}$ 01 if $T_{S^*} \perp [x, y] \neq \perp$ then <b>return</b> $T_{S^*} [x, y]$ ; 02 $M^* \leftarrow \mathcal{TO}^{(1)}(y)$ ; 03 if $y = IV_2$ then 04   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 05   else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x)$ ; 06 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1)$ ; 07 else if $M^* \neq \perp$ then 08   if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M')$ ; 09   else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*)$ ; 10   if $\text{unpad}_S(M^*    m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 11   else $z \leftarrow \mathcal{RO}_n^1(M^*    m)$ ; 12 $w \leftarrow \mathcal{RO}_c^{(1)}(M^*    m)$ ; 13 else $z    w \leftarrow \mathcal{P}_1(x    y)$ ; 14 $\text{Update}_{S^*}(x, y, z, w)$ ; 15 <b>return</b> $z    w$ ; 	$\overline{\mathcal{O}_-(z, w)}$ 1 if $T_{S^*} [z, w] \neq \perp$ then $T_{S^*} [z, w]$ ; 2 $x    y \leftarrow \mathcal{P}_1^{-1}(z    w)$ ; 3 $\text{Update}_{S^*}(x, y, z, w)$ ; 4 <b>return</b> $x    y$ ; 
---	--

Fig. 14. Game S4

$\overline{\mathcal{O}_+(x, y)}$ 01 if $T_{S^*} \perp [x, y] \neq \perp$ then <b>return</b> $T_{S^*} [x, y]$ ; 02 if $y = IV_2$ then 03   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 04   else $z \leftarrow \mathcal{RO}_n^1(IV_1 \oplus x)$ ; 05 $w \leftarrow \mathcal{RO}_c^{(1)}(x \oplus IV_1)$ ; 06 else if $\text{Path}[y] = (M^*, z^*) \neq \perp$ then 07   if $\text{unpad}(M^*) = M' \neq \perp$ then $m \leftarrow x \oplus \mathcal{RO}_n(M')$ ; 08   else $m \leftarrow x \oplus \mathcal{RO}_n^1(M^*)$ ; 09   if $\text{unpad}_S(M^*    m) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 10   else $z \leftarrow \mathcal{RO}_n^1(M^*    m)$ ; 11 $w \leftarrow \mathcal{RO}_c^{(1)}(M^*    m)$ ; 12 else $z    w \leftarrow \mathcal{P}_1(x    y)$ ; 13 $\text{Update}_{S^*}(x, y, z, w)$ ; 14 <b>return</b> $z    w$ ; 	$\overline{\mathcal{O}_-(z, w)}$ 1 if $T_{S^*} [z, w] \neq \perp$ then $T_{S^*} [z, w]$ ; 2 $x    y \leftarrow \mathcal{P}_1^{-1}(z    w)$ ; 3 $\text{Update}_{S^*}(x, y, z, w)$ ; 4 <b>return</b> $x    y$ ; 
--	--

Fig. 15. Game S5

$\overline{\mathcal{O}_+(x, y)}$ 01 if $T_{S^*} \perp [x, y] \neq \perp$ then <b>return</b> $T_{S^*} [x, y]$ ; 02 if $y = IV_2$ then 03   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 04   else $z \xleftarrow{\$} \{0, 1\}^n$ ; 05 else if $\text{Path}[y] = (M^*, z^*) \neq \perp$ then 06   if $\text{unpad}_S(M^*    (z^* \oplus x)) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 07   else $z \xleftarrow{\$} \{0, 1\}^n$ ; 08 else $z \xleftarrow{\$} \{0, 1\}^n$ ; 09 $w \xleftarrow{\$} \{0, 1\}^c$ ; 10 $\text{Update}_{S^*}(x, y, z, w)$ ; 11 <b>return</b> $z    w$ ; 	$\overline{\mathcal{O}_-(z, w)}$ 1 if $T_{S^*} [z, w] \neq \perp$ then $T_{S^*} [z, w]$ ; 2 $x \xleftarrow{\$} \{0, 1\}^n$ ; $y \xleftarrow{\$} \{0, 1\}^c$ ; 3 $\text{Update}_{S^*}(x, y, z, w)$ ; 4 <b>return</b> $x    y$ ; 
---	---

Fig. 16. Game S6

**Game S6.** In this game,  $\mathcal{RO}_c^{(1)}$ ,  $\mathcal{RO}_n^1$ ,  $\mathcal{P}$  and  $\mathcal{P}^{-1}$  are removed and  $z^*$  is used in the step 06 of  $\mathcal{O}_+$ . Notice

$\mathcal{O}_+(x, y)$ 01 if $T_{S_+^*}[x, y] \neq \perp$ then <b>return</b> $T_{S_+^*}[x, y]$ ; 02 if $y = IV_2$ then 03   if $\text{unpad}_S(IV_1 \oplus x) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 04   else $z \xleftarrow{\$} \{0, 1\}^n$ ; 05 else if $\text{Path}[y] = (M^*, z^*) \neq \perp$ then 06   if $\text{unpad}_S(M^*    (z^* \oplus x)) = M \neq \perp$ then $z \leftarrow \mathcal{RO}_n(M)$ ; 07   else $z \xleftarrow{\$} \{0, 1\}^n$ ; 08 else $z \xleftarrow{\$} \{0, 1\}^n$ ; 09 $w \xleftarrow{\$} \{0, 1\}^c \setminus T_F[z]$ ; 10 $\text{Update}_{S^*}(x, y, z, w)$ ; 11 <b>return</b> $z    w$ ; 	$\mathcal{O}_-(z, w)$ 1 if $T_{S_-^*}[z, w] \neq \perp$ then $T_{S_-^*}[z, w]$ ; 2 $x \xleftarrow{\$} \{0, 1\}^n$ ; $y \xleftarrow{\$} \{0, 1\}^c \setminus T_I[x]$ ; 3 $\text{Update}_{S^*}(x, y, z, w)$ ; 4 <b>return</b> $x    y$ ; 
--	--

**Fig. 17.** Game S7

that  $z^* = \mathcal{RO}_n(M')$  in the step 05 of  $\mathcal{O}_+$ . Thus to use  $z^*$  does not affect the distinguisher's view. In Game S5, the outputs of these oracles are random values and for a repeated query the value, which was responded, is returned due to the step 01, that is, the steps 02-14 of  $\mathcal{O}_+$  and the steps 2-4 of  $\mathcal{O}_-$  are not executed. So there is no repeated query to  $\mathcal{RO}_c^{(1)}$ ,  $\mathcal{RO}_n^1$ ,  $\mathcal{P}_1$ , and  $\mathcal{P}_1^{-1}$ . Note that if no collision for the outputs of  $\mathcal{O}_+$  and the outputs of  $\mathcal{O}_-$  occurs, then the table  $T_{S_+^*}$  and  $T_{S_-^*}$  are not redefined. Thus if no collision occurs, the modification for removing  $\mathcal{RO}_c^{(1)}$ ,  $\mathcal{RO}_n^1$ ,  $\mathcal{P}$  and  $\mathcal{P}^{-1}$  does not affect the distinguisher's view. We thus have via a birthday analysis that

$$\Pr[GS5] - \Pr[GS6] \leq \frac{q^2}{2^{b+1}}.$$

**Game S7.** In this game the table  $T_F$  (step 10 of  $\mathcal{O}_+$ ) and the table  $T_I$  (step 2 of  $\mathcal{O}_-$ ). Thus if in Game S6  $w$  does not collide with  $T_F[z]$  in  $\mathcal{O}_+$  and  $x$  does not collide with  $T_I[x]$ , then Game S7 is equal to Game S6. The number of elements in  $T_F[z]$  is at most  $3q + 1$  and the number of elements in  $T_I[x]$  is at most  $2q + 1$ . Thus the collision probabilities for  $T_F[z]$  and  $T_I[x]$  are  $q(3q + 1)/2^c$  and  $q(2q + 1)/2^c$ , respectively. We thus have

$$\Pr[GS6] - \Pr[GS7] \leq \frac{q(5q + 2)}{2^c}.$$

```

 $S^*(x, m)$ 
01 if  $T_{S^*}[x, m] \neq \perp$  then return  $T_{S^*}[x, m]$ ;
02 if  $x = IV$  then
03    $z \leftarrow \mathcal{RO}_n(m)$ ;
04    $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w' || z \in C \cup \{x\}\}$ ;
05    $Path[w || z] \leftarrow m$ ;
06 else if  $Path[x] = M \neq \perp$  then
07    $z \leftarrow \mathcal{RO}_n(M || m)$ ;
08    $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w' || z \in C \cup \{x\}\}$ ;
09    $Path[w || z] \leftarrow M || m$ ;
10 else
11    $z \xleftarrow{\$} \{0, 1\}^n$ ;
12    $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w' || z \in C \cup \{x\}\}$ ;
13    $T_{S^*}[x, m] \leftarrow w || z$ ;  $C \xleftarrow{\cup} \{x, z\}$ ;
14 return  $w || z$ ;

```

**Fig. 18.** Simulator  $S^*$

## D Proof of Theorem 3

We prove Theorem 3 by using the strategy shown in Appendix A.

