Adaptive Preimage Resistance Analysis Revisited: Requirements, Subtleties and Implications

Donghoon Chang[1] and Moti Yung[2]

[1] The Computer Security Division, National Institute of Standards and Technology, USA
pointchang@gmail.com
[2] Google Inc. and Department of Computer Science, Columbia University, USA
my123@columbia.edu

Abstract. In the last few years, the need to design new cryptographic hash functions has led to the intense study of when desired hash multi-properties are preserved or assured under compositions and domain extensions. In this area, it is important to identify the exact notions and provide often complex proofs of the resulting properties. Getting this analysis right (as part of provable security studies) is, in fact, analogous to cryptanalysis. We note that it is important and quite subtle to get indeed the "right" notions and properties, and "right" proofs in this relatively young area. Specifically, the security notion we deal with is "adaptive preimage resistance" (apr) which was introduced by Lee and Park as an extension of "preimage resistance" (pr). In Eurocrypt 2010, in turn, Lee and Steinberger already used the apr security notion to prove "preimage awareness" and "indifferentiable security" of their new double-piped mode of operation. They claimed that if H^P is collision-resistant (cr) and apr, then $F(M) = \mathcal{R}(H^P(M))$ is indifferentiable from a variable output length (VIL) random oracle $\mathcal{F}$, where H^P is a function based on an ideal primitive P and $\mathcal{R}$ is a fixed input length (FIL) random oracle. However, there are some limitations in their claim, because they considered only indifferentiability security notion in the information-theoretic adversarial model, not in the computation-theoretic adversarial model. As we show in the current work, the above statement is *not* correct in the computation-theoretic adversarial model. First in our studies, we give a counterexample to the above. Secondly, we describe *a new requirement* on H^P (called "admissibility") so that the above statement is correct even in the computation-theoretic adversarial model. Thirdly, we show that apr is, in fact, not a strengthened notion of preimage resistance. Fourthly, we explain the relation between preimage awareness and cr+apr+(our new requirement) in the computation-theoretic adversarial model. Finally, we show that a polynomial-based mode of operation [6] satisfies our new requirement; namely, the polynomial-based mode of operation with fixed-input-length random oracles is indifferentiable from a variable-input-length random oracle in the computation-theoretic adversarial model.
Key Words : Adaptive Preimage Resistance, Indifferentiability, Preimage Awareness.

1 Introduction

Security notions that a basic function needs to possess in order to be suitable for domain extension while preserving desired properties of cryptographic hash functions are important. When such a security notion is defined, it should not depend on some specific constructions, but should be a general property of generic or well defined family of functions [4]. Lee and Park [5] defined a new security notion of adaptive preimage resistance (apr), which is defined in the information-theoretic adversarial model, and used the property of the notion to construct a general $\mathcal{F}$-indifferentiably secure (or pseudorandom oracle) constructions of the form $F(M) = \mathcal{R}(H^P(M))$, where P may be an ideal primitive, H^P is a VIL function, $\mathcal{R}$ is a FIL random oracle, and $\mathcal{F}$ is a VIL random oracle. This relation was described again in [6]. It was said, in the information-theoretic adversarial model, that F is indifferentiable from a VIL random oracle $\mathcal{F}$ when H^P is collision-resistant and adaptive preimage resistant. We emphasize that the indifferentiability security notion was introduced in both of the information-theoretic and computation-theoretic adversarial models, but, the apr notion was only defined in the information-theoretic adversarial model. So, it is not clear the implication of indifferentiability security notion in the computation-theoretic adversarial model.

It was further said that apr is a strengthened notion of the known notion of preimage resistance, which is not still clear because preimage resistance can be defined in any adversarial model but the apr is only defined in the information-theoretic adversarial model. Since this area, arguing about random objects, is quite subtle, the above claims require exact formal studies between information-theoretic and computation-theoretic adversarial models. (this scrutiny of formal generic properties is akin of cryptanalysis of constructions in the experimental design area).

What we found is that unfortunately, the definition and implication of apr is, in fact, limited, because there exists an adaptive preimage resistant and collision resistant H^P in the information-theoretic adversarial model such that $F(M) = \mathcal{R}(H^P(M))$ is not indifferentiable from a VIL random oracle $\mathcal{F}$ in the computation-theoretic adversarial model. Furthermore, we found that pr and apr are incomparable notions. To show these, we will describe counterexamples in Section 3 and Section 5. In Section 4, we give a new requirement on H^P (we call "admissibility") so that the above result of indifferentiability is made to hold even in the computation-theoretic adversarial model. But, apr+(our new requirement of Section 4) of H^P is still not a strengthened notion of pr of H^P. In Section 5 we clarify the relation between pr and apr while in Section 6 we explain the relation between preimage awareness (pra) and apr+cr+ (admissible H^P).

In Table 1 we summarize the above results (implications and non implications). Then in Section 7, we apply our results and we show that the polynomial-based mode of operation satisfies our new requirement, which means that the polynomial-based mode of operation based on fixed-input-length random oracles is indifferentiable from a variable-input-length random oracle in the computation-theoretic adversarial model (as originally claimed [6], but here we give a scrutinized proof under the admissibility conditions).

2 Preliminary

In this section, we briefly explain the definitions of indifferentiability, adaptive preimage resistance, preimage awareness, and one-way function.

