# Black-box property of Cryptographic Hash Functions*

Michal Rjaško

Department of Computer Science
Faculty of Mathematics, Physics and Informatics
Comenius University
Mlynská dolina, 842 48 Bratislava, Slovak Republic
rjasko@dcs.fmph.uniba.sk

**Abstract.** We define a new black-box property for cryptographic hash function families $H : \{0,1\}^K \times \{0,1\}^* \to \{0,1\}^y$ which guarantees that for a randomly chosen hash function $H_K$ from the family, everything "non-trivial" we are able to compute having access to the key $K$, we can compute only with oracle access to $H_K$. If a hash function family is pseudo-random and has the black-box property then a randomly chosen hash function $H_K$ from the family is resistant to all non-trivial types of attack. We also show that the HMAC domain extension transform is Prf-BB preserving, i.e. if a compression function $f$ is pseudo-random and has black-box property (Prf-BB for short) then $\text{HMAC}^f$ is Prf-BB. On the other hand we show that the Merkle-Damgård construction is not Prf-BB preserving. Finally we show that every pseudo-random oracle preserving domain extension transform is Prf-BB preserving and vice-versa. Hence, Prf-BB seems to be an all-in-one property for cryptographic hash function families, which guarantees their "total" security.

## 1 Introduction

The primary security property for cryptographic hash functions has historically been collision resistance. For a collision resistant hash function $F : \{0,1\}^* \to \{0,1\}^y$ it is hard to find a pair of messages $(M, M')$ such that $F(M) = F(M')$. Currently used hash functions, such as the SHA family or MD5, are designed using the Merkle-Damgård (MD) construction [7, 10]. The MD construction is a domain extension transform, i.e. it extends a domain of a fixed-input-length (FIL) compression function $f : \{0,1\}^{(y+d)} \to \{0,1\}^y$ to a variable-input-length (VIL) hash function $F$. The key security feature of the MD construction is that it preserves collision resistance. If the compression function $f$ is collision resistant, then so is the resulting hash function $F$.

However, collision resistance is not enough to prove the security of many important applications which involve hash functions. A cryptographic hash function should have "random" behavior, which collision resistance alone cannot ensure. Moreover, for several of the applications (e.g. RSA-FDH) no standard model security property sufficient for proving their security has been found. On the other hand, no realistic attacks against these applications have been found. Hence, Bellare and Rogaway [4] introduced a so called random oracle model, which models a hash function as a publicly available random function (random oracle). Using this framework, one can prove the security of many important schemes. A proof in the random oracle model does not guarantee security when we replace the random oracle with a real hash function [5]. However, such a proof is believed to ensure that there are no structural flaws in the scheme and thus one can heuristically hope that the scheme remains flawless when the random oracle is replaced with a "well designed" hash function.

* Research supported by VEGA grant No. 1/0266/09 and Comenius University grant No. UK/429/2010.

Real hash functions are often built using some smaller components such as compression function in the case of the MD construction. On the other hand, in the random oracle model, hash functions are modeled as a monolithic oracle without any subcomponents. In order to avoid such a contrast between theory and practice, Maurer, Renner and Holenstein introduced the indifferentiability framework [9] and consequently Coron et. al defined a property for hash functions called pseudo-random oracle [6]. If a hash function $F$ is pseudo-random oracle then it is indifferentiable from the random oracle. Hence, $F$ can be used in any cryptosystem instead of the random oracle without loosing the security. The pseudo-random oracle property assumes that a hash function is built from a publicly available FIL random function $f$ (compression function). Thus, the pseudo-random oracle property still requires the random oracle model.

It is hard to define collision resistance for hash functions in the standard model. Due to the pigeonhole principle, each hash function with domain greater than its range has a pair of messages which map to the same image. A potential adversary attacking a hash function can have such a pair hardwired into its code, so that its description is simple and it runs very fast. Hence, formal definitions of security properties for cryptographic hash function are often made in the dedicated-key settings [2, 11]. A hash function with a dedicated-key input is called a hash function family (i.e. $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$), a particular hash function from the family is selected by a key $K$ ($K \in \{0,1\}^k$). In the dedicated-key settings, a potential adversary has to find a collision for a hash function $H_K$ randomly chosen from the family.

*Our contributions.* In this paper we introduce a black-box (BB) property for hash function families. If a hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ has the BB property, then everything "non-trivial" we are able to compute having access to the randomly chosen key $K$, we are able to compute only with oracle access to the hash function $H_K$. A "non-trivial" thing we define as an information which is hard to compute for a random oracle. Clearly, the BB property is not sufficient for "good" cryptographic hash functions. Moreover, the BB property can be easily achieved by a hash function family, which "reveals" its key (e.g. a family for which $H_K(0) = K$). On the other hand, we show that a *pseudo-random* hash function family with the BB property (a Prf-BB hash function family for short) is resistant to all "non-trivial" attacks. For a Prf-BB hash function family, the pseudo-randomness ensures that without access to a randomly chosen key $K$, one cannot distinguish $H_K$ from a random oracle. Additionally, the black-box property ensures that access to the key $K$ does not reveal any "useful" information about the structure of $H_K$.

We show that the MD construction does not preserve the Prf-BB property. On the other hand, we show that the HMAC construction [1, 6] is Prf-BB preserving. Moreover we show that every pseudo-random oracle preserving domain extension transform is Prf-BB preserving and vice-versa. Hence Prf-BB property can be seen as a replacement of the pseudo-random oracle property for the standard model and can become a new primary security goal for hash function families.

*Organization.* In Section 2 we introduce some useful notations and definitions. In Section 3 we define the black-box property and show that a randomly chosen hash function from a Prf-BB hash function family is resistant to all "non-trivial" types of attack. Next, in Section 4 we show that the MD construction is not Prf-BB preserving. The proof that the HMAC construction is Prf-BB preserving is in Section 5. In Section 6 we show the equivalence between pseudo-random oracle preserving domain extension transforms and Prf-BB preserving domain extension transforms.

## 2 Preliminaries

We write $M \xleftarrow{\$} \mathcal{S}$ for the uniform random selection of $M$ from the finite set $\mathcal{S}$. Concatenation of finite strings $M_1$ and $M_2$ is denoted by $M_1||M_2$ or simply $M_1M_2$, $\overline{M}$ denotes bitwise complement of the string $M$. The $i$-th bit of a string $M$ is $M[i]$, thus $M = M[1]||\cdots||M[|M|]$. By $M_1, \ldots, M_l \xleftarrow{d} M$, where $M$ is a string, is denoted the following semantics:

1. Pad $M$ with the suffix pad $:= 1||0^{d-((|M|+1) \mod d)}$
2. Parse the string $M||\text{pad}$ into $M_1, M_2, \ldots M_l$, where $|M_i| = d$ for $1 \leq i \leq l$. It must hold that $M_1||M_2||\ldots||M_l = M||\text{pad}$.

Let $\text{Func}(D, R)$ represent the set of all functions $\rho : D \to R$ and let $RF_{D,R}$ be a function chosen randomly from the set $\text{Func}(D, R)$ (i.e. $RF_{D,R} \xleftarrow{\$} \text{Func}(D, R)$). We sometimes write $RF_{d,r}$ or $\text{Func}(d, r)$ when $D = \{0,1\}^d$ and $R = \{0,1\}^r$. Similarly, we write $RF_{*,r}$ or $\text{Func}(*, r)$ when $D = \{0,1\}^*$ and $R = \{0,1\}^r$. If $i$ is an integer, then $\langle i \rangle_r$ is $r$-bit string representation of $i$. If $r$ is omitted, then $\langle i \rangle$ is the shortest string representation of $i$ (e.g. if $i = 3$, then $\langle i \rangle = 11$).

*Hash function family.* Let $n \in \mathbb{N}$ be a security parameter. A variable input length hash function family is a function $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ computable in a polynomial time, where $k, y \in \mathbb{N}$. In the rest of this paper we assume that $k, y$ are polynomially related to the security parameter $n$ (i.e. $k = p_1(n)$ and $y = p_2(n)$ for some polynomials $p_1, p_2$). We will often write the first argument to $H$ as a subscript, i.e. $H_K(M) := H(K, M)$. A fixed input length hash function family is a function $H : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^y$, where $k, m, y \in \mathbb{N}$ are polynomially related to the security parameter $n$.