Since the simulator  $S$  does not update the internal state,  $\Pr[G0] - \Pr[G1] = 0$ .

We use the result of the indistinguishable security by Chang and Nandi [15]. They define a simulator  $S^*$  which is shown in Fig. 10 which simulates a compression function  $h$ .  $T_{S^*}$  is (initially everywhere  $\perp$ ) tables which records query-response values of  $S^*$ . For the query  $S^*(x, m)$ , the response  $w || z$  is recorded in  $T_{S^*}[x, y]$ .  $Path$  is a (initially everywhere  $\perp$ ) table which records all paths with the Merkle-Damgård style. If triples  $(IV, m_1, w_1 || z_1), (w_1 || z_1, m_2, w_2 || z_2), (w_2 || z_2, m_3, w_3 || z_3)$  are the query-response values where  $T_{S^*}[w_{j-1} || z_{j-1}, m_j] = w_j || z_j$  ( $j = 1, 2, 3$ ) and  $w_0 || z_0 = IV$ , then  $m_1 || m_2 || m_3$  is recoded in  $Path[w_3 || z_3]$ .  $C$  is a (initially empty) set. They show that the advantage  $p^*$  of the indistinguishable security is bounded by  $((3n + 1)q_h + nq_H)/2^s + (q_H + q_h)/2^{n-1} + (lq_H + q_h)^2/2^{s+n+1}$ .

We evaluate the difference  $\Pr[G1] - \Pr[G2]$  where a distinguisher interacts with  $(\mathcal{RO}_n, S)$  in Game 1 and  $(\mathcal{RO}_n, S^*)$  in Game 2. Since the difference between Game 1 and Game 2 is a simulator, we consider the distinguishing game between  $S$  and  $S^*$ . We evaluate the difference  $\Pr[A_1^S \Rightarrow 1] - \Pr[A_1^{S^*} \Rightarrow 1]$  for any distinguisher  $A_1$  which outputs a bit.

We consider the six games Game C0, Game C1, Game C2, Game C3, Game C4, and Game C5. In each game, the distinguisher interacts with  $\mathcal{O}$  shown in Figs. 19, 20, and 21. Game C0 is equal to Game 1 and Game C5 is equal to Game 2. Let  $GC_j$  be an event that  $A_1$  output 1 in Game  $S_j$ . Thus

$$\begin{aligned} \Pr[G1] - \Pr[G2] &= \Pr[GC0] - \Pr[GC4] \\ &= \sum_{j=0}^4 (\Pr[GCj] - \Pr[GC(j+1)]). \end{aligned}$$

In the following, we evaluate each difference  $\Pr[GCj] - \Pr[GC(j+1)]$ .

**Game C1.** In this game, the procedures of  $\mathcal{RO}_s^{(1)}$ ,  $\mathcal{TO}^{(1)}$ , and  $\mathcal{RO}_{n+s}^1$  are hard-coded in  $\mathcal{O}$ . The modification from Game C0 to Game C1 does not affect the distinguisher's view. Thus  $\Pr[GC0] = \Pr[GC1]$ .

**Game C2.** In this game, a new table  $T_{S^*}$  is used which is initially everywhere  $\perp$ . The table ensures that for a repeated query, the value which was previously returned is returned. In Game C1, from the condition of the step 05, the modification does not affect the distinguisher's view if the following cases don't occurs.

- Case 1: a collision for  $F_1$  occurs.
- Case 2:  $F_1[x_1, m_1] = w_1 || z_1$  is defined and then  $F_1^*[w_1] = M$  is defined.



$\mathcal{O}(x, m)$ where $x = x_1    x_2$ ( $ x_1  = s,  x_2  = n$ ) 01 $M \leftarrow \mathcal{TO}^{(1)}(x_1)$ ; 02 if $x = IV$ then 03 $z \leftarrow \mathcal{RO}_n(m)$ ; 04 $w \leftarrow \mathcal{RO}_s^{(1)}(m)$ ; 05 else if $M \neq \perp$ then 06 $z \leftarrow \mathcal{RO}_n(M    m)$ ; 07 $w \leftarrow \mathcal{RO}_s^{(1)}(M    m)$ ; 08 else $w    z \leftarrow \mathcal{RO}_{n+s}^1(x, m)$ ; 09 <b>return</b> $w    z$ ;	$\mathcal{O}(x, m)$ where $x = x_1    x_2$ ( $ x_1  = s,  x_2  = n$ ) 01 if $x = IV$ then 02 $z \leftarrow \mathcal{RO}_n(m)$ ; 03 if $F_1^*[m] = \perp$ then $F_1^*[m] \xleftarrow{\$} \{0, 1\}^s$ ; 04 $w \leftarrow F_1^*[m]$ ; 05 else if $\exists_1 M$ s.t. $F_1^*[M] = x_1$ then 06 $z \leftarrow \mathcal{RO}_n(M    m)$ ; 07 if $F_1^*[M    m] = \perp$ then $F_1^*[M    m] \xleftarrow{\$} \{0, 1\}^s$ ; 08 $w \leftarrow F_1^*[M    m]$ ; 09 else 10 if $F_1[x, m] = \perp$ then $F_1[x, m] \xleftarrow{\$} \{0, 1\}^{s+n}$ ; 11 $w    z \leftarrow F_1[x, m]$ ; 12 $T_{S^*}[x, m] \leftarrow w    z$ ; 13 <b>return</b> $w    z$ ;
--	--

**Fig. 19.** Game C0 (left) and Game C1 (right)

$\mathcal{O}(x, m)$ where $x = x_1    x_2$ ( $ x_1  = s,  x_2  = n$ ) 01 if $T_{S^*}[x, m] \neq \perp$ then <b>return</b> $T_{S^*}[x, m]$ ; 02 if $x = IV$ then 03 $z \leftarrow \mathcal{RO}_n(m)$ ; 04 if $F_1^*[m] = \perp$ then $F_1^*[m] \xleftarrow{\$} \{0, 1\}^s$ ; 05 $w \leftarrow F_1^*[m]$ ; 06 else if $\exists_1 M$ s.t. $F_1^*[M] = x_1$ then 07 $z \leftarrow \mathcal{RO}_n(M    m)$ ; 08 if $F_1^*[M    m] = \perp$ then $F_1^*[M    m] \xleftarrow{\$} \{0, 1\}^s$ ; 09 $w \leftarrow F_1^*[M    m]$ ; 10 else 11 if $F_1[x, m] = \perp$ then $F_1[x, m] \xleftarrow{\$} \{0, 1\}^{s+n}$ ; 12 $w    z \leftarrow F_1[x, m]$ ; 13 $T_{S^*}[x, m] \leftarrow w    z$ ; 14 <b>return</b> $w    z$ ;	$\mathcal{O}(x, m)$ 01 if $T_{S^*}[x, m] \neq \perp$ then <b>return</b> $T_{S^*}[x, m]$ ; 02 if $x = IV$ then 03 $z \leftarrow \mathcal{RO}_n(m)$ ; 04 if $F_1^*[m] = \perp$ then $F_1^*[m] \xleftarrow{\$} \{0, 1\}^s$ ; 05 $w \leftarrow F_1^*[m]$ ; 06 $Path[w    z] \leftarrow m$ ; 07 else if $Path[x] = M \neq \perp$ then 08 $z \leftarrow \mathcal{RO}_n(M    m)$ ; 09 if $F_1^*[M    m] = \perp$ then $F_1^*[M    m] \xleftarrow{\$} \{0, 1\}^s$ ; 10 $w \leftarrow F_1^*[M    m]$ ; 11 $Path[w    z] \leftarrow M    m$ ; 12 else 13 if $F_1[x, m] = \perp$ then $F_1[x, m] \xleftarrow{\$} \{0, 1\}^{s+n}$ ; 14 $w    z \leftarrow F_1[x, m]$ ; 15 $T_{S^*}[x, m] \leftarrow w    z$ ; 16 <b>return</b> $w    z$ ;
---	---

**Fig. 20.** Game C2 (left) and Game C3 (right)

The probability that Case 1 occurs is bounded by  $q_h^2/2^{s+1}$  from a birthday analysis. The probability that Case 2 occurs is bounded by  $q_h^2/2^s$  since the number of queries to  $S^*$  is at most  $q_h$ . Thus

$$\Pr[GC1] - \Pr[GC2] \leq \frac{3q_h^2}{2^{s+1}}$$

**Game C3.** In this game, a new table  $Path$  is used which is initially everywhere  $\perp$  and recodes paths with Merkle-Damgård style. In the step 07  $Path$  is used in this game, while  $F_1^*$  is used in Game C2. Note that in Game C3 if  $Path[x] = M$  and no collision occurs for  $F_1^*$  then  $F_1^*[M] = x_1$  where  $x = x_1 || x_2$  and  $|x_1| = s$ . Thus if no collision occurs for  $F_1^*$  in Game C3 then this modification does not affect the distinguisher's view. We thus have via a birthday analysis that

$$\Pr[GC2] - \Pr[GC3] \leq \frac{q_h^2}{2^{s+1}}.$$

**Game C4.** In this game, tables  $F_1$  and  $F_1^*$  are removed. Due to the table  $T_{S^*}$ , for a repeated query, the steps 02-12 are not executed and the value which was previously returned is returned, that is, these tables are not used. Thus this modification does not affect the distinguisher's view and  $\Pr[GC3] = \Pr[GC4]$ .