Indifferentiability. The security notion of indifferentiability was introduced by Maurer *et al.* in TCC'04 [7]. In CRYPTO'05, Coron *et al.* were the first to adopt it as a security notion for hash functions [1]. Here, we only consider the security notion in this context of hash functions. Let F be a hash function based on ideal primitives $P_1, ..., P_j$ (such as an ideal permutation, an ideal block cipher, and FIL random oracle) and $\mathcal{F}$ be a VIL (Variable Input Length) random oracle, and $S^{\mathcal{F}} = (S_1^{\mathcal{F}}, ..., S_j^{\mathcal{F}})$ be a simulator with access to $\mathcal{F}$, where S_i's can communicate to each other. We note that S *should be computationally efficient* in the computation-theoretic adversarial model. Then, for any information-theoretic or computation-theoretic adversary A, the indifferentiability advantage against A is defined by

$$\mathrm{Adv}^{\mathrm{pro}}_{F^{P_1,\dots,P_j},S^{\mathcal{F}}}(A) = |\Pr[A^{F^{P_1,\dots,P_j},P_1,\dots,P_j} = 1] - \Pr[A^{\mathcal{F},S_1^{\mathcal{F}},\dots,S_j^{\mathcal{F}}} = 1]|.$$

Case	Result	Admissible	reference
1	$H^P : cr + pra \Rightarrow H^P : wpra$	N	[2, 3]
2	$H^P : cr + wpra \Rightarrow H^P : pra$	N	[2, 3]
3	$H^P : pra \Rightarrow F^{P,\mathcal{R}} : pro$	N	[2, 3]
4	$H^P : cr + apr \Rightarrow F^{P,\mathcal{R}} : pro$	Y	Sect. 4
5	$H^P : cr + apr \not\Rightarrow F^{P,\mathcal{R}} : pro$	N	Sect. 3
6	$H^P : apr \not\Rightarrow H^P : pr$	Y	Sect. 5.1
7	$H^P : apr \not\Rightarrow H^P : pr$	N	Sect. 5.1
8	$H^P : pr \not\Rightarrow H^P : apr$	Y	Sect. 5.2
9	$H^P : pr \not\Rightarrow H^P : apr$	N	Sect. 5.2
10	$H^P : pra \not\Rightarrow H^P : cr + apr$	Y	Sect. 6.1
11	$H^P : pra \not\Rightarrow H^P : cr + apr$	N	Sect. 6.1
12	$H^P : cr + apr \Rightarrow H^P : pra$	Y	Sect. 6.2
13	$H^P : cr + apr \not\Rightarrow H^P : pra$	N	Sect. 6.3

Table 1. The relationships (implications/ non-implications) between Collision Resistance (cr), Preimage Resistance (pr), Adaptive Preimage Resistance (apr) and Preimage Awarenenss (pra) and Weak Preimage Awareness (wpra) and Pseudorandom Oracle (pro) in the computation-theoretic adversarial model. H^P is a function based on a set P of ideal primitives and $F^{P,\mathcal{R}}(M) = \mathcal{R}(H^P(M))$, where $\mathcal{R}$ is a FIL random oracle. 'N' means that there is no condition on H^P while 'Y' means that the admissibility condition on H^P is needed.

When the value of the above advantage is small, we say that the hash function F is indifferentiable from the VIL random oracle $\mathcal{F}$. Maurer *et al.* [7] also proved that if F is indifferentiable from the VIL random oracle $\mathcal{F}$ in the computation-theoretic adversarial model (or in the information-theoretic adversarial model), then $\mathcal{F}$ used in any cryptosystem can be replaced with F in the computation-theoretic adversarial model (or in the information-theoretic adversarial model) with only a small loss of security. In other words, F can be used as a VIL pseudorandom oracle. Coron *et al.* [1] proved that prefix-free Merkle-Damgård construction, chop Merkle-Damgård construction, NMAC and HMAC constructions are indifferentiable from the VIL random oracle $\mathcal{F}$ in the FIL (Fixed Input Length) random oracle and the ideal cipher models.

Adaptive Preimage Resistance [5, 6]. Let A be any information-theoretic adversary, which means that A has an unbounded computing power. Let H^P be a function with access to the oracles $P = (P_1, P_2, ..., P_k)$. Let $\mathcal{Q}$ be the history of query-response pairs to P. Let $\mathsf{Map}_H(\mathcal{Q})$ be the set of input-output pairs of H^P that are information-theoretically determined by the history $\mathcal{Q}$ and H^P. Let A's i-th query be x_i and $\mathcal{Q}_i$ be the history determined by the first i query-response pairs. The adaptive preimage resistance experiment is defined as follows: for each i, after A gets $\mathcal{Q}_i$, A can adaptively commit elements z's of the range of H^P such that $\mathcal{Q}_i$ has not information-theoretically determined any preimage of z for H^P. Then, the adversary A wins the adaptive preimage resistance experiment whenever A finds a preimage of any one among all committed values. More precisely, given an adaptive preimage-finding adversary A, the adaptive preimage resistance of H^P is defined by

$$\mathrm{Adv}^{\mathrm{apr}}_{H,P}(A) = \Pr[\mathrm{Exp}^{\mathrm{apr}}_{H,P,A} \Rightarrow 1].$$

Then, the following theorem was given:

$\mathrm{Exp}^{\mathrm{apr}}_{H,P,A}$:
A^P updates $\mathcal{Q}$ and $\mathcal{L}$
if $\exists\ v$ such that $(v, w) \in \mathsf{Map}_H(\mathcal{Q})$ for some $w \in \mathcal{L}$ then return 1 otherwise 0

Fig. 1. Experiment for defining Adaptive Preimage Resistance (apr) for a hash function H and information-theoretic adversary A. Let $\mathcal{Q}$ be the history of query-response pairs to P and let $\mathcal{L}$ be the list of all the committed values.