*Negligible function.* A function $f$ is negligible if for every polynomial $p(\cdot)$ there exists $N$ such that for every $n > N$ it holds that $f(n) < \frac{1}{p(n)}$. Negligible functions are denoted as $\text{negl}(\cdot)$.

*Interactive Turing machines.* An interactive Turing machine (ITM) $T$ accepts inputs via input tape, performs some local computations and outputs via output tape. An ITM $T$ can have "oracle" access to several other ITMs $T_1, \ldots, T_l$. The communication between $T$ and $T_1, \ldots, T_l$ is performed via "oracle" input tapes $t_1, \ldots, t_l$ and output tapes $t'_1, \ldots, t'_l$. Whenever $T$ writes some input on the tape $t_i$, the ITM $T_i$ is invoked on that input and its output is written on the oracle output tape $t'_l$. We call such operation a query to the oracle $T_i$. All queries are performed in unit time (i.e. computation of $T_i$ is not counted into $T$'s running time). By $T^{T_1,\ldots,T_l}$ we denote that the ITM $T$ has oracle access to $T_1, \ldots, T_l$.

Each ITM can implement various interfaces $(f_1, f_2, \ldots)$. An interface specifies what needs to be written on the input type to invoke particular functionality of the ITM. We write $T = (f_1, f_2, \ldots)$ meaning that $T$ implements interfaces $f_1, f_2, \ldots$.

We sometimes distinguish between private and public interfaces of an ITM $T$. In this case we write $T = ((f_1, f_2, \ldots), (f'_1, f'_2, \ldots))$, where $f_1, f_2, \ldots$ are private interfaces and $f'_1, f'_2, \ldots$ are public. We write $P^{T_{pub}}$ to denote that an ITM $P$ has oracle access only to public interfaces of an ITM $T$.

*Adversary.* An adversary is a probabilistic polynomial-time ITM. Running time of an adversary $A$ is the expected running time of $A$ plus the description size of $A$ (hence one cannot precompute some large amount of information and store it into $A$'s description). Running time of an adversary is polynomial in length of its inputs and the security parameter $n$. Without loss of generality we assume that an adversary always stop and returns some output.

*Games.* A game $G^{O,A}$ is a probabilistic polynomial ITM which output is always a bit $b \in \{0,1\}$. If $b = 1$ we say that the adversary $A$ won the game $G$ for the oracle $O$. If $b = 0$ we say that $A$ lost the game $G$ for $O$. In this paper we focus on the games with the first oracle being a hash function or a hash function family.

*Example 1.* Let $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family, and let $G_{\mathrm{CR}}$ be the following algorithm:

**Game** $G_{CR}$
$G_{CR}$ has access to $H(\cdot,\cdot)$ and adversary $A(\cdot)$
1. choose $K \xleftarrow{\$} \{0,1\}^k$
2. query $A(K) \to (M, M')$
3. if $M \neq M'$ and $H(K, M) = H(K, M')$ return 1
4. otherwise return 0.

The game $G_{CR}$ represents the well known collision resistance experiment for the hash function family $H$. If no polynomial adversary $A$ can win the game $G_{CR}$ for $H$ with non-negligible probability we say $H$ is collision resistant. Note that we can define games also for all other standard properties of hash function families like preimage resistance, second-preimage resistance, their everywhere and always versions [11], unforgeability, etc.

*Example 2.* The following game $G_{CRF}$ for a hash function $F : \{0,1\}^* \to \{0,1\}^y$ is an "unkeyed" adaptation of the game $G_{CR}$ from the Example 1.

**Game** $G_{CRF}$
$G_{CRF}$ has access to $F(\cdot)$ and adversary $A$
1. query $A \to (M, M')$
2. if $M \neq M'$ and $F(M) = F(M')$ return 1
3. otherwise return 0.

Note that for all hash functions $F$ there exists an efficient adversary $A$ which returns a collision for $F$. Since there exists collisions in $F$, $A$ just needs to have one of the collisions hardwired into its description. Hence, we cannot define collision resistance for hash functions.

A hash function $F : \{0,1\}^* \to \{0,1\}^y$ and a hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ can represent the same function $\rho(K, M) = F(K||M) = H(K, M)$. Hence, when considering an arbitrary game $G$, we cannot tell whether it treats it's oracle as a hash function (e.g. $G_{CRF}$) or hash function family (e.g. $G_{CR}$). This is undesirable in some cases, where we want to utilize advantages of hash function families (e.g. ability to define collision resistance). Because of this, in the following definitions of a non-trivial game and the black-box property, we make a random choice of a key before the game starts. Then the game $G$ is given access to the hash function $H_K$ chosen randomly from the family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ (but $K$ is not given to $G$). Thus, we can utilize the advantages of hash function families and we don't restrict how games should treat their oracle.

*Non-trivial games.* There are games, which are easy to win (e.g. a game which always returns 1) and games which cannot be won (a game always returning 0). Informally, a trivial game $G$ is a game, which utilizes adversary's knowledge of the key so that it can be won for a keyed random function. Our formal definition follows.

**Definition 1 (Non-trivial game).** *Let $\mathcal{F} : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a publicly available random function. Game $G$ is non-trivial if for all adversaries $A$ there exists a simulator $S$ and a negligible function* negl *such that*

$$\mathrm{negl}(n) \geq \Big| \Pr\left[\mathcal{F} \leftarrow RF_{k\times *,y}; K \xleftarrow{\$} \{0,1\}^k; G^{\mathcal{F}_K, A^K} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow RF_{k\times *,y}; K \xleftarrow{\$} \{0,1\}^k; G^{\mathcal{F}_K, S^{\mathcal{F}_K}} \to 1\right]\Big|.$$

*Where the probabilities are taken over random choice of $\mathcal{F}$, random selection of the key $K$ and random coins of $G$ and $A$ ($S$ in the second experiment). If $\mathcal{F}$ is a fixed input length (FIL) keyed random function ($\mathcal{F} : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^y$) then we say that $G$ is non-trivial for FIL hash functions.*

Note that the game $G_{CRF}$ defined in the Example 2 is non-trivial. The game $G_{CR}$ expects its oracle $H$ to be a hash function family, i.e. a function with two inputs $K$ and $M$. If we modify the game $G_{CR}$ so that it expects $H$ to be a function only with one input $K||M$ then $G_{CR}$ is also non-trivial.

*Example 3.* The following game $G_{keyGuess}$ is an example of a trivial game (i.e. a game which is not non-trivial). The game is parametrized by a hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$, from which a hash function $H_K$ is chosen uniformly randomly.

**Game** $G_{keyGuess}(H)$

$G_{keyGuess}$ has access to $H_K(\cdot)$ and adversary $A^K$ for randomly chosen key $K \xleftarrow{\$} \{0,1\}^k$.

1. query $A^K \to K'$
2. choose $M \xleftarrow{\$} \{0,1\}^m$ for some integer $m$.
3. if $H_K(M) = H_{K'}(M)$ return 1.
4. otherwise return 0.

There exists an adversary $A^K$ which finds the correct key for all functions $H_K$. The adversary $A^K$ asks its oracle for the key $K$ and outputs the same. Hence, $A^K$ wins $G_{keyGuess}(\mathcal{F})$ for random function $\mathcal{F}$ and thus violates the first statement from the Definition 1.

## 3 The Black-box Property

Let $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family, $G$ be a game, $A$ an adversary and $S$ a simulator. We define the following experiment:

**Experiment** $\mathrm{HashBB}(H, G, A, S)$

1. choose $K \xleftarrow{\$} \{0,1\}^k$
2. run $G^{H_K, A^K} \to b$
3. run $G^{H_K, S^{H_K}} \to b'$
4. if $b \neq b'$ return 1
5. otherwise return 0

**Definition 2 (Black-box property).** *We say that the hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ has the black-box property if for all non-trivial games $G$, all adversaries $A$ there exist a polynomial simulator $S$ and a negligible function* negl*, such that*

$$\Pr\left[\mathrm{HashBB}(H, G, A, S) = 1\right] \leq \mathrm{negl}(n).$$

*Remark 1.* Informally, if a hash function family $H$ has the black-box property, everything "non-trivial" we are able to compute having access to the randomly chosen key $K$, we are able to compute only with oracle access to the hash function $H_K$.