$\mathcal{O}(x, m)$	$\mathcal{O}(x, m)$
01 if $T_{S^*}[x, m] \neq \perp$ then <b>return</b> $T_{S^*}[x, m]$ ;	01 if $T_{S^*}[x, m] \neq \perp$ then <b>return</b> $T_{S^*}[x, m]$ ;
02 if $x = IV$ then	02 if $x = IV$ then
03 $z \leftarrow \mathcal{RO}_n(m)$ ;	03 $z \leftarrow \mathcal{RO}_n(m)$ ;
04 $w \xleftarrow{\$} \{0, 1\}^s$ ;	04 $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w'    z \in C \cup \{x\}\}$ ;
05 $Path[w  z] \leftarrow m$ ;	05 $Path[w  z] \leftarrow m$ ;
06 else if $Path[x] = M \neq \perp$ then	06 else if $Path[x] = M \neq \perp$ then
07 $z \leftarrow \mathcal{RO}_n(M  m)$ ;	07 $z \leftarrow \mathcal{RO}_n(M  m)$ ;
08 $w \xleftarrow{\$} \{0, 1\}^s$ ;	08 $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w'    z \in C \cup \{x\}\}$ ;
09 $Path[w  z] \leftarrow M  m$ ;	09 $Path[w  z] \leftarrow M  m$ ;
10 else $w  z \xleftarrow{\$} \{0, 1\}^{s+n}$ ;	10 else
11 $T_{S^*}[x, m] \leftarrow w  z$ ;	11 $z \xleftarrow{\$} \{0, 1\}^n$ ;
12 <b>return</b> $w  z$ ;	12 $w \xleftarrow{\$} \{0, 1\}^s \setminus \{w' : w'    z \in C \cup \{x\}\}$ ;
	13 $T_{S^*}[x, m] \leftarrow w  z$ ; $C \leftarrow \bigcup \{x, z\}$ ;
	14 <b>return</b> $w  z$ ;

**Fig. 21.** Game C4 (left) and Game C5 (right)

**Game C5.** In this game, for a query  $\mathcal{O}(x, m)$ ,  $w$  is randomly chosen from  $\{0, 1\}^n \setminus \{w' : w' \in C \cup \{x\}\}$ , while in Game C4 it is randomly chosen from  $\{0, 1\}^n$ . Thus if in Game C4  $w$  does not collide with one of  $\{w' : w' \in C \cup \{x\}\}$  then this modification does not affect the distinguisher's view. The number of elements in  $\{w' : w' \in C \cup \{x\}\}$  is at most  $q_h + 1$ . We thus have that

$$\Pr[GC4] - \Pr[GC5] \leq \frac{(q_h + 1)^2}{2^n}.$$

$\underline{S_+^*(k, x)}$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z' \leftarrow \text{pad}_{\text{BLAKE}}(s, M_1) = a  s  m  t$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)}  t^{(3)} = t^{(2)}  t^{(4)}$ then 05 $P \leftarrow \text{FindPath}(z', s, k, t^{(1)}  t^{(3)})$ ; 06 if $P \neq \emptyset$ then 07 let $P = (M, a)$ ; 08 $z \leftarrow \mathcal{R}\mathcal{O}_n(s, M)$ ; $y \xleftarrow{\$} \beta_{z', s}^{-1}(z)$ ; 09 $\text{AddPath}(\beta_{z', s}(y), z', s, k, t^{(1)}  t^{(3)})$ ; 10 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 11 <b>return</b> $T_{S^*}^+[k, x]$	$\underline{\text{FindPath}(h, s, m, t)}$ 01 $P \leftarrow \emptyset$ ; 02 for all $(M, a) \in \text{Path}[h]$ do 03 if $\exists M_1$ s.t. $\text{pad}_{\text{BLAKE}}(s, M_1) = a  s  m  t$ then 04 $P \leftarrow \bigcup (M_1, a  s  m  t)$ ; 05 if $P = \emptyset$ then <b>return</b> $\perp$ ; 06 else <b>return</b> $(M^*, a^*) \xleftarrow{\$} P$ ;  $\underline{S_+(k, x)}$ 01 $z' \leftarrow \text{pad}_{\text{BLAKE}}(s, M) = a  s  k  t^{(1)}  t^{(3)}$ ; 02 $y \leftarrow E_I(k, x)$ ; 03 if $t^{(1)}  t^{(3)} = t^{(2)}  t^{(4)}$ then 04 $a \leftarrow \mathcal{T}\mathcal{O}^{(1)}(z')$ ; 05 if $a \neq \perp$ or $z' = IV$ then 06 if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a  s  k  t^{(1)}  t^{(3)}$ then 07 $z \leftarrow \mathcal{R}\mathcal{O}_n(s, M)$ ; 08 else $z \leftarrow \mathcal{R}\mathcal{O}_n^{(1)}(a  s  k  t^{(1)}  t^{(3)})$ ; 09 $y_1 \leftarrow \mathcal{R}\mathcal{O}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1  y_2$ ; 10 <b>return</b> $y$ ;  $\underline{S_-(k, y)}$ 01 $k^*  x \leftarrow \mathcal{T}\mathcal{O}^{(2)}(y^L)$ ; 02 if $k^*  x \neq \perp$ and $k^* = k$ then <b>return</b> $x$ ; 03 $x \leftarrow D_I(k, y)$ ; 04 <b>return</b> $x$ ;  $\underline{\text{AddPath}(z, h, s, m, t)}$ 01 for all $(M, a) \in \text{Path}[h]$ do 02 $\text{Path}[z] \leftarrow \bigcup (M  m, a  s  m  t)$ ; 
$\underline{S_-^*(k, y)}$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $z \leftarrow \text{pad}_{\text{BLAKE}}(s, M) = a  s  k  t^{(1)}  t^{(3)}$ ; 03 if $t^{(1)}  t^{(3)} = t^{(2)}  t^{(4)}$ then 04 $\text{AddPath}(\beta_{z, s}(y), z, s, k, t^{(1)}  t^{(3)})$ ; 05 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 06 <b>return</b> $T_{S^*}^-[k, y]$ ;  $\underline{\text{AddPath}(z, h, s, m, t)}$ 01 for all $(M, a) \in \text{Path}[h]$ do 02 $\text{Path}[z] \leftarrow \bigcup (M  m, a  s  m  t)$ ; 	

**Fig. 22.**  $S^*$  (left and top of right) and  $S$  (right)

## E Reset Indifferentiability for the BLAKE Hash Function

First define notations used in this subsection.  $[x]_2 = x||x$  is the concatenation of two copies of  $x$ . If  $x$  is of even length, then  $x^L$  and  $x^R$  denote its left and right halves where  $|x^L| = |x^R|$ .