Theorem 1 (Ro domain extension via cr+apr). *[5, 6] Let $F^{P,\mathcal{R}}(M) = \mathcal{R}(H^P(M))$, where $\mathcal{R}$ is a FIL random oracle and H^P is a function based on a set of ideal primitives $P = (P_1, .., P_k)$. For any indifferentiability adversary A there exists a simulator S such that*

$$\mathrm{Adv}^{\mathrm{pro}}_{F^{P,\mathcal{R}},S^{\mathcal{F}}}(A) \leq \mathrm{Adv}^{\mathrm{coll}}_{H^P,P}(q) + \mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, q_c),$$

where q is the maximum number of P queries and q_c is the maximum number of committed values in the adaptive preimage resistance experiment and $\mathcal{F}$ is a VIL random oracle. $\mathrm{Adv}^{\mathrm{coll}}_{H^P,P}(q)$ *denotes the maximum probability of finding a collision of H^P with q P-queries.* $\mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, q_c)$ *denotes the maximum probability of winning the adaptive preimage resistance experiment with q P-queries and q_c committed values.*

Preimage Awareness [2, 3]. Dodis, Ristenpart and Shrimpton defined the security notion of *Preimage Awareness* for hash functions [2, 3]. They proved that if H^P is preimage aware(pra), then $F^P(M) = \mathcal{R}(H^P(M))$ is indifferentiable from a VIL random oracle, where $\mathcal{R}$ is a FIL random oracle. The *extraction oracle* **Ex** is constructed with an *extractor* $\mathcal{E}$ and an advice string α, where α has the information of all query-response pairs of the oracle **P**, and the extractor $\mathcal{E}$ is an *efficient deterministic* algorithm. In the experiment of preimage awareness, the computational efficient adversary A can only access the ideal primitive P via the oracle **P**. In the experiment, A wins the game whenever A finds an input message M such that $H^P(M) = y$ and $M \neq \mathbf{Ex}(y)$ for any y, where H^P is a hash function based on the ideal primitive P, the domain of H^P be *Dom*, and the output $\mathbf{Ex}(y)$ belongs to $Dom \cup \{\perp\}$. *We note that $\perp$ cannot be an input message of H^P.*

$\mathrm{Exp}^{\mathrm{pra}}_{H,P,\mathcal{E},A}$	**oracle P**(u):	**oracle Ex**(y):
$M \xleftarrow{\$} A^{\mathbf{P},\mathbf{Ex}}$	$v \leftarrow P(u)$	$Q[y] \leftarrow 1$
$y \leftarrow H^P(M)$	$\alpha \leftarrow \alpha \vert\vert (u, v)$	$V[y] \leftarrow \mathcal{E}(y, \alpha)$
Return $(M \neq V[y] \wedge Q[y] = 1)$	Return v	Return $V[y]$

Fig. 2. Experiment for defining preimage awareness (PrA) for hash function H, extractor $\mathcal{E}$, and adversary A. The extractor $\mathcal{E}$ returns a point in $Dom \cup \{\perp\}$.

Then, given an extractor $\mathcal{E}$ and an computation-theoretic adversary A, the preimage awareness advantage of H^P is defined by

$$\mathrm{Adv}^{\mathrm{pra}}_{H,P,\mathcal{E}}(A) = \Pr[\mathrm{Exp}^{\mathrm{pra}}_{H,P,\mathcal{E},A} \Rightarrow \mathsf{true}].$$

And, if there exists an extractor $\mathcal{E}$ such that $\mathrm{Adv}^{\mathrm{pra}}_{H,P,\mathcal{E}}(A)$ is small for all reasonable adversaries A, the hash function H^P is called *preimage aware* (PrA). Then, the following theorem holds.

Theorem 2 (Ro domain extension via PrA). *[2, 3] Let $F^{P,\mathcal{R}}(M) = \mathcal{R}(H^P(M))$, where $\mathcal{R}$ is a FIL random oracle and H^P is a function based on a set of ideal primitives $P = (P_1, .., P_k)$. For any given extractor $\mathcal{E}$, we can construct a simulator $S^{\mathcal{F}} = (S_1, S_2^{\mathcal{F}})$ such that for any indifferentiability adversary A making at most (q_1, q_2, q_3) queries to its three oracles, there exists a preimage awareness adversary B_A making at most (q_p, q_e) queries to its two oracles such that*

$$\mathrm{Adv}^{\mathrm{pro}}_{F^{P,\mathcal{R}},(S_1,S_2^{\mathcal{F}})}(A) \leq \mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(B_A)$$

One-Way Permutation. $f : \{0,1\}^n \to \{0,1\}^n$ is a permutation and it is called one way if for any computational efficient adversary A the following holds.

$$\Pr[x \xleftarrow{\$} \{0,1\}^n; A(f(x)) = x] = \mathsf{neg}(n)$$

where $\mathsf{neg}(n)$ is a negligible function of n.

3 cr and apr of H^P are not sufficient for the indifferentiable security of $F(M) = \mathcal{R}(H^P(M))$

Lee and Park [5, 6] claimed that the collision resistance and adaptive preimage resistance of H^P are sufficient for the indifferentiable security of $F(M) = \mathcal{R}(H^P(M))$, where $\mathcal{R}$ is a FIL random oracle. However, their proof is limited, because they only consider the information-theoretic adversarial model. Think about the following example. We define a function $H^P(x) : \{0,1\}^* \to \{0,1\}^n$ as follows, where $P : \{0,1\}^* \to \{0,1\}^{n-1}$ is a VIL random oracle.

$$\begin{aligned} H^P(x) &= f(x)||1 \quad &&\text{if } |x| = n-1 \\ &= P(x)||0 &&\text{otherwise,} \end{aligned}$$

where $f : \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ is an one-way permutation.