There exist hash function families, which have the black-box property "trivially". Let $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family and let $H'$ be defined as:

$$H'_K(M) = \begin{cases} K & \text{if } M = 0 \\ H_K(M) & \text{otherwise} \end{cases}$$

Hence, a simulator $S^{H_K}$ can query $H_K(0)$ and it receives the key $K$. If $S$ knows the key $K$, it can simulate an adversary $A$ and thus it can compute the same as $A^K$ can. Therefore the black-box property alone is not enough for "strong" cryptographic hash function family.

*Pseudo-randomness.* A hash function family is pseudo-random, if a randomly chosen hash function from the family is indistinguishable from the random function. More formally, let $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family and let

$$\mathbf{Adv}^{\mathrm{Prf}}_H(A) := \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; A^{H_K} \to 1\right] - \Pr\left[\mathcal{F} \xleftarrow{\$} \mathrm{RF}_{*,y}; A^{\mathcal{F}} \to 1\right] \right|$$

We say that the hash function family $H$ is a pseudo-random function (Prf), if for all adversaries $A$ there exists a negligible function negl, such that

$$\mathbf{Adv}^{\mathrm{Prf}}_H(A) \leq \mathrm{negl}(n).$$

**Definition 3.** *We say that a hash function family $H$ is Prf-BB if it is a pseudo-random function and has the black-box property.*

*Remark 2.* It remains an open problem, whether Prf-BB hash function family exists. However, for the existence of a Prf-BB hash function family it is crucial that games like the key guessing game $G_{keyGuess}$ defined in the Example 3 are not non-trivial. If games, which can be won only by "simple utilization" of knowledge of the key $K$ (e.g. $G_{keyGuess}$), would be non-trivial, then no hash function family with black-box property could be pseudo-random. Let $H$ be hash function family with the black-box property and assume that $G_{keyGuess}$ is non-trivial. Since $H$ has the black-box property for all adversaries $A$ there exists a simulator $S$ such that for a randomly chosen key $K$ with a non-negligible probability holds

$$G^{H_K,A^K}_{keyGuess} = G^{H_K,S^{H_K}}_{keyGuess}.$$

However, there exists an adversary $A^K$ which wins the game $G^{H_K,A^K}_{keyGuess}$ for all keys $K$ (it just outputs the key it has as an oracle). Hence there exists a simulator $S^{H_K}$ which wins the game $G^{H_K,S^{H_K}}_{keyGuess}$ with non-negligible probability. But then, the algorithm $D := G^{H_K,S^{H_K}}_{keyGuess}$ can distinguish $H_K$ from a random function. What means that $H$ cannot be pseudo-random.

In the following theorem we show, that a randomly chosen hash function $H_K$ from the Prf-BB hash function family is as resistant as the random oracle to all types of attacks which can be represented by a non-trivial game $G^{H_K}$.

**Theorem 1.** *Let $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a Prf-BB hash function family and $G$ be a non-trivial game. Then for all adversaries $A$ there exists a polynomial simulator $S$ a negligible function* negl *such that*

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1\right] - \Pr\left[\mathcal{F} \xleftarrow{\$} \mathrm{RF}_{*,y}; G^{\mathcal{F}, S^{\mathcal{F}}} \to 1\right]\right| \leq \mathrm{negl}(n).$$

*Proof.* Fix some adversary $A$ and let

$$\varepsilon(n) := \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1].$$

Let $S$ be some polynomial simulator.

$$\begin{aligned}
\varepsilon(n) &= \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1 \wedge G^{H_K, S^{H_K}} \to 0] \\
&\quad + \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1 \wedge G^{H_K, S^{H_K}} \to 1] \\
&\leq \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1 \wedge G^{H_K, S^{H_K}} \to 0] \\
&\quad + \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1] \\
&\leq \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to b \wedge G^{H_K, S^{H_K}} \to b' \wedge b \neq b'] \\
&\quad + \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1].
\end{aligned}$$

Since $H$ has the black-box property, there exists a simulator $S$ and a negligible function $\mathrm{negl}_0$ such that

$$\varepsilon(n) \leq \mathrm{negl}_0(n) + \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1]. \tag{1}$$

The hash function family $H$ is pseudo-random, hence for all adversaries $D$ there exists a negligible function $\mathrm{negl}_1$, such that

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; D^{H_K} \to 1] - \Pr\left[\mathcal{F} \xleftarrow{\$} \mathrm{RF}_{*,y}; D^{\mathcal{F}} \to 1\right]\right| \leq \mathrm{negl}_1(n).$$

The statement above holds also for the adversary $D^{\mathcal{X}}$, which simulates $G^{\mathcal{X}, S^{\mathcal{X}}}$, where $\mathcal{X}$ is an arbitrary ITM. Thus

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1] - \Pr\left[\mathcal{F} \xleftarrow{\$} \mathrm{RF}_{*,y}; G^{\mathcal{F}, S^{\mathcal{F}}} \to 1\right]\right| \leq \mathrm{negl}_1(n).$$

Hence,

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, A^K} \to 1\right] - \Pr\left[\mathcal{F} \xleftarrow{\$} \mathrm{RF}_{*,y}; G^{\mathcal{F}, S^{\mathcal{F}}} \to 1\right]\right| \leq \mathrm{negl}_0(n) + \mathrm{negl}_1(n).$$

□

## 4 Merkle-Damgård and the Black-box Property

In this section we show that the well known Merkle-Damgård domain extension transform does not preserve the black-box property.

*Merkle-Damgård construction.* The strengthened Merkle-Damgård (SMD) domain extension transform operates in the following way (see fig. 1).

**Algorithm SMD$^f(K, M)$**
the algorithm has oracle access to $f : \{0,1\}^k \times \{0,1\}^y \times \{0,1\}^d \to \{0,1\}^y$.

1. $(M_1, \ldots, M_l) \xleftarrow{d} M$
2. $M_{l+1} \leftarrow \langle |M| \rangle_d$
3. $Y_0 \leftarrow IV$
4. **for** $i = 1$ **to** $l + 1$ **do**
5. $\quad Y_i \leftarrow f_K(Y_{i-1}, m_i)$
6. **return** $Y_{l'}$

By SMD$^f$ we denote the hash function family created by the SMD domain extension transform from the compression function $f : \{0,1\}^k \times \{0,1\}^d \times \{0,1\}^y \to \{0,1\}^y$. We often write $\text{SMD}^f_K(\cdot)$ instead of $\text{SMD}^f(K, \cdot)$. If $g : \{0,1\}^d \times \{0,1\}^y \to \{0,1\}^y$ is an unkeyed compression function, then SMD$^g$ denotes a hash function created by the unkeyed SMD construction.

Note that SMD$^f$ as defined above can process messages only of length up to $2^d$ bits. We can modify the algorithm SMD$^f$ so that it can process messages of arbitrary length (we just need to parse $|M|$ into several blocks, if needed). In the rest of this section we will assume that SMD$^f$ can process messages of arbitrary length, but to simplify the presentation we consider that processed messages are of length at most $2^d$ bits.