Let the output length of BLAKE be  $n$  bits. Then BLAKE takes as input a salt  $s$  of  $n/2$  bits (chosen by the user), and a message  $M$  of arbitrary length. The evaluation of  $\text{BLAKE}^{\text{BC}_{2n, 2n}}(s, M)$  is done as follows where a block cipher  $\text{BC}_{2n, 2n} = (E, D)$  is used where  $E$  is the encryption function and  $D$  is the decryption function with the key size and the plain text size of  $2n$  bits. Firstly, the message  $M$  is padded into message blocks  $m_1, \dots, m_k$  of  $2n$  bits, where the padding function  $\text{pad}_B$  is defined as  $\text{pad}_B(M) = M||10^{-(|M|-n/2-2) \bmod 2n}1||(|M|)_{n/2}$ . Along with these message blocks, counter blocks  $t_1, \dots, t_k$  of length  $n/4$  bits are generated. This counter keeps track of the number of message bits hashed so far and equals 0 if the  $i$ -th message block contains no message bits. Starting from an initial state value  $z_0 \in \{0, 1\}^n$ , the message blocks  $m_i$  and counter blocks  $t_i$  are compressed iteratively into the state using a compression function  $f : \{0, 1\}^n \times \{0, 1\}^{n/2} \times \{0, 1\}^{2n} \times \{0, 1\}^{n/4} \rightarrow \{0, 1\}^n$ . Here, the second input to  $f$  denotes the salt  $s$ . The outcome of the BLAKE hash function is defined as its final state value  $H(s, M) = z_k$ .  $f$  is defined as Fig. 22. Here  $C \in \{0, 1\}^n$  is a constant.

$$\begin{aligned} & \underline{f(z_{i-1}, s, m_i, cb_i)} \\ & v_i \leftarrow (z_{i-1}||s||[t_i^L]_2||[t_i^R]_2) \oplus (0^n||C); \\ & w_i \leftarrow E(m_i, v_i); \\ & z_i \leftarrow w_i^L \oplus w_i^R \oplus z_{i-1} \oplus [s]_2; \\ & \mathbf{return} \ z_i; \end{aligned}$$

We evaluate the reset indifferentiability security from  $\mathcal{VO}$  for the BLAKE hash function in the ideal cipher model. We define the parameter of  $\mathcal{VO}$  as  $v = 1$ ,  $n_1 = n$ ,  $u = 2$ ,  $t = 1$ ,  $w_1 = n$ ,  $w_2 = n$ ,  $k_1 = 2n$  and  $m_1 = 2n$ . Thus in this case,  $\mathcal{VO}.priv = \mathcal{R}\mathcal{O}_n$  and  $\mathcal{VO}.pub = (\mathcal{R}\mathcal{O}_n, \mathcal{TR}\mathcal{O}_n^{(1)}, \mathcal{TR}\mathcal{O}_n^{(2)}, \text{IC}_{2n, 2n}^{(1)})$ . The following theorem shows that the BLAKE hash function in the ideal cipher model is reset indifferentiable from  $\mathcal{VO}$ .

**Theorem 8.** Let  $\text{IC}_{2n,2n} = (E_I, D_I)$  be an ideal cipher where the length of each elements is of  $2n$  bits. There exists a simulator  $S$  such that for any distinguisher  $\mathcal{A}$ , the following holds,

$$\text{Adv}_{\text{BLAKE}^{\text{IC}_{2n,2n}}, \mathcal{V}_{\mathcal{O}, S}}^{r\text{-indiff}}(\mathcal{A}) \leq 3 \frac{(lq_H + q_E)(lq_H + q_E + 1)}{2^n} + \frac{5q_E^2}{2^{2n+1}} + \frac{q_E^2}{2^{n-1}}.$$

where  $\mathcal{A}$  can make queries to  $\text{BLAKE}^{\text{IC}_{2n,2n}}/\mathcal{RO}_n$  and  $\text{IC}_{2n,2n}/S_{\text{BLAKE}}$  at most  $q_H, q_E$  times, respectively, and  $l$  is a maximum number of blocks of a query to  $\text{BLAKE}^{\text{IC}_{2n,2n}}/\mathcal{RO}_n$ .  $S_{\text{BLAKE}}$  makes at most  $2q_h$  queries and runs in time  $\mathcal{O}(q_h)$ .  $\blacklozenge$

First, we define a padding function  $\text{pad}_{\text{BLAKE}}$  as  $\text{pad}_{\text{BLAKE}}(s, M) = (s||m_1||t_1)||\cdots||s||m_k||t_k)$ . We also define  $\beta_{z,s}$  and  $\beta_{z,s}^{-1}$  as  $\beta_{z,s}(w) = w^L \oplus w^R \oplus z \oplus [s]_2$  for  $w \in \{0, 1\}^{2n}$  and  $\beta_{z,s}^{-1}(z') = \{w \in \{0, 1\}^{2n} | w^L \oplus w^R \oplus z \oplus [s]_2 = z'\}$  for  $z' \in \{0, 1\}^{2n}$ . In the proof of the theorem, we use the result of the indifferentiability security from a RO by Andreeva *et al.* [1] They define a simulator  $S^*$  which can be implemented as Fig. 22.  $S^*$  simulates the ideal cipher  $\text{IC}_{2n,2n}$  so that the relation among  $(\text{BLAKE}^{\text{IC}_{2n,2n}}, \text{IC}_{2n,2n})$  holds among  $(\mathcal{RO}_n, S^*)$ .  $S_+^*$  and  $S_-^*$  simulate the encryption oracle  $E_I$  and the decryption oracle  $D_I$  of  $\text{IC}_{2n,2n}$ , respectively. In this simulator, the function  $\text{FindPath}$  and the procedure  $\text{AddPath}$  are used.

$T_{S_+^*}^+$  and  $T_{S_-^*}^-$  are (initially everywhere  $\perp$ ) tables which record query-response values of  $S^*$ . If the query  $S_+^*(k, x)$  is made, the output  $y$  is recorded in  $T_{S_+^*}^+[k, x]$  and  $x$  is recoded in  $T_{S_+^*}^+[k, y]$ . Similarly, the query-response values for  $S_-^*$  are recoded in these tables.  $\text{Path}$  is a (initially everywhere  $\emptyset$ ) table which records all paths with the BLAKE style. Namely, if  $(k_1, x_1, y_1)$  is recoded in  $T_{S_+^*}^+$  such that  $T_{S_+^*}^+[k_1, x_1] = y_1$ ,  $x_1 = z_0 || s_1 || t_1^L || t_1^L || t_1^R || t_1^R$ , and  $z_1 = \beta_{z_0, s_1}(y_1)$ ,  $(k_1, s_1 || k_1 || t_1)$  is recoded in  $\text{Path}[z_1]$ <sup>5</sup>. Then, for the query  $S_+^*(k_2, x_2)$ , if the query and some query-response pairs of  $S^*$  have the BLAKE structure, the output is defined by  $\mathcal{RO}_n$ . Namely, if  $x_2 = z_1 || s_2 || t_2^L || t_2^L || t_2^R || t_2^R$ ,  $s_1 = s_2$  and there exists  $M$  such that  $\text{pad}_{\text{BLAKE}}(s_2, M) = (s_1 || k_1 || t_1) || (s_2 || k_2 || t_2)$ , then the output  $y_2$  is randomly chosen from  $\beta_{z_1, s_2}^{-1}(\mathcal{RO}_n(s_2, M))$  to ensure the BLAKE consistency.

**The Simulator  $S$ .** We define the simulator  $S$  in Fig. 22.  $\mathcal{TRO}_n^{(1)}$  and  $\mathcal{TRO}_n^{(2)}$  realizes the functionality of recording a path and constructing a new path. For the query  $S_+(k_1, x_1)$  where  $x_1 = IV || s_1 || t_1^{(1)} || t_1^{(1)} || t_1^{(3)} || t_1^{(3)}$  and there does not exist  $M$  such that  $\text{pad}_{\text{BLAKE}}(s_1, M) = s_1 || k_1 || t_1^{(1)} || t_1^{(3)}$ , the simulator makes the queries  $\mathcal{RO}_n^{(1)}(s_1 || k_1 || t_1^{(1)} || t_1^{(3)})$  and  $\mathcal{RO}_n^{(2)}(k_1, x_1)$  where the responses are  $z_1$  and  $y_{1,1}$ , respectively, then  $y_{1,2} = y_{1,1} \oplus z \oplus [s_1]_2 \oplus IV$  and the response  $y_1$  of the query  $S_+(k_1, x_1)$  is defined by  $y_1 = y_{1,1} || y_{1,2}$ . Then, for the query  $S_{\text{BLAKE},+}(k_2, x_2)$  where  $x_2 = z_1 || s_2 || t_2^{(1)} || t_2^{(1)} || t_2^{(3)} || t_2^{(3)}$  and there exists  $M$  such that  $\text{pad}_{\text{BLAKE}}(M) = s_1 || k_1 || t_1^{(1)} || t_1^{(3)} || s_2 || k_2 || t_2^{(1)} || t_2^{(3)}$ , the response  $y_2$  of the query  $S_+(k_2, x_2)$  is defined by  $y_{2,1} || y_{2,2}$  to ensure the BLAKE consistency. The simulator can obtain  $s_1 || k_1 || t_1^{(1)} || t_1^{(3)}$  by the query  $\mathcal{TO}^{(1)}(z_1)$  and thus can make the queries  $\mathcal{RO}_n(s_2, M)$  and  $\mathcal{RO}_n^{(2)}(k_2, x_2)$  where the outputs are  $z_2$  and  $y_{2,1}$ , respectively, and  $y_{2,2} = y_{2,1} \oplus z \oplus [s_2]_2 \oplus z_1$ . Thus the simulator  $S_+$  can make a response with the same procedure to  $S_+^*$ . For the inverse query  $S_-(k_2, y_2)$ , the simulator can obtain  $x_2$  by the query  $\mathcal{TO}^{(2)}(y_2^R)$ . Thus the simulator  $S_-$  can also make a response with the same procedure to  $S_-^*$ . The formal evaluation of the difference  $\Pr[G1] - \Pr[G2]$  is given as follows where  $\Pr[G1] - \Pr[G2] \leq 5q_E^2/2^{2n+1} + q_E^2/2^{n-1}$ . Since the simulator  $S$  does not update the internal state,  $\Pr[G0] = \Pr[G1]$  (in Subsection ??). The indifferentiability bound from  $\mathcal{RO}_n$  in [1] is  $3(lq_H + q_E)(lq_H + q_E + 1)/2^n$ . There results yield the bound of Theorem 8.