Then, we can show that even if H^P is collision resistant and adaptive preimage resistant in the information-theoretic adversarial model, $F^{P,R}(M) = \mathcal{R}(H^P(M))$ is not indifferentiable from a VIL random oracle $\mathcal{F}$ in the computation-theoretic adversarial model, where H^P is defined in above and $\mathcal{R} : \{0,1\}^n \to \{0,1\}^n$ is a FIL random oracle.

Indifferentiable Attack on F in the computation-theoretic adversarial model. Let $(\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3)$ be $(F^P, P, \mathcal{R})$ or $(\mathcal{F}, S_1^{\mathcal{F}}, S_2^{\mathcal{F}})$, where $S = (S_1^{\mathcal{F}}, S_2^{\mathcal{F}})$ is any efficient simulator. Now we construct an indifferentiability adversary A as follows. Firstly, A chooses $(n-1)$-bit x randomly and computes $y = f(x)$. Then, A makes the query y to $\mathcal{O}_3$ and obtains its response z. Next, A makes the x query to $\mathcal{O}_1$ and obtains its response z'. If $z = z'$, A finally outputs 1. If $(\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3)$ is $(F^P, P, \mathcal{R})$, then $z = z'$ with probability 1. Next, we consider the case that $(\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3)$ is $(\mathcal{F}, S_1^{\mathcal{F}}, S_2^{\mathcal{F}})$. Note that the simulator S should be efficient in the computation-theoretic adversarial model, which means that S should be able to be implemented by a probabilistic Turing machine. Note that f is a one-way permutation, which means that no efficient algorithm can find x from $f(x)$ with better than non-negligible probability, where x is chosen randomly from the domain of f. So, no S can find x from $y(= f(x))$, which means that the probability that $z = z'$ is negligible. Therefore, F is not indifferentiable from a VIL random oracle $\mathcal{F}$ in the computation-theoretic adversarial model.

On the other hand, the following theorem says that H^P is, nevertheless, collision-resistant and adaptive preimage resistant in the information-theoretic adversarial model.

Theorem 3 (apr and cr of H^P). *Let H^P be the above function. Then, the following holds.*

$$\mathrm{Adv}^{\mathrm{apr}}_{H^{\mathcal{F}},\mathcal{F}}(q,q_c) \le \frac{q\cdot q_c}{2^{n-1}} \text{ and } \mathrm{Adv}^{\mathrm{cr}}_{H^{\mathcal{F}},\mathcal{F}}(q) \le \frac{q^2}{2^n}.$$

Proof. According to the definition of apr, the adversary A has an unbounded computing power. That means that A can compute all input-output pairs of f with no query to P. So, by the definition of apr, A cannot commit any value whose least significant value is '1', because all input-output pairs of f are computable without any query-response pair of P. So, A has to find an adaptive preimage of P. Since P is a VIL random oracle, by using $\mathrm{Adv}^{\mathrm{apr}}_{H^{\mathcal{F}},\mathcal{F}}(q,q_c) \le q_c \cdot \mathrm{Adv}^{\mathrm{apr}}_{H^{\mathcal{F}},\mathcal{F}}(q,1)$, which is easily proved, we get that $\mathrm{Adv}^{\mathrm{apr}}_{H^{\mathcal{F}},\mathcal{F}}(q,q_c) \le \frac{q\cdot q_c}{2^{n-1}}$. Second, we consider its collision resistance. Sine f is a permutation, any collision-finding adversary should find a collision of P. Therefore, we get that $\mathrm{Adv}^{\mathrm{cr}}_{H^{\mathcal{F}},\mathcal{F}}(q) \le \frac{q^2}{2^n}$, because P is a VIL random oracle with the output bit size of $n-1$. ■

4 Admissible H^P: a new Sufficient Requirement for using the Notion of Adaptive Preimage Resistance

The main problem of the definition of adaptive preimage resistance is that the simulator of the notion of indifferentiability in the computation-theoretic adversarial model is computationally efficient but the adversary in apr experiment is information-theoretic. So, there is a gap between their powers. Due to the gap, S, A, and the apr Experiment interpret differently the definition of $\mathsf{Map}_H(\mathcal{Q})$, where $\mathcal{Q}$ is the history of query-response pairs of P and H is a function based on a ideal primitive P. Therefore, we need a condition that S, A, and the apr Experiment should share the identical definition of $\mathsf{Map}_H(\mathcal{Q})$.

How can we achieve the above setting? We need *a new sufficient requirement* as follows;

$$\mathsf{Map}_H(\mathcal{Q}) \textit{ can be obtained by an efficient algorithm from the history } \mathcal{Q} \textit{ and } H,$$

where $\mathsf{Map}_H(\mathcal{Q})$ was already defined in the information-theoretic setting. If $\mathsf{Map}_H(\mathcal{Q})$ is defined by the computational notion, the apr experiment cannot check whether a commitment made by an apr adversary belongs to $\mathsf{Map}_H(\mathcal{Q})$ or not. We note that $\mathsf{Map}_H(\mathcal{Q})$, which satisfies our new requirement, depends on the structure of H^P. We say that H^P is *admissible* if H^P satisfies the new requirement. So, we *emphasize* that the notion of adaptive preimage resistance can be only used to quantify the security just of "admissible hash functions," but not any (generic) hash function because of our new requirement.

5 The Incomparability of Adaptive Preimage Resistance and Preimage Resistance

Similar to the above refutation in Section 3, it can also be shown that Theorem 1 in [5] is not correct, since we show that there is no relation between apr and PR, even with the admissibility condition of Section 4.