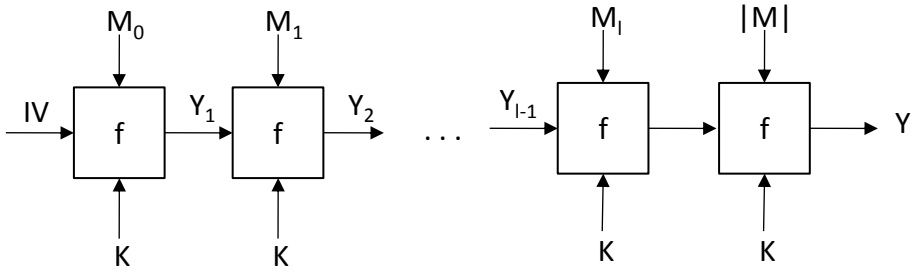


**Fig. 1.** Merkle-Damgård domain extension transform

**Theorem 2.** *Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \to \{0,1\}^y$ be a compression function, which is Prf-BB. Then the hash function family* SMD$^f : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ *does not have the black-box property.*

*Proof.* We utilize the idea of the extension attack [6, 8]. Let $G$ be the following game:

**Game** $G$
$G$ has access to $H_K(\cdot)$ and adversary $B(\cdot)$

1. choose $M \xleftarrow{\$} \{0,1\}^m$
2. query $H_K(M) \to Y$
3. query $B(Y) \to (X, Y')$
4. if $H_K(M||X) = Y'$ return 1

5. otherwise return 0.

Clearly such a game $G$ is non-trivial. We show that there exists an adversary $A^K$ that wins the game $G$ for $\mathrm{SMD}_K^f(\cdot)$. Moreover we show that no polynomial simulator $S^{\mathrm{SMD}_K^f(\cdot)}$ can win the game $G$ with non-negligible probability. Consider the following $A$

**Adversary** $A^K(Y)$
$A$ has access to the key $K$
1. Choose $X \xleftarrow{\$} \{0,1\}^d$
2. Compute $\mathrm{SMD}^f_{[IV:=Y]}(K, \langle |M| \rangle_d) || X) \rightarrow Y'$
3. Output $Y'$

Clearly, $A$ runs in a polynomial time and always wins the game $G$ for $\mathrm{SMD}^f$. Let $S$ be a simulator and let

$$\varepsilon(n) := \Pr\left[G^{\mathrm{SMD}_K^f, S^{\mathrm{SMD}_K^f}} \rightarrow 1\right].$$

Consider the following adversary $D$ attacking pseudo-randomness of $\mathrm{SMD}^f$:

**Adversary** $D$
$D$ has access to oracle $O$, which is either $\mathrm{SMD}_K^f(\cdot)$ or a random function $\mathcal{F}$.
1. choose $M \xleftarrow{\$} \{0,1\}^m$
2. query $O(M) \rightarrow Y$
3. simulate $S^O(Y) \rightarrow (X, Y')$
4. if $O(M||X) = Y'$ return 1
5. otherwise return 0.

Consider that $D$'s oracle is $\mathrm{SMD}_K^f(\cdot)$. In this case $S$'s view is the same as in the game $G$, hence

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; D^{\mathrm{SMD}_K^f(\cdot)} \rightarrow 1\right] = \varepsilon(n).$$

On the other hand, if $D$'s oracle is the random function $\mathcal{F}$, then it returns 1 only with negligible probability. The simulator $S^{\mathcal{F}}$ does not know the message $M$, hence the only chance $S^{\mathcal{F}}(Y)$ returns $(X, Y')$ for which $\mathcal{F}(M||X) = Y'$ is that it guesses $M$ or $Y'$. The probability that $S$ correctly guesses $M$ is $O(\frac{1}{2^m})$ and the probability that $S$ correctly guesses $Y'$ is $\mathcal{O}(\frac{1}{2^y})$. Thus,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SMD}^f}(D) = \varepsilon(n) - \mathcal{O}\Big(\frac{1}{\min\{2^m, 2^y\}}\Big).$$

Since $\mathrm{SMD}^f$ is pseudo-random, it must hold that $\varepsilon(n)$ is negligible. □

## 5 HMAC is Prf-BB Preserving Domain Extension Transform

In this section we show that the HMAC domain extension transform (fig. 2) is Prf-BB preserving.

**Algorithm** $\mathbf{HMAC}^f(K, M)$
the algorithm has oracle access to $f : \{0,1\}^k \times \{0,1\}^y \times \{0,1\}^d \rightarrow \{0,1\}^y$.
1. $(M_1, \ldots, M_l) \xleftarrow{d} M$
2. $Y_0 \leftarrow IV_0$
3. **for** $i = 1$ **to** $l$ **do**

4. $Y_i \leftarrow f_K(Y_{i-1}, m_i)$
5. **if** $y < d$ **then** $Y' := Y_l || 0^{d-y}$
6. **else** $Y' := Y_l[0] || \ldots || Y_l[d]$
7. $Y \rightarrow f_K(IV_1, Y')$
8. **return** $Y$

By $\text{HMAC}^f$ we denote the hash function family created by the HMAC domain extension transform from the compression function $f : \{0,1\}^k \times \{0,1\}^d \times \{0,1\}^y \rightarrow \{0,1\}^y$. We often write $\text{HMAC}^f_K(\cdot)$ instead of $\text{HMAC}^f(K, \cdot)$. If $g : \{0,1\}^d \times \{0,1\}^y \rightarrow \{0,1\}^y$ is an unkeyed compression function, then $\text{HMAC}^g$ denotes a hash function created by the unkeyed HMAC construction.

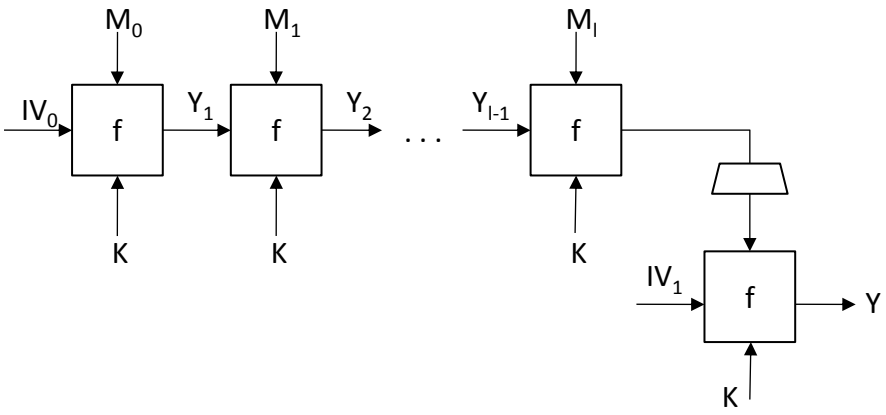


**Fig. 2.** HMAC domain extension transform

In the Lemma 1 we show that for a Prf compression function $f$, all games $G$ and all simulators $S$ there exists a simulator $S'$ such that $G$ cannot distinguish whether it is interacting with $\text{HMAC}^f_K$ and $S^{f_K}$ or $\text{HMAC}^f_K$ and $S'^{\text{HMAC}^f_K}$. In other words, if $f$ is pseudo-random then $S'$ is able to simulate $f_K$ using $\text{HMAC}^f_K$ for randomly chosen key $K \in \{0,1\}^k$.

**Lemma 1.** *Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \rightarrow \{0,1\}^y$ be a compression function which is Prf. Then for all games $G$ and all simulators $S$ there exists a simulator $S'$ and a negligible function* $\text{negl}(n)$ *such that*

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\text{HMAC}^f_K, S^{f_K}} \rightarrow 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\text{HMAC}^f_K, S'^{\text{HMAC}^f_K}} \rightarrow 1] \right| \leq \text{negl}(n)$$

*Proof.* Fix some simulator $S$ and let

$$\varepsilon(n) := \left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\text{HMAC}^f_K, S^{f_K}} \rightarrow 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\text{HMAC}^f_K, S'^{\text{HMAC}^f_K}} \rightarrow 1] \right|$$

Hence,

$$\varepsilon(n) \leq \Big|\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S^g} \to 1]\Big|$$
$$+\Big|\Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S^g} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S'^{\mathrm{HMAC}^g}} \to 1]\Big|$$
$$+\Big|\Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S'^{\mathrm{HMAC}^g}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big|$$

We show that all three terms on the right-hand side of the equation above are negligible. Thus, we want to prove the following three statements.