*Proof.* We consider ten games, Game B0, Game B1, Game B2, Game B3, Game B4, Game B5, Game B6, Game B7, Game B8, and Game B9, which are shown in Figs. 23, 24, 25, 26, 27, 28, 29, 30, 31, and 32, respectively. In each game, the distinguisher  $\mathcal{A}$  interacts with  $(\mathcal{O}_+, \mathcal{O}_-)$ .  $(\mathcal{O}_+, \mathcal{O}_-)$  in Game B0 is equal to the simulator  $S$  in Game 1, and  $(\mathcal{O}_+, \mathcal{O}_-)$  in Game B7 is equal to the simulator  $S^*$  in Game 2. Notice that in this proof  $\mathcal{RO}_n$  queries are removed, since the difference between Game 1 and Game 2 is just the simulator.

<sup>5</sup> Note that in [1], the paths are recorded by using the graph representation, but the table  $\text{Path}$  realizes the same role as the graph.

$\mathcal{O}_+(k, x)$ 01 $z' \parallel s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C)$ ; 02 $y \leftarrow E_I(k, x)$ ; 03 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 04 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 05     if $a \neq \perp$ or $z' = IV$ then 06         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)}$ then 07 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 08         else $z \leftarrow \mathcal{RO}_n^{(1)}(a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)})$ ; 09 $y_1 \leftarrow \mathcal{RO}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1 \parallel y_2$ ; 10 <b>return</b> $y$ ;	$\mathcal{O}_-(k, y)$ 01 $k^* \parallel x \leftarrow \mathcal{TO}^{(2)}(y^L)$ ; 02 if $k^* \parallel x \neq \perp$ and $k^* = k$ then <b>return</b> $x$ ; 03 $x \leftarrow D_I(k, y)$ ; 04 <b>return</b> $x$ ;
--	--

**Fig. 23.** Game B0

$\mathcal{O}_+(k, x)$ 01 $z' \parallel s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C)$ ; 02 $y \leftarrow E^*(k, x)$ ; 03 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 04 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 05     if $a \neq \perp$ or $z' = IV$ then 06         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)}$ then 07 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 08         else $z \leftarrow \mathcal{RO}_n^{(1)}(a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)})$ ; 09 $y_1 \leftarrow \mathcal{RO}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1 \parallel y_2$ ; 10 <b>return</b> $y$ ;	$\mathcal{O}_-(k, y)$ 01 $k^* \parallel x \leftarrow \mathcal{TO}^{(2)}(y^L)$ ; 02 if $k^* \parallel x \neq \perp$ and $k^* = k$ then <b>return</b> $x$ ; 03 $x \leftarrow D^*(k, y)$ ; 04 <b>return</b> $x$ ;  $E^*(k, x)$ 01 if $E^*[k, x] = \perp$ then $E^*[k, x] \xleftarrow{\$} \{0, 1\}^{2n}$ ; 02 $D^*[k, E^*[k, x]] \leftarrow x$ ; 03 <b>return</b> $E^*[k, x]$ ;  $D^*(k, y)$ 01 if $D^*[k, y] = \perp$ then $D^*[k, y] \xleftarrow{\$} \{0, 1\}^{2n}$ ; 02 $E^*[k, D^*[k, y]] \leftarrow y$ ; 03 <b>return</b> $D^*[k, y]$ ;
--	--

**Fig. 24.** Game B1

Let  $GB_j$  be an event that the distinguisher  $\mathcal{A}$  output 1 in Game B $_j$ . Thus

$$\begin{aligned} \Pr[G1] - \Pr[G2] &= \Pr[GB0] - \Pr[GB9] \\ &= \sum_{j=0}^8 (\Pr[GB_j] - \Pr[GB(j+1)]). \end{aligned}$$

In the following, we evaluate the each difference  $\Pr[GB_j] - \Pr[GB(j+1)]$ .

**Game B1.** In Game B0 the ideal cipher  $(E_I, D_I)$  is used, while in Game B1  $(E^*, D^*)$  is used where an output is randomly chosen from  $\{0, 1\}^{2n}$ .  $E^*$  and  $D^*$  are (initially everywhere  $\perp$ ) tables. We thus have via birthday analysis that

$$\Pr[GB0] - \Pr[GB1] \leq \frac{2q_E^2}{2^{2n+1}}.$$

**Game B2.** In this game, new tables  $T_{S^*}^+$  and  $T_{S^*}^-$  are used which are initially everywhere  $\perp$ . In Game B2, if no collision for the outputs of  $\mathcal{O}_+$  and the output of  $\mathcal{O}_-$  occurs, for a repeated query, the value which was previously returned is returned. In Game B1, the procedure of  $\mathcal{O}_+$  depends on the output of  $\mathcal{TO}^{(1)}$  and the procedure of  $\mathcal{O}_-$  depends on the output of  $\mathcal{TO}^{(2)}$ . Thus in Game B1 if no collision for the outputs of  $\mathcal{RO}_n^{(1)}$  and the output of  $\mathcal{RO}_n^{(2)}$  occurs then for a repeated query, the value which was previously returned is returned. Thus, in both game, if a collision for the outputs of  $\mathcal{RO}_n^{(1)}$ , the output of  $\mathcal{RO}_n^{(2)}$ , the outputs

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z' \leftarrow \mathcal{R} \left( s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C) \right)$ ; 03 $y \leftarrow E^*(k, x)$ ; 04 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 05 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 06     if $a \neq \perp$ or $z' = IV$ then 07         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)}$ then 08 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 09             else $z \leftarrow \mathcal{RO}_n^{(1)}(a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)})$ ; 10 $y_1 \leftarrow \mathcal{RO}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1 \parallel y_2$ ; 11 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 12 <b>return</b> $T_{S^*}^+[k, x]$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $k^* \parallel x^* \leftarrow \mathcal{TO}^{(2)}(y^L)$ ; 03 if $k^* \parallel x^* \neq \perp$ and $k^* = k$ then $x \leftarrow x^*$ ; 04 else $x \leftarrow D^*(k, y)$ ; 05 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 06 <b>return</b> $T_{S^*}^-[k, y]$ ;  $E^*(k, x)$ 01 if $E^*[k, x] = \perp$ then $E^*[k, x] \xleftarrow{\$} \{0, 1\}^{2n}$ ; 02 $D^*[k, E^*[k, x]] \leftarrow x$ ; 03 <b>return</b> $E^*[k, x]$ ;  $D^*(k, y)$ 01 if $D^*[k, y] = \perp$ then $D^*[k, y] \xleftarrow{\$} \{0, 1\}^{2n}$ ; 02 $E^*[k, D^*[k, y]] \leftarrow y$ ; 03 <b>return</b> $D^*[k, y]$ ; 
---	---

Fig. 25. Game B2

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z' \leftarrow \mathcal{R} \left( s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C) \right)$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 05 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 06     if $a \neq \perp$ or $z' = IV$ then 07         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)}$ then 08 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 09             else $z \leftarrow \mathcal{RO}_n^{(1)}(a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)})$ ; 10 $y_1 \leftarrow \mathcal{RO}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1 \parallel y_2$ ; 11 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 12 <b>return</b> $T_{S^*}^+[k, x]$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $k^* \parallel x^* \leftarrow \mathcal{TO}^{(2)}(y^L)$ ; 03 if $k^* \parallel x^* \neq \perp$ and $k^* = k$ then $x \leftarrow x^*$ ; 04 else $x \xleftarrow{\$} \{0, 1\}^{2n}$ ; 05 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 06 <b>return</b> $T_{S^*}^-[k, y]$ ; 
--	--