5.1 Adaptive Preimage Resistance does not imply Preimage Resistance, even under admissible H^P

Without any formal proof, Lee and Park [5] claimed that $\mathrm{Adv}^{\mathrm{pre}}_{H^P,P}(q) \le \mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q,1)$. But, their insight is not correct, and, in fact, there is a counterexample showing H^P is not preimage resistant but adaptive preimage resistant (even satisfying our new requirement in Section 4). This means that the notion of adaptive preimage resistance is not a strengthened notion of preimage resistance. This indicates that the name apr cannot really be justified. *We need to change the notion of apr into another notion.* Consider the following example. We define a hash function $H^P(x) : \{0,1\}^* \to \{0,1\}^n$ as follows, where $P : \{0,1\}^* \to \{0,1\}^{n-1}$ is a VIL random oracle.

$$\begin{aligned} H^P(x) &= x||1 \quad && \text{if } |x| = n-1 \\ &= P(x)||0 && \text{otherwise.} \end{aligned}$$

The H^P is above not preimage resistant, because given a random output of H^P, we can find a preimage with at least 1/2 probability. On the the hand, we can prove that H^P is adaptive preimage resistant (even in the case of our new alternative definition of adaptive preimage resistance).

Admissibility of H^P. Let Q be the history of query-response pairs of the random oracle P and let $\mathsf{Map}_{H^P}(\mathcal{Q})$ be the set of input-output pairs of H^P that are information-theoretically determined by the history $\mathcal{Q}$ and H^P. Now, what we have to show is to construct an efficient algorithm $\mathcal{A}$ generating $\mathsf{Map}_{H^P}(\mathcal{Q})$ from $\mathcal{Q}$ and H^P. Let q be the number of non-repeated P-queries and T be the empty set.

algorithm $\mathcal{A}(\mathcal{Q}, H^P)$

100 For each i-th query-response pair $(x_i, y_i) \in \mathcal{Q}$, $\quad //1 \le i \le q$
101 if $|x_i| = n-1$, then $T \leftarrow T \cup \{(x_i, y_i||0)\}$
200 $T \leftarrow T \cup \{(z, z||1)\}$ for all $(n-1)$-bit string z's
300 Return T

Now, we want to check the implementation complexity of $\mathcal{A}$. Line 100 and 101 can be done with complexity $O(q)$. Our main concern is about line 200. Even though we have to consider all $(n-1)$-bit strings, we can efficiently store $(bin_{n-1}(i), bin_{n-1}(i)||1)$ in T, because there is a simple relation between input and output. So, line 200 can be also efficiently implemented. So, we can know that T is exactly same as $\mathsf{Map}_{H^P}(\mathcal{Q})$. Therefore, H^P is admissible.

Theorem 4. *Let H^P be the above function. Then, the following holds.*

$$\mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, q_c) \le \frac{q \cdot q_c}{2^{n-1}}.$$

Proof. Let A be any adaptive preimage-finding adversary with q P-queries and q_c commitments. By the definition of apr, A cannot commit any value whose least significant value is 1, because the preimage corresponding to any output value whose least significant value is 1 can be obviously computed with no query and with very small time complexity. Therefore, A should succeed in finding an adaptive preimage of the VIL random oracle P. Using $\mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, q_c) \le q_c \cdot \mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, 1)$, we get that $\mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(q, q_c) \le \frac{q \cdot q_c}{2^{n-1}}$. ■

5.2 Preimage Resistance does not imply Adaptive Preimage Resistance, even under admissible H^P

Consider the following example: We define a hash function $H^{P_1,P_2}(x) : \{0,1\}^* \to \{0,1\}^n$ as follows, where $P_1 : \{0,1\}^n \to \{0,1\}$ is a FIL random oracle and $P_2 : \{0,1\}^* \to \{0,1\}^n$ is a VIL random oracle.

$$\begin{aligned} H^{P_1,P_2}(x) &= P_1(x)||1^{n-1} \qquad \text{if } x = 0^n \\ &= P_2(x) \quad \text{otherwise.} \end{aligned}$$

It can be easily shown that H^{P_1,P_2} is preimage resistant, because the outputs of all inputs except for one input are obtained by the VIL random oracle P_2. Also it is easily shown that H^{P_1,P_2} is admissible in the similar way described in Section 5.1. However, H^{P_1,P_2} is not adaptive preimage resistant.

Adaptive Preimage-Finding Attack on H^{P_1,P_2}. Our adversary A works as follows. Firstly, A commits $0||1^{n-1}$ and 1^n to the apr experiment, where the preimage of two values cannot be computable without the query 0^n to P_1 because we don't know that $P_1(0^n) = 0||1^{n-1}$ or 1^n. Then, A makes the query 0^n to P_1 and obtains its response $z = H^{P_1,P_2}(0^n)$. Since $z = 0||1^{n-1}$ or 1^n with probability 1, A wins the apr experiment.

6 Relations Between Preimage Awareness and apr+cr, under admissible H^P

Dodis, Ristenpart and Shrimpton [2, 3] showed that if H^P is preimage aware, then $F(M) = \mathcal{R}(H^P(M))$ is indifferentiable from a VIL random oracle, where $\mathcal{R}$ is a FIL random oracle. Now we wonder what is the relation between Preimage awareness and cr+apr+(the condition in Section 4).