(1) For all simulators $S$ there exists a negligible function $\mathrm{negl}_1$ such that

$$\Big|\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S^g} \to 1]\Big| \leq \mathrm{negl}_1(n)$$

(2) For all simulators $S$ there exists a simulator $S'$ and a negligible function $\mathrm{negl}_2$ such that

$$\Big|\Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S^g} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S'^{\mathrm{HMAC}^g}} \to 1]\Big| \leq \mathrm{negl}_2(n)$$

(3) For all simulators $S'$ there exists a negligible function $\mathrm{negl}_3$ such that

$$\Big|\Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S'^{\mathrm{HMAC}^g}} \to 1] -$$
$$-\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big| \leq \mathrm{negl}_3(n)$$

Statements (1) and (3) are given by the fact that $f$ is pseudo-random. For the case (1) we create a distinguisher $D^X$, which simulates $G^{\mathrm{HMAC}^X, S^X}$. Since $f$ is pseudo-random, there exists a negligible function $\mathrm{negl}_1$ such that

$$\big|\Pr[K \xleftarrow{\$} \{0,1\}^k; D^{f_K} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; D^g \to 1]\big| \leq \mathrm{negl}_1(n).$$

However $D^X$ simulates $G^{\mathrm{HMAC}^X, S^X}$, hence

$$\Big|\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{\mathrm{HMAC}^g, S^g} \to 1]\Big| \leq \mathrm{negl}_1(n)$$

Similarly we can prove the statement (3).
For the statement (2) fix some simulator $S$ and consider the following simulator $S'$.

**Simulator** $S'^{\mathrm{HMAC}^g}(w)$
$S'$ has oracle access to $\mathrm{HMAC}^g$ and takes on input some string $w$ ($w$ represents a query asked by $G$ to $S'$). Let $q$ be the maximum number of queries $S$ asks to $g$. $S'$ maintains a table $T$ of triples $(X, Y, Y')_0^q$. An entry $(X, Y, Y')_i$ means that $S$'s $i$-th query was $(X, Y)$ and $S'$ responded $Y'$. $S'$ also maintains a "chain" list $L$ of chains $(IV_0 \xrightarrow{X_0} Y_0 \xrightarrow{X_1} Y_1 \xrightarrow{X_2} \cdots \xrightarrow{X_{l_i}} Y_{l_i})_{i=0}^r$. An entry (chain) in the list means, that $S$ during its execution asked queries $\{(X_0, IV_0) \to Y_0, (X_1, Y_0) \to Y_1, \ldots, (X_{l_i}, Y_{l_i-1}) \to Y_{l_i}\}$ (queries need not to be asked in the same order).

1. **Simulate** $S^g(w) \to o$. When $S$ asks a query $(X, Y)$, search $T$ for entry $(X, Y, Y')$.

(a) If such an entry exists, answer $Y'$.
(b) Otherwise:
   i. If $Y \neq IV_0$ and $Y \neq IV_1$, chose $Y' \xleftarrow{\$} \{0,1\}^y$ and add $(X, Y, Y')$ to $T$. Check if $(X, Y)$ can be added to the end of some chain. If so, add $(X, Y)$ to the end of that chain. Answer $Y'$.
   ii. If $Y = IV_0$, choose $Y' \xleftarrow{\$} \{0,1\}^y$ and add $(X, Y, Y')$ to $T$, create a new chain $IV_0 \xrightarrow{X} Y'$) and add it to $L$. Answer $Y'$.
   iii. If $Y = IV_1$ search for a chain with the last entry $\xrightarrow{?} X$. If no such chain exists, choose $Y' \xleftarrow{\$} \{0,1\}^y$ and add $(X, Y, Y')$ to $T$.
   Otherwise let $IV_0 \xrightarrow{X_0} Y_0 \xrightarrow{X_1} \cdots \xrightarrow{X_{l_i-1}} Y_{l_i-1} \xrightarrow{X_{l_i}} X$ be the found chain. Query $Y' := \mathrm{HMAC}^g(X_0 || \ldots || X_{l_i})$, store $(X, Y, Y')$ into the table $T$ and answer $Y'$.
2. **Return** $o$

It is clear that $S'$ runs in a polynomial time. The view of $S$ in the simulation during execution of $S'^{\mathrm{HMAC}^g}$ ($g \leftarrow \mathrm{RF}_{y+d,y}$) is the same as in the case when $S^g$ is executed alone. Hence, the game $G$ can distinguish $\mathrm{HMAC}^g, S'^{\mathrm{HMAC}^g}$ from $\mathrm{HMAC}^g, S^g$ only if output of $S'^{\mathrm{HMAC}^g}$ is "inconsistent" with $G$'s first oracle $\mathrm{HMAC}^g$. Such inconsistency can occur only if $S'$ is unable to maintain all chains created by $S$ during its simulation. The simulator $S$ can create a chain which $S'$ cannot notice only if $S$ asks a query $(X, Y)$, gets respond $Z$ and it previously asked a query $(X', Y')$ with respond $Z'$ such that $(X', Y') \neq (X, Y)$ and either $Z = X'$ or $Z = Z'$. However the probability that such event occurs is $\mathrm{negl}_3(n) := \mathcal{O}(\frac{q^2}{2^y})$, where $q$ is the maximum number of queries $S$ asks its oracle.
By combining statements (1), (2) and (3) we conclude that

$$\varepsilon(n) \leq \mathrm{negl}_1(n) + \mathrm{negl}_2(n) + \mathrm{negl}_3(n).$$

□

**Theorem 3.** *Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \to \{0,1\}^y$ be a compression function, which is Prf-BB. Then $HMAC^f : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ is Prf-BB.*

*Proof.* Let $f : \{0,1\}^k \times \{0,1\}^d \times \{0,1\}^y \to \{0,1\}^y$ be a compression function which is Prf-BB and $\mathrm{HMAC}^f : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family created by the HMAC construction from $f$. We want to show that $HMAC^f$ is Prf-BB too. Since $f$ has black-box property there exists a negligible function $\mathrm{negl}_0(n)$, such that

$$(\forall \text{non-trivial } G)(\forall A)(\exists S)\, \Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{f_K, A^K} \to b \wedge G^{f_K, S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}_0(n). \tag{2}$$

Let $G$ be some non-trivial game and $A$ some adversary. We want to show that there exists a simulator $S$ and a negligible function $\mathrm{negl}_1$ such that

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{\mathrm{HMAC}_K^f, A^K} \to b \wedge G^{\mathrm{HMAC}_K^f, S^{\mathrm{HMAC}_K^f}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}_1(n). \tag{3}$$

Consider the game $G'^{f_K, X}$, which simulates $G^{\mathrm{HMAC}_K^f, X}$. When $G$ asks its first oracle $\mathrm{HMAC}_K^f$ a query $M$, then $G'$ computes $Y = \mathrm{HMAC}_K^f(M)$ and answers $Y$. Since $G'$ is able to simulate $\mathrm{HMAC}_K^f$ using its oracle $f_K$, it is clear that for all ITMs $X$ and all keys $K \in \{0,1\}^k$ is

$$\Pr[G^{\mathrm{HMAC}_K^f, X} \to 1] = \Pr[G'^{f_K, X} \to 1].$$

It is also clear that $G'$ is non-trivial too. Using the equation (2) we have that there exists a simulator $S$ such that

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G'^{f_K, A^K} \to b \wedge G'^{f_K, S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}_0(n).$$

However $G^{\mathrm{HMAC}^f_K, X}$ and $G'^{f_K, X}$ do the same. Thus

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{\mathrm{HMAC}^f_K, A^K} \to b \wedge G^{\mathrm{HMAC}^f_K, S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}_0(n). \tag{4}$$

By the Lemma 1 for the simulator $S$ there exists a simulator $S'$ and a negligible function $\mathrm{negl}_2$ such that

$$\begin{aligned}
\mathrm{negl}_2(n) \geq \Big| & \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] \\
& - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big| \\
= \Big| & \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] \\
& - \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big|
\end{aligned}$$

$$\begin{aligned}
\mathrm{negl}_2(n) \geq \Big| & \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{\mathrm{HMAC}^f_K, A^K} \to 0] \cdot \Pr[G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] \\
& - \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{\mathrm{HMAC}^f_K, A^K} \to 0] \cdot \Pr[G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big| \qquad (5) \\
= \Big| & \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to 0 \wedge G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1] \\
& - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to 0 \wedge G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 1]\Big|, \qquad (6)
\end{aligned}$$

where the inequality (5) is given by the fact that $0 \leq \Pr[G^{\mathrm{HMAC}^f_K, A^K} \to 0] \leq 1$ (for all games $G$ and all adversaries $A$). The equation (6) holds, because the events $G^{\mathrm{HMAC}^f_K, A^K} \to 0$ and $G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1$ or $G^{\mathrm{HMAC}^f_K, A^K} \to 0$ and $G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 1$ are independent for some fixed key $K$ (since in both simulations $G$, $A$ and $S$ use fresh new random coins). Similarly we can prove the following inequality

$$\begin{aligned}
\mathrm{negl}_2(n) \geq \Big| & \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to 1 \wedge G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to 0] \\
& - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to 1 \wedge G^{\mathrm{HMAC}^f_K, S^{f_K}} \to 0]\Big|.
\end{aligned}$$