Fig. 26. Game B3

of  $\mathcal{O}_+$  and the output of  $\mathcal{O}_-$ , the modification for Game B2 does not affect the distinguisher's view and so Game B2 is equal to Game B1. We thus have via a birthday analysis that

$$\Pr[\text{GB1}] - \Pr[\text{GB2}] \leq \frac{2q_E^2}{2^{n+1}} + \frac{2q_E^2}{2^{2n+1}}.$$

**Game B3.** In this game,  $(E^*, D^*)$  is removed. Outputs of  $E^*$  and  $D^*$  are randomly chosen from  $\{0, 1\}^{2n}$ . In Game B2, if no collision occurs for  $\mathcal{O}_+$ ,  $\mathcal{O}_-$ , for a repeated query, the value which was previously returned is returned by the tables  $T_{S^*}^+$  and  $T_{S^*}^-$ . Thus in both games if no collision occurs for the outputs of  $\mathcal{O}_+$  and the outputs of  $\mathcal{O}_-$ , the modification does not affect the distinguisher's view. We thus have via a birthday analysis that

$$\Pr[\text{GB2}] - \Pr[\text{GB3}] \leq \frac{2q_E^2}{2^{2n+1}}.$$

**Game B4.** In this game,  $\mathcal{TO}^{(2)}$  in  $\mathcal{O}_-$  is removed.  $k^* \parallel x^* (= \mathcal{TO}(y^L)) \neq \perp$  means that the value corresponding with the query  $(k, y)$  is recoded. If no collision occurs for the output of  $\mathcal{O}_+$  and the output of  $\mathcal{O}_-$ , for a repeated query, the value which was previously returned is returned. That is, if no collision occurs,  $\mathcal{TO}^{(2)}$  is

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z'    s    t^{(1)}    t^{(2)}    t^{(3)}    t^{(4)} \leftarrow x \oplus (0^n    C)$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)}    t^{(3)} = t^{(2)}    t^{(4)}$ then 05 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 06     if $a \neq \perp$ or $z' = IV$ then 07         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a    s    k    t^{(1)}    t^{(3)}$ then 08 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 09         else $z \leftarrow \mathcal{RO}_n^{(1)}(a    s    k    t^{(1)}    t^{(3)})$ ; 10 $y_1 \leftarrow \mathcal{RO}_n^{(2)}(k, x)$ ; $y_2 \leftarrow y_1 \oplus z' \oplus [s]_2 \oplus z$ ; $y \leftarrow y_1    y_2$ ; 11 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 12 <b>return</b> $T_{S^*}^+[k, x]$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $x \xleftarrow{\$} \{0, 1\}^{2n}$ ; 03 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 04 <b>return</b> $T_{S^*}^-[k, y]$ ; 
---	--

Fig. 27. Game B4

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z'    s    t^{(1)}    t^{(2)}    t^{(3)}    t^{(4)} \leftarrow x \oplus (0^n    C)$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)}    t^{(3)} = t^{(2)}    t^{(4)}$ then 05 $a \leftarrow \mathcal{TO}^{(1)}(z')$ ; 06     if $a \neq \perp$ or $z' = IV$ then 07         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a    s    k    t^{(1)}    t^{(3)}$ then 08 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 09         else $z \leftarrow \mathcal{RO}_n^{(1)}(a    s    k    t^{(1)}    t^{(3)})$ ; 10 $y \xleftarrow{\$} \beta_{z', s}^{-1}(z)$ ; 11 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 12 <b>return</b> $T_{S^*}^+[k, x]$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $x \xleftarrow{\$} \{0, 1\}^{2n}$ ; 03 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 04 <b>return</b> $T_{S^*}^-[k, y]$ ; 
--	--

Fig. 28. Game B5

not used and thus Game B3 is equal to Game B2. We thus have via a birthday analysis that

$$\Pr[GB3] - \Pr[GB4] \leq \frac{2q_E^2}{2^{2n+1}}.$$

**Game B5.** In this game,  $\mathcal{RO}_n^{(2)}$  is removed. In both Game B4 and Game B5,  $y$  is randomly chosen from  $\{0, 1\}^{2n}$  with a relation that  $\beta_{z', s}(y) = z$ . Thus Game B5 is equal to Game B4 and  $\Pr[GB4] = \Pr[GB5]$ .

**Game B6.** In this game,  $\mathcal{TR}\mathcal{O}_n^{(1)}$  is removed. Instead, the functions  $FindPath_1$  and  $AddPath_1$  are used.  $Path$  is a (initially everywhere  $\perp$ ) table. If no collision occurs for the outputs of  $AddPath_1$ , then  $AddPath_1$  and  $FindPath_1$  behave as  $\mathcal{RO}_n^{(1)}$  and  $\mathcal{TO}^{(1)}$ , respectively. That is, if no collision occurs, Game B6 is equal to Game B5. We thus have via a birthday analysis that

$$\Pr[GB5] - \Pr[GB6] \leq \frac{q_E^2}{2^{n+1}}.$$

**Game B7.** In this game,  $AddPath$  and  $FindPath$  are used instead of  $AddPath_1$  and  $FindPath_1$ . For some value  $z$ , in  $AddPath_1$ , the number of paths in  $Path_1[z]$  is at most 1, while in  $AddPath$ , the number of paths in  $Path[z]$  not limited. Thus, if for any value  $z$  the number of paths in  $Path[z]$  is at most 1, Game B7 is equal to Game B6. That is, if no collision for  $\beta_{z', s}$  (step 07 in  $\mathcal{O}_+$ ) occurs then Game B7 is equal to Game B6. Since  $y$  is randomly chosen from  $\{0, 1\}^{2n}$ , an output of  $\beta_{z', s}$  is a random value of  $n$  bits. We thus via

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z' \leftarrow \{s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C)$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 05 $a \leftarrow \text{FindPath}_1(z')$ ; 06     if $a \neq \perp$ or $z' = IV$ then 07         if $\exists M$ s.t. $\text{pad}_{\text{BLAKE}}(s, M) = a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)}$ then 08 $z \leftarrow \mathcal{RO}_n(s, M)$ ; 09             else $z \leftarrow \text{AddPath}_1(a \parallel s \parallel k \parallel t^{(1)} \parallel t^{(3)})$ ; 10 $y \xleftarrow{\$} \beta_{z', s}^{-1}(z)$ ; 11 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 12 <b>return</b> $T_{S^*}^+[k, x]$ ;  $\text{AddPath}_1(M)$ 01 if $\exists z$ s.t. $\text{Path}_1[z] = M$ then <b>return</b> $z$ ; 02 $z \xleftarrow{\$} \{0, 1\}^n$ ; 03 $\text{Path}_1[z] \leftarrow M$ ; 04 <b>return</b> $z$ ;  $\text{FindPath}_1(z)$ 01 if $\text{Path}_1[z] \neq \perp$ then <b>return</b> $\text{Path}[z]$ ; 02 <b>return</b> $\perp$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $x \xleftarrow{\$} \{0, 1\}^{2n}$ ; 03 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 04 <b>return</b> $T_{S^*}^-[k, y]$ ;  $\text{AddPath}_1(M)$ 01 if $\exists z$ s.t. $\text{Path}_1[z] = M$ then <b>return</b> $z$ ; 02 $z \xleftarrow{\$} \{0, 1\}^n$ ; 03 $\text{Path}_1[z] \leftarrow M$ ; 04 <b>return</b> $z$ ;  $\text{FindPath}_1(z)$ 01 if $\text{Path}_1[z] \neq \perp$ then <b>return</b> $\text{Path}[z]$ ; 02 <b>return</b> $\perp$ ; 
--	--

**Fig. 29.** Game B6

$\mathcal{O}_+(k, x)$ 01 if $T_{S^*}^+[k, x] \neq \perp$ then <b>return</b> $T_{S^*}^+[k, x]$ ; 02 $z' \leftarrow \{s \parallel t^{(1)} \parallel t^{(2)} \parallel t^{(3)} \parallel t^{(4)} \leftarrow x \oplus (0^n \parallel C)$ ; 03 $y \xleftarrow{\$} \{0, 1\}^{2n}$ ; 04 if $t^{(1)} \parallel t^{(3)} = t^{(2)} \parallel t^{(4)}$ then 05 $P \leftarrow \text{FindPath}(z', s, k, t)$ ; 06     if $P \neq \perp$ then let $P = (M, a)$ ; $z \leftarrow \mathcal{RO}_n(s, M)$ ; 07     else $\text{AddPath}(\beta_{z', s}(y), z', s, k, t^{(1)} \parallel t^{(3)})$ ; 08 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 09 <b>return</b> $T_{S^*}^+[k, x]$ ;  $\text{AddPath}(z, h, s, m, t)$ 01 for all $(M, a) \in \text{Path}[h]$ do 02 $\text{Path}[z] \xleftarrow{\cup} (M \parallel m, a \parallel s \parallel m \parallel t)$ ; 	$\mathcal{O}_-(k, y)$ 01 if $T_{S^*}^-[k, y] \neq \perp$ then <b>return</b> $T_{S^*}^-[k, y]$ ; 02 $x \xleftarrow{\$} \{0, 1\}^{2n}$ ; 03 $T_{S^*}^+[k, x] \leftarrow y$ ; $T_{S^*}^-[k, y] \leftarrow x$ ; 04 <b>return</b> $T_{S^*}^-[k, y]$ ;  $\text{FindPath}(h, s, m, t)$ 01 $P \leftarrow \emptyset$ ; 02 for all $(M, a) \in \text{Path}[h]$ do 03     if $\exists M_1$ s.t. $\text{pad}_{\text{BLAKE}}(s, M_1) = a \parallel s \parallel m \parallel t$ then 04 $P \xleftarrow{\cup} (M_1, a \parallel s \parallel m \parallel t)$ ; 05 if $P = \emptyset$ then <b>return</b> $\perp$ ; 06 else <b>return</b> $(M^*, a^*) \xleftarrow{\$} P$ ; 
---	---