6.1 Preimage awareness does not imply apr+cr, even under admissible H^P

Consider the following example. Let $t \gg n$. We define a function $H^P(x) : \{0,1\}^* \to \{0,1\}^*$ as follows, where $P : \{0,1\}^n \to \{0,1\}^{tn}$ is a FIL random oracle with a condition that the XOR of all output strings of P is 0^{tn} or 1^{tn} with probability $\frac{1}{2}$, where a^{tn} means the tn-bit string of all a.

$$\begin{aligned} H^P(x) &= P(x)||1 \qquad \text{if } |x| = n \\ &= x||0 \qquad\quad \text{otherwise.} \end{aligned}$$

It is easily shown that H^P is admissible in the similar way described in Section 5.1.

Theorem 5. *Let $t \gg n$ and let H^P be the above function. For any preimage awareness adversary A making at most (q_p, q_e) queries to the oracles **P** and **Ex**, there exists an extractor $\mathcal{E}$ such that*

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(A) \leq \frac{q_p q_e}{2^{tn}} + \frac{q_p^2}{2^{tn+1}} + \frac{1}{2^{(t-1)n-1}},$$

Proof. We use Lemma 3.3 and the proof technique of Lemma 3.4 in [3], which are related to the definition of the weak preimage awareness. In the definition of the weak preimage awareness, a multi-point extractor $\mathcal{E}^+$ is used instead of an extractor $\mathcal{E}$. Below, we define a multi-point extractor $\mathcal{E}^+$. Note that a multi-point extractor does not return a single value like an extractor but returns a set of values $\mathcal{X}$. Then, we define $\mathcal{E}$ in the same way of [3]; on input (z, α) runs $\mathcal{X} \leftarrow \mathcal{E}^+(z, \alpha)$ and outputs the first element in $\mathcal{X}$. We note that $\mathcal{E}^+$ defined in below is not a honest multi-point extractor, so we cannot directly use the result of Lemma 3.4 in [3]. Any honest multi-point extractor should output a set of real preimages. However, we can use the relation shown in the proof of Lemma 3.4 in [3] as follows.

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(A) \leq q_e \mathrm{Adv}^{1-\mathrm{wpra}}_{H^P,P,\mathcal{E}^+}(B) + \Pr[\mathsf{coll}]$$

where $\Pr[\mathsf{coll}]$ means the probability that $\mathcal{E}^+$ outputs a set of size larger than one. Note that $\Pr[\mathsf{coll}]$ cannot be bounded by the collision resistance of H^P because $\mathcal{E}^+$ is not honest. So, we have to show the following two inequalities. First, we need to show that there exists a multi-point extractor $\mathcal{E}^+$ such that for any weak preimage awareness adversary B with a single query to $\mathbf{Ex}$, $\mathrm{Adv}^{1-\mathrm{wpra}}_{H^P,P,\mathcal{E}^+}(B) \leq \frac{q_p}{2^{tn}}$. Second, we need to show that $\Pr[\mathsf{coll}] \leq \frac{q_p^2}{2^{tn+1}} + \frac{1}{2^{(t-1)n-1}}$. Then, the theorem holds.

α is the list of query-response pairs of $\mathbf{P}$, $\mathcal{X} = \emptyset$, and $chop_1(x)$ is the least significant 1-bit chopping function.

algorithm $\mathcal{E}^+(z, \alpha)$:

001 If $lsb(z)$=1 then $\mathcal{X} = \mathcal{X} \cup \{M : chop_1(z) = P(M) \textit{ is computable from } \alpha\}$
002 If $lsb(z)$=1 and $chop_1(z) = T \oplus \bigoplus_{i=1}^{2^n-1} y_i$ such that $2^n - 1$ input-output pairs (x_i, y_i)
003 of P are determined from α, where all x_i's are different
004 and $T = 0^{tn}$ or 1^{tn}, then $\mathcal{X} = \mathcal{X} \cup \{M : M = \bigoplus_{i=1}^{2^n-1} x_i\}$
005 If $lsb(z)$=0 then $\mathcal{X} = \mathcal{X} \cup \{chop_1(z)\}$
006 Return $\mathcal{X}$

Note that B is any weak preimage awareness adversary with a single query to $\mathbf{Ex}$. So, once B makes a query z to $\mathbf{Ex}$, B wins the weak preimage awareness game when B finds a new preimage M' such that $H^P(M') = z$. Since P is a random oracle with a condition that the XOR of all output strings of P is 0^{tn} or 1^{tn} and B can make at most q_p queries to $\mathbf{P}$, the probability that B wins is at most $\frac{q_p}{2^{tn}}$.

Next, we consider an upper bound on $\Pr[\mathsf{coll}]$, where $\Pr[\mathsf{coll}] = \Pr[|\mathcal{X}| > 1]$. Note that $\mathcal{X}$ is updated in lines 001, 004 and 005. Line 005 does not influence the value of $\Pr[\mathsf{coll}]$, because if $\mathcal{X}$ is updated in line 005, then $|\mathcal{X}| = 1$. So we focus on lines 001 and 004.