Hence,

$$\begin{aligned}
2 \cdot \mathrm{negl}_2(n) \geq \Big| & \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to b \wedge G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to b' \wedge b \neq b'] \\
& - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to b \wedge G^{\mathrm{HMAC}^f_K, S^{f_K}} \to b' \wedge b \neq b']\Big|. \qquad (7)
\end{aligned}$$

By the equation (4) the second term of the equation (7) is negligible:

$$2 \cdot \mathrm{negl}_2(n) \geq \Big| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to b \wedge G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to b' \wedge b \neq b'] - \mathrm{negl}_0(n) \Big|.$$

Thus,

$$2 \cdot \mathrm{negl}_2(n) + \mathrm{negl}_0(n) \geq \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{\mathrm{HMAC}^f_K, A^K} \to b \wedge G^{\mathrm{HMAC}^f_K, S'^{\mathrm{HMAC}^f_K}} \to b' \wedge b \neq b'].$$

For the proof that $\mathrm{HMAC}^f$ is pseudo-random if $f$ is pseudo-random see [2]. □

## 6 Prf-BB and Pseudo-random Oracle

*Pseudo-random oracle.* Pseudo-random oracle [2, 3, 6] is a property of cryptographic hash functions based on the indifferentiability framework introduced by Maurer, Renner and Holenstein [9]. A hash function $F^g : \{0,1\}^* \to \{0,1\}^y$ based on an ideal compression function $g$ is pseudo-random oracle if it is indifferentiable from a random oracle. More formally, let

$$\mathbf{Adv}^{\mathrm{Pro}}_{F,S}(A) := \Big| \Pr\Big[g \leftarrow \mathrm{RF}_{y+d,y}; A^{F^g, g} \to 1\Big] - \Pr\Big[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; A^{\mathcal{F}, \mathcal{S}^{\mathcal{F}}} \to 1\Big] \Big|$$

We say that a hash function $F^g : \{0,1\}^* \to \{0,1\}^y$ based on an ideal compression function $g$ is pseudo-random oracle if for all adversaries there exists a polynomial simulator $S$ and a negligible function negl such that

$$\mathbf{Adv}^{\mathrm{Pro}}_{F,S}(A) \leq \mathrm{negl}(n).$$

The pseudo-random oracle property (Pro) is meaningful only in the random-oracle model. Since $F$ is based on an "uncertain" random compression function $g$, the Pro is rather a property of domain extension transforms. We say that $F$ is Pro preserving domain extension transform if $F^g$ is Pro. Thus $F$ securely extends the domain of the fixed-input length random oracle $g$ to the variable-input length pseudo-random oracle. This is also the reason why we do not define the pseudo-random oracle property for hash function families. Given a domain extension transform $F^g : \{0,1\}^* \to \{0,1\}^y$ we can construct a hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ by replacing $g$ with a keyed compression function $f_K$. However, if $f_K$ is not random, the security of the resulting hash function family is uncertain [3]. In this section we show that every Pro preserving domain extension transform is also Prf-BB preserving and vice-versa. Hence Prf-BB can be seen as an equivalent to the Pro property in the standard model. We prove this equivalence in the following two theorems.

**Theorem 4.** *Let $F$ be a domain extension transform, which is Prf-BB preserving. Then $F$ is Pro preserving.*

*Proof.* Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \to \{0,1\}^y$ be a compression function which is Prf-BB, $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ be a hash function family such that $H_K(M) := F^{f_K}(M)$. Clearly, we just need to consider non-trivial games $G$ (there are no keys in the Pro experiments). Let $G$ be a non-trivial game.

We prove the following three statements:

(1) There exists a negligible function $\mathrm{negl}_0$ such that

$$\left| \Pr\left[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^g,g} \to 1\right] - \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 1\right] \right| \leq \mathrm{negl}_0(n).$$

Since $f$ is Prf, for all adversaries $A$ there exists a negligible function $\mathrm{negl}_0$ such that

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; A^{f_K} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; A^g \to 1] \right| \leq \mathrm{negl}_0(n) \tag{8}$$

If we substitute $A^X := G^{F^X,X}$ in the equation 8 we get the statement (1).

(2) There exists a negligible function $\mathrm{negl}_1$ and a simulator $S$ such that

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 1\right] - \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,S^{H_K}} \to 1\right] \right| \leq \mathrm{negl}_1(n).$$

Since the hash function family $H_K(M)$ has the black-box property, for all non-trivial games $G$ and all adversaries $A$ there exists a simulator $S$ and a negligible function $\mathrm{negl}_1$ such that

$$\begin{aligned}
\mathrm{negl}_1(n) &\geq \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,A^K} \to b \wedge G^{H_K,S^{H_K}} \to b' \wedge b \neq b'\right] \\
&= \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,A^K} \to 1 \wedge G^{H_K,S^{H_K}} \to 0\right] \\
&\quad + \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,A^K} \to 0 \wedge G^{H_K,S^{H_K}} \to 1\right]
\end{aligned}$$

An adversary $A^K$ can simulate $f_K$, since it knows the key. Thus for all games $G$ there exists a simulator $S$ such that

$$\begin{aligned}
\mathrm{negl}_1(n) &\geq \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 1 \wedge G^{H_K,S^{H_K}} \to 0\right] \\
&\quad + \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 0 \wedge G^{H_K,S^{H_K}} \to 1\right] \\
&\geq \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 1 \wedge G^{H_K,S^{H_K}} \to 0\right]
\end{aligned}$$

$$\begin{aligned}
\mathrm{negl}_1(n) &\geq \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr\left[G^{H_K,f_K} \to 1\right] \left(1 - \Pr\left[G^{H_K,S^{H_K}} \to 1\right]\right) \\
&= \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \left(\Pr\left[G^{H_K,f_K} \to 1\right] - \Pr\left[G^{H_K,f_K} \to 1\right] \Pr\left[G^{H_K,S^{H_K}} \to 1\right]\right) \\
&\geq \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \left(\Pr\left[G^{H_K,f_K} \to 1\right] - \Pr\left[G^{H_K,S^{H_K}} \to 1\right]\right) \\
&= \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,f_K} \to 1\right] - \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,S^{H_K}} \to 1\right]
\end{aligned}$$

(3) There exists a negligible function $\mathrm{negl}_2$ such that

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K,S^{H_K}} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F},S^{\mathcal{F}}} \to 1\right] \right| \leq \mathrm{negl}_2(n).$$

From the assumption that $F$ is Prf-BB preserving we know that the hash function family $H_K(M) := F^{f_K}(M)$ is Prf. Hence, for all adversaries $A$ there exists a negligible function $\text{negl}_2$ such that

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; A^{H_K} \to 1] - \Pr[\mathcal{F} \leftarrow \text{RF}_{*,y}; A^{\mathcal{F}} \to 1] \right| \leq \text{negl}_2(n) \tag{9}$$

If we substitute $A^X := G^{F^X, X}$ in the equation (9) we get the statement (3).