**Fig. 30.** Game B7

birthday analysis that

$$\Pr[\text{GB6}] - \Pr[\text{GB7}] \leq \frac{q_E^2}{2^{n+1}}.$$

**Game B8.** In Game B8, “else” for the step using *AddPath* is removed. Since  $\text{pad}_{\text{BLAKE}}$  is a prefix-free padding, the path constructed from the value defined the steps 06-08 is not used. Thus the modification does not affect the distinguisher’s view. So we have that  $\Pr[\text{GB7}] = \Pr[\text{GB8}]$ .

**Game B9.** In this game, *AddPath* is added in  $\mathcal{O}_-$ . Since  $x$  is randomly chosen from  $\{0, 1\}^{2n}$ , the probability that in  $\mathcal{O}_-$  a new path is added in the table *Path* is at most  $q_E^2/2^n$  where the number of paths stored in *Path* is at most  $q_E$ . We thus have that

$$\Pr[\text{GB8}] - \Pr[\text{GB9}] \leq \frac{q_E^2}{2^n}.$$

□



$\mathcal{O}_B^+(k, x)$ <pre> 01 if <math>T_{S^*}^+[k, x] \neq \perp</math> then <b>return</b> <math>T_{S^*}^+[k, x]</math>; 02 <math>z' \leftarrow \{0, 1\}^n</math>; <math>t^{(1)} \leftarrow x \oplus (0^n \  C)</math>; 03 <math>y \xleftarrow{\\$} \{0, 1\}^{2n}</math>; 04 if <math>t^{(1)} \  t^{(3)} = t^{(2)} \  t^{(4)}</math> then 05   <math>P \leftarrow \text{FindPath}(z', s, k, t^{(1)} \  t^{(3)})</math>; 06   if <math>P \neq \emptyset</math> then 07     let <math>P = (M, a)</math>; 08     <math>z \leftarrow \mathcal{RO}_n(s, M)</math>; <math>y \xleftarrow{\\$} \beta_{z', s}^{-1}(z)</math>; 09   <math>\text{AddPath}(\beta_{z', s}(y), z', s, k, t^{(1)} \  t^{(3)})</math>; 10 <math>T_{S^*}^+[k, x] \leftarrow y</math>; <math>T_{S^*}^-[k, y] \leftarrow x</math>; 11 <b>return</b> <math>T_{S^*}^+[k, x]</math>; </pre> $\text{AddPath}(z, h, s, m, t)$ <pre> 01 for all <math>(M, a) \in \text{Path}[h]</math> do 02   <math>\text{Path}[z] \leftarrow \cup (M \  m, a \  s \  m \  t)</math>; </pre>	$\mathcal{O}_B^-(k, y)$ <pre> 01 if <math>T_{S^*}^-[k, y] \neq \perp</math> then <b>return</b> <math>T_{S^*}^-[k, y]</math>; 02 <math>x \xleftarrow{\\$} \{0, 1\}^{2n}</math>; 03 <math>T_{S^*}^+[k, x] \leftarrow y</math>; <math>T_{S^*}^-[k, y] \leftarrow x</math>; 04 <b>return</b> <math>T_{S^*}^-[k, y]</math>; </pre> $\text{FindPath}(h, s, m, t)$ <pre> 01 <math>P \leftarrow \emptyset</math>; 02 for all <math>(M, a) \in \text{Path}[h]</math> do 03   if <math>\exists M_1</math> s.t. <math>\text{pad}_{\text{BLAKE}}(s, M_1) = a \  s \  m \  t</math> then 04     <math>P \leftarrow \cup (M_1, a \  s \  m \  t)</math>; 05 if <math>P = \emptyset</math> then <b>return</b> <math>\perp</math>; 06 else <b>return</b> <math>(M^*, a^*) \xleftarrow{\\$} P</math>; </pre>
--	---

Fig. 31. Game B8

$\mathcal{O}_+(k, x)$ <pre> 01 if <math>T_{S^*}^+[k, x] \neq \perp</math> then <b>return</b> <math>T_{S^*}^+[k, x]</math>; 02 <math>z' \leftarrow \{0, 1\}^n</math>; <math>t^{(1)} \leftarrow x \oplus (0^n \  C)</math>; 03 <math>y \xleftarrow{\\$} \{0, 1\}^{2n}</math>; 04 if <math>t^{(1)} \  t^{(3)} = t^{(2)} \  t^{(4)}</math> then 05   <math>P \leftarrow \text{FindPath}(z', s, k, t^{(1)} \  t^{(3)})</math>; 06   if <math>P \neq \emptyset</math> then 07     let <math>P = (M, a)</math>; 08     <math>z \leftarrow \mathcal{RO}_n(s, M)</math>; <math>y \xleftarrow{\\$} \beta_{z', s}^{-1}(z)</math>; 09   <math>\text{AddPath}(\beta_{z', s}(y), z', s, k, t^{(1)} \  t^{(3)})</math>; 10 <math>T_{S^*}^+[k, x] \leftarrow y</math>; <math>T_{S^*}^-[k, y] \leftarrow x</math>; 11 <b>return</b> <math>T_{S^*}^+[k, x]</math>; </pre> $\text{AddPath}(z, h, s, m, t)$ <pre> 01 for all <math>(M, a) \in \text{Path}[h]</math> do 02   <math>\text{Path}[z] \leftarrow \cup (M \  m, a \  s \  m \  t)</math>; </pre>	$\mathcal{O}_-(k, y)$ <pre> 01 if <math>T_{S^*}^-[k, y] \neq \perp</math> then <b>return</b> <math>T_{S^*}^-[k, y]</math>; 02 <math>z \leftarrow \{0, 1\}^n</math>; <math>t^{(1)} \leftarrow x \oplus (0^n \  C)</math>; 03 if <math>t^{(1)} \  t^{(3)} = t^{(2)} \  t^{(4)}</math> then 04   <math>\text{AddPath}(\beta_{z, s}(y), z, s, k, t^{(1)} \  t^{(3)})</math>; 05 <math>T_{S^*}^+[k, x] \leftarrow y</math>; <math>T_{S^*}^-[k, y] \leftarrow x</math>; 06 <b>return</b> <math>T_{S^*}^-[k, y]</math>; </pre> $\text{FindPath}(h, s, m, t)$ <pre> 01 <math>P \leftarrow \emptyset</math>; 02 for all <math>(M, a) \in \text{Path}[h]</math> do 03   if <math>\exists M_1</math> s.t. <math>\text{pad}_{\text{BLAKE}}(s, M_1) = a \  s \  m \  t</math> then 04     <math>P \leftarrow \cup (M_1, a \  s \  m \  t)</math>; 05 if <math>P = \emptyset</math> then <b>return</b> <math>\perp</math>; 06 else <b>return</b> <math>(M^*, a^*) \xleftarrow{\\$} P</math>; </pre>
--	---

Fig. 32. Game B9

## F Proof of Theorem 4

We show the following lemma.