$$\begin{aligned}
\Pr[\mathsf{coll}] &= \Pr[\mathsf{coll} \wedge (\mathcal{X} \textit{ is updated in line } 001) \wedge (\mathcal{X} \textit{ isn't updated in line } 004)] \\
&\quad + \Pr[\mathsf{coll} \wedge (\mathcal{X} \textit{ is updated in line } 001) \wedge (\mathcal{X} \textit{ is updated in line } 004)] \\
&\leq \Pr[\mathsf{coll} \wedge (\mathcal{X} \textit{ is updated in line } 001) \wedge (\mathcal{X} \textit{ isn't updated in line } 004)] \\
&\quad + \Pr[y_j = T \oplus \textstyle\bigoplus_{i=1}^{2^n-1} y_i \textit{ for a } j] \qquad // \ T = 0^{tn} \text{ or } 1^{tn} \\
&\leq \Pr[\mathcal{X} \textit{ is a set of size larger than one in line } 001 | y_j \neq T \oplus \textstyle\bigoplus_{i=1}^{2^n-1} y_i \textit{ for all } j] \\
&\quad + \Pr[y_j = T \oplus \textstyle\bigoplus_{i=1}^{2^n-1} y_i \textit{ for a } j] \\
&\leq \tfrac{q_p^2}{2^{tn+1}} + \Pr[y_j = T \oplus \textstyle\bigoplus_{i=1}^{2^n-1} y_i \textit{ for a } j] \qquad \cdots \ (1) \\
&\leq \tfrac{q_p^2}{2^{tn+1}} + \tfrac{1}{2^{(t-1)n-1}} \qquad \cdots \ (2)
\end{aligned}$$

First, we explain (1). The condition that $y_j \neq T \oplus \bigoplus_{i=1}^{2^n-1} y_i \textit{ for all } j$ means that for each x_i, $y_i = P(x_i)$ is a random value. So (1) holds, because there are at most q_p P-queries. Next, we explain (2). For each x_i $(1 \leq i \leq 2^n - 1)$, y_i is a random value, because $y = P(\bigoplus_{i=1}^{2^n-1} x_i)$ is only non-random by the definition of P. So, the probability that there exists a y_j $(1 \leq j \leq 2^n - 1)$ such that $y_j = T \oplus \bigoplus_{i=1}^{2^n-1} y_i$ is at most $\frac{2 \cdot (2^n-1)}{2^{tn}}$ $(< \frac{1}{2^{(t-1)n-1}})$, where $T = 0^{tn}$ or 1^{tn}. ∎

Adaptive Preimage-Finding Attack on the above H^P. Let $t \gg n$. We construct an adaptive preimage-finding adversary A with $2^n - 1$ P-queries and two commitments. Firstly, for all n-bit x's except for $x = 1^n$ A makes query x to P and gets y from P. We denote all query-response pairs by (x_i, y_i), where $1 \le i \le 2^n - 1$. Next, A commits $y||1$ and $y \oplus 1^{tn}||1$, where $y = \bigoplus_{i=1}^{2^n-1} y_i$. In the definition of apr, committed values should not be determined from all current query-response pairs. Here, preimages of $y||1$ and $y \oplus 1^{tn}||1$ cannot be determined from all query-response pairs of P because no one knows the exact value of the XOR of all output strings of P. Note that the XOR of all output strings of P is 0^{tn} or 1^{tn} with probability $\frac{1}{2}$, not 1. Finally, A returns $x = 1^n$ to the adaptive preimage experiment, where $H^P(1^n) = y||1$ or $y \oplus 1^{tn}||1$. So, A wins the apr experiment.

6.2 apr+cr implies Preimage awareness, under admissible H^P

Here, we want to show that apr+cr+(the admissible requirement on H^P in Section 4) of H^P means Preimage awareness of H^P, by proving the next theorem. We can easily generalize the following theorem in the case that $P = (P_1, ..., P_k)$ is a tuple of ideal primitives P_i's.

Theorem 6. *Let H^P be a function based on an ideal primitive P. H^P satisfies the new requirement in Section 4. Then we can construct an extractor $\mathcal{E}$ such that for any preimage awareness adversary A making at most (q_p, q_e) queries to oracles $\boldsymbol{P}$ and $\boldsymbol{Ex}$, there exist an adaptive preimage-finding adversary B_A making at most q_e P-queries and q_e commitments, and a collision-finding adversary C_A making at most q_p P-queries such that*

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(A) \le \mathrm{Adv}^{\mathrm{apr}}_{H^P,P}(B_A) + \mathrm{Adv}^{\mathrm{coll}}_{H^P,P}(C_A)$$

Proof. Let α be the history of query-response pairs of $\mathbf{P}$. By the new requirement in Section 4, our $\mathcal{E}$ has an ability to compute $\mathsf{Map}_H(\alpha)$, where $\mathsf{Map}_H(\alpha)$ is the set of input-output pairs of H^P that is information-theoretically determined by α. We define $\mathcal{E}$ as follows.

algorithm $\mathcal{E}(z, \alpha)$:

001 If there exists at least one M such that $z = H^P(M)$ is determined from $\mathsf{Map}_H(\alpha)$, then return any such M
002 Otherwise return $\perp$

Whenever A wins the preimage awareness experiment, at least one of two following events occurs by the definition of the above $\mathcal{E}$.

Event 1. A obtains M such that $H^P(M) = z$ and $\mathbf{Ex}(z) = \perp$ occurred before, which means that such z was not determined from $\mathsf{Map}_H(\alpha)$ at that time by the definition of the above $\mathcal{E}$.

Event 2. A obtains M and M' ($M \ne M'$) such that $H^P(M) = H^P(M')$ is determined from $\mathsf{Map}_H(\alpha)$. In other words,

$$\mathrm{Adv}^{\mathrm{pra}}_{H^P,P,\mathcal{E}}(A) \le \Pr[\textit{Event } 1 \textit{ occurs}] + \Pr[\textit{Event } 2 \textit{ occurs}].$$

And it is clear that whenever Event 1 occurs, B_A wins the apr experiment, and whenever Event 2 occurs, C_A wins the cr experiment. Therefore, the theorem holds.

algorithm B^P_A // Initialize $Z = \emptyset$.

First step.