Hence, for all games $G$ there exists a simulator $S$ and a negligible functions $\text{negl}_0$, $\text{negl}_1$, $\text{negl}_2$, such that

$$\begin{aligned}
&\left| \Pr\left[g \leftarrow \text{RF}_{y+d,y}; G^{F^g, g} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \text{RF}_{*,y}; G^{\mathcal{F}, S^{\mathcal{F}}} \to 1\right] \right| \leq \\
&\quad \leq \left| \Pr\left[g \leftarrow \text{RF}_{y+d,y}; G^{F^g, g} \to 1\right] - \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, f_K} \to 1\right] \right| \\
&\qquad + \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, f_K} \to 1\right] - \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1\right] \right| \\
&\qquad + \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; G^{H_K, S^{H_K}} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \text{RF}_{*,y}; G^{\mathcal{F}, S^{\mathcal{F}}} \to 1\right] \right| \\
&\quad \leq \text{negl}_0(n) + \text{negl}_1(n) + \text{negl}_2(n).
\end{aligned}$$

Thus, $F$ is Pro preserving. □

**Theorem 5.** *Let $F$ be a domain extension transform, which is Pro preserving. Then $F$ is Prf-BB preserving.*

The proof of this theorem is similar to the proof of the Theorem 3. In the Lemma 2 we prove that a hash function family $H(K, M) := F^{f_K}(M)$ is pseudo-random if the compression function $f$ is pseudo-random. In the Lemma 3 (generalization of the Lemma 1) we show that for a Prf compression function $f$, all games $G$ and all simulators $S$ there exists a simulator $S'$ such that $S'$ is able to simulate $S^{f_K}$ using $F_K^f$ for randomly chosen key $K \in \{0,1\}^k$. We utilize the Lemma 3 to prove that the hash function family $H$ has black-box property if $f$ is Prf-BB.

**Lemma 2.** *Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \to \{0,1\}^y$ be a compression function which is Prf and let $F$ be a Pro preserving domain extension transform. Then a hash function family $H(K, M) := F^{f_K}(M)$ is Prf, i.e. for all adversaries $A$ there exists a negligible function* negl *such that*

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; A^{H_K} \to 1\right] - \Pr\left[\mathcal{F} \xleftarrow{\$} \text{RF}_{*,y}; A^{\mathcal{F}} \to 1\right] \right| \leq \text{negl}(n).$$

*Proof.* The domain extension transform $F$ is Pro preserving, hence for all adversaries $A$ there exists a simulator $S$ and negligible function $\text{negl}_0$ such that

$$\left| \Pr\left[g \leftarrow \text{RF}_{y+d,y}; A^{F^g, g} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \text{RF}_{*,y}; A^{\mathcal{F}, \mathcal{S}^{\mathcal{F}}} \to 1\right] \right| \leq \text{negl}_0(n).$$

The statement above holds also for adversaries $A'$ which "ignore" their second oracle. Hence, for all adversaries $A'$ there exists a negligible function $\text{negl}_0$ such that

$$\left| \Pr\left[g \leftarrow \text{RF}_{y+d,y}; A'^{F^g} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \text{RF}_{*,y}; A'^{\mathcal{F}} \to 1\right] \right| \leq \text{negl}_0(n). \tag{10}$$

The compression function $f$ is Prf, hence for all adversaries $D$ there exists a negligible function $\mathrm{negl}_1$ such that

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; D^{f_K} \to 1\right] - \Pr\left[g \xleftarrow{\$} \mathrm{RF}_{y+d,y}; D^{g} \to 1\right] \right| \leq \mathrm{negl}_1(n).$$

The statement above holds also for adversaries of the form $D := A'^F$, where $A'$ is an arbitrary adversary. Therefore for all adversaries $A'$ there exists a negligible function $\mathrm{negl}_1$ such that

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; A'^{F^{f_K}} \to 1\right] - \Pr\left[g \xleftarrow{\$} \mathrm{RF}_{y+d,y}; A'^{F^{g}} \to 1\right] \right| \leq \mathrm{negl}_1(n). \tag{11}$$

Finally, from the equations (10) and (11) we conclude that for all adversaries $A'$ there exists a negligible functions $\mathrm{negl}_0$ and $\mathrm{negl}_1$ such that

$$\left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k; A'^{F^{f_K}} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; A'^{\mathcal{F}} \to 1\right] \right| \leq \mathrm{negl}_0(n) + \mathrm{negl}_1(n).$$

□

**Lemma 3.** *Let $f : \{0,1\}^k \times \{0,1\}^{(y+d)} \to \{0,1\}^y$ be a compression function which is Prf-BB and let $F$ be a Pro preserving domain extension transform. Then for all games $G$ and all simulators $S$ there exists a simulator $S'$ and a negligible function* $\mathrm{negl}(n)$ *such that*

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S^{f_K}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S'^{F^{f_K}}} \to 1] \right| \leq \mathrm{negl}(n)$$

*Proof.* Fix some game $G$ and let

$$\begin{aligned}
\varepsilon(n) := & \left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S^{f_K}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S'^{F^{f_K}}} \to 1] \right| \\
\leq & \left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S^{f_K}} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^{g}, S^{g}} \to 1] \right| \\
& + \left| \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^{g}, S^{g}} \to 1] - \Pr[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F}, S'^{\mathcal{F}}} \to 1] \right| \\
& + \left| \Pr[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F}, S'^{\mathcal{F}}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S'^{F^{f_K}}} \to 1] \right|.
\end{aligned}$$

We prove the lemma in three steps.

(1) For all simulators $S$ there exists a negligible function $\mathrm{negl}_1$ such that

$$\left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S^{f_K}} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^{g}, S^{g}} \to 1] \right| \leq \mathrm{negl}_1(n).$$

(2) For all simulators $S$ there exists a simulator $S'$ and a negligible function $\mathrm{negl}_2$ such that

$$\left| \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^{g}, S^{g}} \to 1] - \Pr[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F}, S'^{\mathcal{F}}} \to 1] \right| \leq \mathrm{negl}_2(n).$$

(3) For all simulators $S'$ there exists a negligible function $\mathrm{negl}_3$ such that

$$\left| \Pr[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F}, S'^{\mathcal{F}}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K}, S'^{F^{f_K}}} \to 1] \right| \leq \mathrm{negl}_3(n).$$

The statement (1) is given by the fact that $f$ is pseudo-random. We create a distinguisher $D^X$, which simulates $G^{F^X,S^X}$. Since $f$ is pseudo-random, there exists a negligible function $\mathrm{negl}_1$ such that

$$\left|\Pr[K \xleftarrow{\$} \{0,1\}^k; D^{f_K} \to 1] - \Pr[g \leftarrow \mathrm{RF}_{y+d,y}; D^g \to 1]\right| \leq \mathrm{negl}_1(n).$$

However $D^X$ simulates $G^{F^X,S^X}$, hence the statement (1) holds. Similarly we can prove the statement (3), where we utilize the Lemma 2 which states that $F^{f_K}$ is pseudo-random.

The statement (2) is given by the fact, that $F$ is Pro preserving. Hence, for all adversaries $A$ there exists a simulator $S''$ and a negligible function $\mathrm{negl}_2$ such that

$$\left|\Pr\left[g \leftarrow \mathrm{RF}_{y+d,y}; A^{F^g,g} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; A^{\mathcal{F},\mathcal{S}''^{\mathcal{F}}} \to 1\right]\right| \leq \mathrm{negl}_2(n)$$

Now fix some simulator $S$, the statement above must hold also for all adversaries of the form $A^{O_1,O_2} := G^{O_1,S^{O_2}}$, where $G$ is an arbitrary game. Hence,

$$\left|\Pr\left[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^g,S^g} \to 1\right] - \Pr\left[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F},S^{\mathcal{S}''^{\mathcal{F}}}} \to 1\right]\right| \leq \mathrm{negl}_2(n).$$

By a simple substitution $S'^{\mathcal{F}} := S^{S''^{\mathcal{F}}}$ we get the statement (2)

$$\left|\Pr[g \leftarrow \mathrm{RF}_{y+d,y}; G^{F^g,S'^{F^g}} \to 1] - \Pr[\mathcal{F} \leftarrow \mathrm{RF}_{*,y}; G^{\mathcal{F},S^{\mathcal{F}}} \to 1]\right| \leq \mathrm{negl}_2(n).$$

By combining statements (1), (2) and (3) we have

$$\varepsilon(n) \leq \mathrm{negl}_1(n) + \mathrm{negl}_2(n) + \mathrm{negl}_3(n).$$