**Lemma 5.** *For any CDA1 adversary  $A_1, A_2$ , making  $\mathcal{RO}_n$  queries at most  $q$  times, of a PKE scheme  $\mathcal{AE}$  where the length of the randomness  $\mathbf{r}$  is 0, there exists a PRIV adversary  $B_1, B_2$  of the PKE scheme such that*

$$\text{Adv}_{\mathcal{AE}, \mathcal{RO}_n}^{\text{cda1}}(A_1, A_2) \leq \text{Adv}_{\mathcal{AE}, \mathcal{RO}_n}^{\text{priv}}(B_1, B_2).$$

$A_1, A_2$  can make  $\mathcal{RO}_n$  queries at most  $q$  times. The running time of  $B_1, B_2$  is at most that of  $A_1, A_2$ .  $\blacklozenge$

*Proof.* We construct the PRIV adversary  $B_1, B_2$  by using the CDA1 adversary  $A_1, A_2$ . The PRIV adversary is shown in Fig. 33. The adversary  $B_1$  outputs two values, the  $B_1$ 's output and the  $A_1$ 's output.  $B_1$  uses only  $s$  which one element of the output of  $A_1$ .  $B_1$  defines messages of  $A_1$  such that  $\mathbf{m}_0$  and  $\mathbf{m}_1$  are bit strings of length  $\omega$  and  $\mathbf{m}_b[i] \neq \mathbf{m}_b[j]$  for all  $1 \leq i < j \leq \nu$  and all  $b \in \{0, 1\}$  such that the source has mini-entropy  $\mu$ .

<u>Adversary <math>B_1</math></u> 1 $((\mathbf{m}_0^*, \mathbf{m}_1^*), s) \leftarrow A_1^{\mathcal{R}O_n}$ 2 generates $(\mathbf{m}_0, \mathbf{m}_1)$ where the $bit_s(\mathbf{m}_{b^*}) = b^*$ for $b^* = 0, 1$ . 3 outputs $(\mathbf{m}_0, \mathbf{m}_1)$ as the $B_1$ 's output.	<u>Adversary <math>B_2</math></u> 1 obtains the cipher text $\mathbf{c}$ 2 $b' \leftarrow A_2^{\mathcal{R}O_n}(\mathbf{c})$ 3 <b>return</b> $b'$
---	---

**Fig. 33.** PRIV Adversary

$A_1$  and  $A_2$  does not share the state and the second adversary  $A_2$  obtains just the cipher text  $\mathbf{c}$  whose the plain text has mini-entropy  $\mu$ . Thus  $A_2$  does not find that the plain text is defined by  $B_1$ . The adversary PRIV  $B_1, B_2$  wins if the CDA1 adversary wins.  $\square$

## G Proof of Theorem 5

**Lemma 6.** For any CDA2 adversary  $A_1, A_2$  of REwH in the  $\mathcal{RO}_n$  model, there exists a CDA adversary  $B_1, B_2$  in the  $\mathcal{RO}_n$  model such that

$$\text{Adv}_{\text{REwH}, \mathcal{RO}_n}^{\text{cda2}}(A_1, A_2) \leq \text{Adv}_{\text{REwH}, \mathcal{RO}_n}^{\text{cda}}(B_1, B_2).$$

where the running time of  $B_1, B_2$  is at most that of  $A_1, A_2$ .  $\blacklozenge$

*Proof.* We consider the following events.

- Event 1:  $A_1$  outputs  $((\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}), i)$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is some bit of  $\mathbf{r}$ .
- Event 2:  $A_1$  outputs  $((\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}), i)$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is some bit of  $\mathbf{m}_b$ .

Let CDA2 be the event that true is returned in the CDA2 security game. Thus we have the following.

$$\begin{aligned} \Pr[\text{CDA2}_{\text{REwH}, \mathcal{RO}_n}^{A_1, A_2} \Rightarrow \text{true}] &= \Pr[\text{CDA2}] \\ &\leq \Pr[\text{GDA2}|\text{Event 1}] \Pr[\text{Event 1}] + \Pr[\text{GDA2}|\text{Event 2}] \Pr[\text{Event 2}] \\ &= \Pr[\text{GDA2}|\text{Event 1}] \times p + \Pr[\text{GDA2}|\text{Event 2}] \times (1 - p) \end{aligned}$$

where  $p = \Pr[\text{Event 1}]$ .

We evaluate the probability  $\Pr[\text{CDA2}|\text{Event 1}]$ . In the CDA2 security game,  $A_2$  obtains the cipher text  $\mathbf{c}$  where each component is  $\mathcal{E}_r(pk, \mathbf{m}_b[t]; \mathcal{RO}_n(pk || \mathbf{m}_b[t] || \mathbf{r}[t]))$ . Since  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is a random bit and the bit is hidden by  $\mathcal{RO}_n$ ,  $\Pr[\text{CDA2}|\text{Event 1}] = 1/2$ .

We evaluate the probability  $\Pr[\text{CDA2}|\text{Event 2}]$ . Let CDA1 be the event that the CDA1 adversary  $A_1^*, A_2^*$  wins the CDA1 security game. Let Event 2' be the event that in the CDA1 security game  $A_2^*$  outputs  $((\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}), i)$  such that  $\text{bit}_i(\mathbf{m}_b, \mathbf{r})$  is a bit of  $\mathbf{m}_b$ . From Lemma 1, for any CDA2 adversary  $A_1, A_2$  there exists a CDA1 adversary  $A_1^*, A_2^*$  such that

$$\Pr[\text{CDA2}|\text{Event 2}] \leq \Pr[\text{CDA1}|\text{Event 2}']$$

Under Event 2', we can construct a CDA adversary from the CDA1 adversary by using the same proof in Appendix F. Thus, for any CDA1 adversary  $A_1^*, A_2^*$ , there exists a CDA adversary  $B_1, B_2$  such that

$$\Pr[\text{CDA1}|\text{Event 2}'] \leq \Pr[\text{CDA}_{\text{REwH}, \mathcal{RO}_n}^{B_1, B_2} \Rightarrow \text{true}]$$

From above discussion, for any CDA2 adversary  $A_1, A_2$  there exists CDA adversary  $B_1, B_2$  such that

$$\begin{aligned} \Pr[\text{CDA2}_{\text{REwH}, \mathcal{RO}_n}^{A_1, A_2} \Rightarrow \text{true}] &\leq \frac{1}{2} \times p + \Pr[\text{CDA}_{\text{REwH}, \mathcal{RO}_n}^{B_1, B_2} \Rightarrow \text{true}] \times (1 - p) \\ &\leq \Pr[\text{CDA}_{\text{REwH}, \mathcal{RO}_n}^{B_1, B_2} \Rightarrow \text{true}]. \end{aligned}$$

□

Adversary $B_1$	Adversary $B_2$
1 $((\mathbf{m}_0^*, \mathbf{m}_1^*, \mathbf{r}), s) \leftarrow A_1^{\mathcal{RC}_n}$	1 obtains the cipher text $\mathbf{c}$
2 generates $((\mathbf{m}_0, \mathbf{r}_0), (\mathbf{m}_1, \mathbf{r}_1))$ such that $\text{bits}_s(\mathbf{m}_{b^*}, \mathbf{r}_{b^*}) = b^*$ for $b^* = 0, 1$ .	2 $b' \leftarrow A_2^{\mathcal{RC}_n}(\mathbf{c})$
3 outputs $((\mathbf{m}_0, \mathbf{r}_0), (\mathbf{m}_1, \mathbf{r}_1))$ as the $B_1$ 's output.	3 <b>return</b> $b'$

**Fig. 34.** PRIV Adversary

## H Proof of Theorem 6

**Lemma 7.** *For any CDA1 adversary  $A_1, A_2$  of PtD in the  $\mathcal{RC}_n$  model, there exists a CDA adversary  $B_1, B_2$  in the  $\mathcal{RC}_n$  model such that*

$$\text{Adv}_{\text{PtD}, \mathcal{RC}_n}^{\text{cda1}}(A_1, A_2) \leq \text{Adv}_{\mathcal{AE}_d, \mathcal{RC}_n}^{\text{priv}}(B_1, B_2).$$

where the running time of  $B_1, B_2$  is at most that of  $A_1, A_2$ .  $\blacklozenge$

*Proof.* We construct the PRIV adversary  $B_1, B_2$  by using the CDA1 adversary  $A_1, A_2$ . The PRIV adversary is shown in Fig. 34.  $B_1$  uses only  $s$  which one element of the output of  $A_1$ .  $B_1$  defines messages of  $A_1$  such that  $\mathbf{m}_0$  and  $\mathbf{m}_1$  are bit strings of length  $\omega$ , all components of  $\mathbf{r}_0, \mathbf{r}_1$  are bit strings of length  $\rho$ , and  $(\mathbf{m}_b[i], \mathbf{r}_b[i]) \neq (\mathbf{m}_b[j], \mathbf{r}_b[j])$  for all  $1 \leq i < j \leq \nu$  and all  $b \in \{0, 1\}$  such that the source has mini-entropy  $\mu$ .  $A_1$  and  $A_2$  does not share the state and the second adversary  $A_2$  obtains just the cipher text  $\mathbf{c}$  whose the plain text has mini-entropy  $\mu$ . Thus  $A_2$  cannot find that the plain text is defined by  $B_1$ . If the CDA1 adversary wins then the PRIV adversary  $B_1, B_2$  wins.  $\square$