100 Run $A^{\mathbf{P},\mathbf{Ex}}$.
110 On **P**-query x
111 $y = P(x)$ // B_A has the access to the oracle P.
112 $\alpha = \alpha || (x, y)$
120 Respond y to A
121 On **Ex**-query z
122 $M = \mathcal{E}(z, \alpha)$.
123 If $M = \perp$ then commit z to the apr experiment and $Z = Z \cup \{z\}$
124 Respond M to A

Second step. (after finishing running $A^{\mathbf{P},\mathbf{Ex}}$.)

200 If $\exists$ M such that $H^P(M)$ is determined from $\mathsf{Map}_H(\alpha)$ and $H^P(M) \in Z$, then return an adaptive preimage M to the apr experiment.

algorithm C_A^P // Initialize $Z = \emptyset$.

First step.

100 Run $A^{\mathbf{P},\mathbf{Ex}}$.
110 On **P**-query x
111 $y = P(x)$ // B_A has the access to the oracle P.
112 $\alpha = \alpha || (x, y)$
120 Respond y to A
121 On **Ex**-query z
122 $M = \mathcal{E}(z, \alpha)$.
123 Respond M to A

Second step. (after finishing running $A^{\mathbf{P},\mathbf{Ex}}$.)

200 If $\exists$ M and M' ($M \neq M'$) such that $H^P(M) = H^P(M')$ is determined from $\mathsf{Map}_H(\alpha)$, then return the collision pair (M, M') to the cr experiment. ■

6.3 apr+cr doesn't mean Preimage awareness

This is clear by the cases 3 and 5 in the Table 1.

7 Security Analysis of Lee-Steinberger's Domain Extension Revisited

Lee and Steinberger [6] proposed a new double-piped mode of operation for multi-property-preserving domain extension of MACs, PRFs, and PROs (pseudorandom oracles). Due to wrong definition of apr, we cannot guarantee that Lemma 2, Theorem 5, Theorem 6 of [6] are right. So, we need to check whether their new domain extension satisfies our new security requirement described in Section 4 or not. In [6], they proposed a compression function $\phi[f]$ depicted in Fig. 3, where $f : \{0,1\}^{3n} \to \{0,1\}^n$. Therefore, it is crucial to check if $\phi[f]$ satisfies our new security requirement (admissibility) when f is a fixed-input length random oracle.

Let Q be the history of query-response pairs of the random oracle f and let $\mathsf{Map}_{\phi[f]}(\mathcal{Q})$ be the set of input-output pairs of $\phi[f]$ that are information-theoretically determined by the

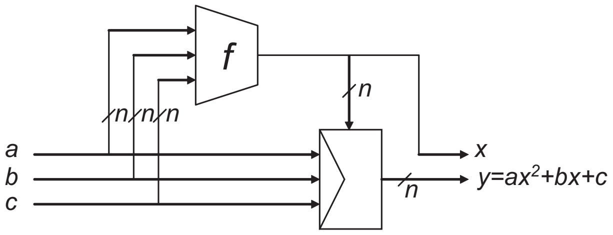

Fig. 3. The compression function $\phi[f]$ proposed in [6].

history $\mathcal{Q}$ and $\phi[f]$. Now, what we have to show is to construct an efficient algorithm $\mathcal{A}$ generating $\mathsf{Map}_{\phi[f]}(\mathcal{Q})$ from $\mathcal{Q}$ and $\phi[f]$. Let q be the number of non-repeated f-queries and T be the empty set.

algorithm $\mathcal{A}(\mathcal{Q}, \phi[f])$
100 For each i-th query-response pair $((a_i||b_i||c_i), x_i) \in \mathcal{Q}$, $//1 \leq i \leq q$
101 Compute $y_i = a_i x_i^2 + b_i x + c_i$ and $T \leftarrow T \cup \{((a_i||b_i||c_i), (x_i, y_i))\}$
200 Return T

It is easy to check that $\mathcal{A}$ can be efficiently implemented with complexity $O(q)$ and input-output pairs of f and $\phi[f]$ are in one-to-one correspondence, which means that $\mathsf{Map}_{\phi[f]}(\mathcal{Q}) = T$. So, $\phi[f]$ is admissible. Therefore, we conclude that Lemma 2, Theorem 5, Theorem 6 of [6] are valid by the result of this section.

References

1. J. S. Coron, Y. Dodis, C. Malinaud and P. Puniya, *Merkle-Damgard Revisited: How to Construct a Hash Function*, Advances in cryptology-crYPTO'05, LNCS 3621, Springer-Verlag, pp. 430-448, 2005.
2. Y. Dodis, T. Ristenpart and T. Shrimpton, *Salvaging Merkle-Damgård for Practial Applications*, Advances in cryptology – EUROcrYPT'09, LNCS 5479, Springer-Verlag, pp. 371-388, 2009.
3. Y. Dodis, T. Ristenpart and T. Shrimpton, *Salvaging Merkle-Damgård for Practial Applications*, cryptology ePrint Archive 2009/177 (full version Eurocrypt 09 paper).
4. O. Goldreich, *Foundations of cryptography : Volume I Basic Tools*, Cambridge University Press, 2001.
5. J. Lee and J. H. Park, *Adaptive Preimage Resistance and Permutation-based Hash Functions*, cryptology ePrint Archive: Report 2009/066, 2009.
6. J. Lee and J. Steinberger, *Multi-property-preserving Domain Extension Using Polynomial-based Modes of Operation*, Advances in cryptology – EUROcrYPT'10, LNCS , Springer-Verlag, pp. . (See http://eprint.iacr.org/2010/131.)
7. U. Maurer, R. Renner and C. Holenstein, *Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology*, TCC'04, LNCS 2951, Springer-Verlag, pp. 21-39, 2004.