□

*Proof of the Theorem 5.* Let $f : \{0,1\}^k \times \{0,1\}^d \times \{0,1\}^y \to \{0,1\}^y$ be a compression function which is Prf-BB. We show that $F^{f_K}$ is Prf-BB. Since $f$ has black-box property there exists a negligible function $\mathrm{negl}(n)$ such that

$$(\forall \text{non-trivial } G)(\forall A)(\exists S)\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{f_K,A^K} \to b \wedge G^{f_K,S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}(n). \tag{12}$$

Let $G$ be some non-trivial game and $A$ some adversary. We want to show that there exists a simulator $S$ such that

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{F_K^f,A^K} \to b \wedge G^{F_K^f,S^{F_K^f}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}(n). \tag{13}$$

Consider the game $G'^{f_K,X}$, which simulates $G^{H_K,X}$. When $G$ asks its first oracle $H_K$ a query $M$, then $G'$ computes $Y = F_K^f(M)$ and answers $Y$. Since $G'$ is able to simulate $F_K^f$ using its oracle $f_K$, it is clear that for all ITMs $X$ and all keys $K \in \{0,1\}^k$ is

$$\Pr[G^{F_K^f,X} \to 1] = \Pr[G'^{f_K,X} \to 1].$$

It is also clear that $G'$ is non-trivial too. Using the equation (12) we have that there exists a simulator $S$ such that

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G'^{f_K,A^K} \to b \wedge G'^{f_K,S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}(n).$$

However $G^{F_K^f,X}$ and $G'^{f_K,X}$ do the same. Thus

$$\Pr\left[K \xleftarrow{\$} \{0,1\}^K; G^{F_K^f,A^K} \to b \wedge G^{F_K^f,S^{f_K}} \to b' \wedge b \neq b'\right] \leq \mathrm{negl}(n). \tag{14}$$

Now by the Lemma 3 for all simulators $S$ there exists a simulator $S'$ and a negligible function $\mathrm{negl}_0$ such that

$$\begin{aligned}
\mathrm{negl}_0(n) &\geq \left| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},S^{f_K}} \to 1] - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},S'^{F^{f_K}}} \to 1] \right| \\
&= \left| \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{F^{f_K},S^{f_K}} \to 1] - \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{F^{f_K},S'^{F^{f_K}}} \to 1] \right| \\
&\geq \Big| \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{F^{f_K},A^K} \to 0] \cdot \Pr[G^{F^{f_K},S^{f_K}} \to 1] \\
&\quad - \frac{1}{2^k} \sum_{K \in \{0,1\}^k} \Pr[G^{F^{f_K},A^K} \to 0] \cdot \Pr[G^{\mathcal{F}^{f_K},S'^{F^{f_K}}} \to 1] \Big| \qquad (15) \\
&= \Big| \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to 0 \wedge G^{F^{f_K},S^{f_K}} \to 1] \\
&\quad - \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to 0 \wedge G^{F^{f_K},S'^{F^{f_K}}} \to 1] \Big|, \qquad (16)
\end{aligned}$$

where the inequality (15) is given by the fact that $0 \leq \Pr[G^{F^{f_K},A^K} \to 0] \leq 1$ (for all games $G$ and all adversaries $A$). The equation (16) holds, because the events $G^{F^{f_K},A^K} \to 0$ and $G^{F^{f_K},S^{f_K}} \to 1$ or $G^{F^{f_K},A^K} \to 0$ and $G^{F^{f_K},S^{f_K}} \to 1$ are independent for some fixed key $K$. Similarly we can prove the following inequality

$$\begin{aligned}
\mathrm{negl}_0(n) \geq \Big| &\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to 1 \wedge G^{F^{f_K},S'^{F^{f_K}}} \to 0] \\
&- \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to 1 \wedge G^{F^{f_K},S^{f_K}} \to 0] \Big|. \qquad (17)
\end{aligned}$$

Hence,

$$\begin{aligned}
2 \cdot \mathrm{negl}_0(n) \geq \Big| &\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to b \wedge G^{F^{f_K},S'^{F^{f_K}}} \to b' \wedge b \neq b'] \\
&- \Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to b \wedge G^{F^{f_K},S^{f_K}} \to b' \wedge b \neq b'] \Big|. \qquad (18)
\end{aligned}$$

By the inequality (12) we know that the second term of the inequality (18) is negligible, hence

$$\begin{aligned}
2 \cdot \mathrm{negl}_0(n) \geq \Big| &\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to b \wedge G^{F^{f_K},S'^{F^{f_K}}} \to b' \wedge b \neq b'] \\
&- \mathrm{negl}(n) \Big|. \qquad (19)
\end{aligned}$$

Thus,

$$\Pr[K \xleftarrow{\$} \{0,1\}^k; G^{F^{f_K},A^K} \to b \wedge G^{F^{f_K},S'^{F^{f_K}}} \to b' \wedge b \neq b'] \leq 2 \cdot \mathrm{negl}_0(n) + \mathrm{negl}(n),$$

The fact that $F^{f_K}$ is Prf is proved in the Lemma 2.

## 7 Conclusion

In this paper we introduced the black-box property for hash function families, which guarantees that for a hash function family $H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$ everything "non-trivial" we are able to compute with access to a randomly chosen key $K$ is possible to compute only with oracle access to the hash function $H_K$. We showed that a pseudo-random hash function family with black-box property (Prf-BB) is resistant to all "non-trivial" types of attack. We proved that the Merkle-Damgård construction is not Prf-BB preserving and conversely that the HMAC construction is Prf-BB preserving. Moreover we proved that every pseudo-random oracle preserving domain extension transform is Prf-BB preserving and vice-versa.

We believe that a Prf-BB property is all-in-one property – it guarantees "total" security of a hash function family and should be a primary security goal for designers of hash functions.

A natural and interesting question is whether a Prf-BB hash function family exists. A combination of two hash function families $H(K_1, K_2, M) := H_1(K_1, H_2(K_2, M))$, where $H_1$ is pseudo-random and $H_2$ is collision resistant seems to be a good candidate. The collision resistant hash function family $H_2$ ensures that a potential adversary $A$ is unable to arbitrarily select inputs to the pseudo-random hash function family $H_1$. Hence $H_2$ minimizes adversary's ability to utilize the key $K_1$. The pseudo-randomness of $H_1$ guarantees that the output of $H_1$ has random behavior and hides possible "non-random" behavior of $H_2$.

## References


1. M. Bellare, R. Canneti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In *Advances in Cryptology – Crypto 96, LNCS vol. 1109*, pages 1–15. Springer, 1996.
2. M. Bellare and T. Ristenpart. Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms. In *International Colloquim on Automata, Languages, and Progamming, LNCS vol. 4596*, pages 399–410. Springer, 2006.
3. M. Bellare and T. Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In *Advances in Cryptology - ASIACRYPT 2006, LNCS vol. 4284*, pages 299–314. Springer, 2006.
4. M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.
5. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Journal of the ACM, vol. 51, issue 4*, pages 557–594. ACM, 2004.
6. J.S. Coron, Y. Dodis, C. Malinaud, and P. Puniya. Merkle-Damgård Revisited: How to Construct a Hash Function. In *Advances in Cryptology – CRYPTO 2005, LNCS vol. 3621*, pages 430–448. Springer, 2005.
7. I. Damgard. A design principle for hash functions. In *Advances in Cryptology – CRYPTO 89, LNCS vol. 435*, pages 416–427. Springer, 1989.
8. Y. Dodis, T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In *Advances in Cryptology - EUROCRYPT 09, LNCS vol. 5479*, pages 371–388. Springer, 2009.
9. U. Maurer, R. Renner, and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In *Theory of Cryptography, LNCS vol. 2951*, pages 21–39. Springer, 2004.
10. R. Merkle. One way hash functions and DES. In *Advances in Cryptology – CRYPTO 89, LNCS vol. 435*, pages 428–446. Springer, 1989.
11. P. Rogaway and T. Shrimpton. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In *Fast Software Encryption, LNCS vol. 3017*, pages 371–388. Springer, 2004.