

A Tweak for a PRF Mode of a Compression Function and Its Applications

Shoichi Hirose¹ and Atsushi Yabumoto²

¹ Faculty of Engineering, University of Fukui, Japan
hrs_shch@u-fukui.ac.jp

² Graduate School of Engineering, University of Fukui, Japan

Abstract. We discuss a tweak for the domain extension called Merkle-Damgård with Permutation (MDP), which was presented at ASIACRYPT 2007. We first show that MDP may produce multiple independent pseudorandom functions (PRFs) using a single secret key and multiple permutations if the underlying compression function is a PRF against related-key attacks with respect to the permutations. Using this result, we then construct a hash-function-based MAC function, which we call FMAC, using a compression function as its underlying primitive. We also present a scheme to extend FMAC so as to take as input a vector of strings.

Keywords: Compression function, MAC, Pseudorandom function, Vector-input PRF

1 Introduction

Background. HMAC [3] is the widely deployed function for message authentication (MAC function) constructed from a cryptographic hash function. HMAC is defined with a hash function H as follows:

$$\text{HMAC}(K, M) = H((K \oplus \text{opad}) \| H((K \oplus \text{ipad}) \| M)) ,$$

where K is a secret key, M is an input message, $\|$ represents concatenation, \oplus represents bitwise XOR, $\text{ipad} = 0\text{x}3636 \cdots 36$ and $\text{opad} = 0\text{x}5c5c \cdots 5c$. It is also depicted in Fig. 1.

Due to the length extension property of standardized hash functions such as SHA-1, SHA-256 and SHA-512 [17], HMAC invokes the underlying hash function twice. The drawback of the adoption of this structure is inefficiency for short messages. Inefficiency of HMAC may also come from the padding of the underlying hash function based on the Merkle-Damgård strengthening. More efficient scheme is expected to be constructed if a compression function of a hash function is used as an underlying primitive instead of the hash function itself.

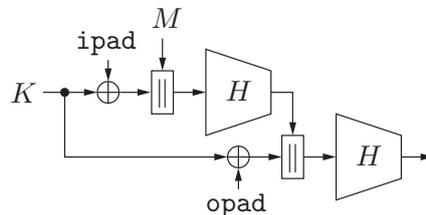


Fig. 1: HMAC. H is a cryptographic hash function. K is a secret key. M is an input message. \oplus represents bitwise XOR operation. $\|$ represents concatenation of sequences. $\text{ipad} = 0\text{x}3636 \cdots 36$ and $\text{opad} = 0\text{x}5c5c \cdots 5c$.

Recently, an approach attracts a lot of interest to construct symmetric-key schemes using a public permutation. It is emerged from the sponge construction [10], which is the basis of the

SHA-3 hash function [18]. Following the approach, methods to construct authenticated encryption schemes and pseudorandom generators are proposed [11]. The Even-Mansour cipher [15, 16], which is constructed from a public permutation, also attracts renewed interest, and schemes for encryption, message authentication and authenticated encryption are proposed based on it [22, 23, 25, 31]. Chaskey is a recently proposed MAC function based on a permutation [27].

The approach to construct secret-key schemes using a compression function is not new. The plain Merkle-Damgård cascade is shown to be a PRF against adversaries making prefix-free queries if the underlying compression function is a PRF [4]. In the context of multi-property preservation [7], some schemes are proposed such as EMD (Enveloped MD) [7] and MDP [19], which may produce PRFs with some appropriate keying strategies. The recent proposal OMD (Offset Merkle-Damgård) [14] for authenticated encryption is constructed with a compression function.

Our Contribution. This paper extends the MDP domain extension [19] to construct efficient pseudorandom functions (PRFs). It is first shown that the MDP domain extension with a single key and multiple permutations may produce multiple independent PRFs if the underlying compression function is PRF against related-key attacks with respect to the permutations. Based on this result, a PRF with minimum padding is proposed, which is called FMAC (compression-Function-based MAC). We say that padding is minimum if the produced message blocks does not include message blocks only with the padding sequence for any non-empty input message. Finally, a vector-input PRF is constructed with FMAC, which is called vFMAC. A vector-input PRF (vPRF) takes as input a vector of strings. For vFMAC, the number of the components in an input vector is bounded from above and the upper bound is determined by the number of the permutations used in vFMAC.

Related Work. It is shown that HMAC is a PRF if the compression function of the underlying hash function is a PRF with respect to two keying strategies [1]. In particular, for one of the keying strategies, the compression function is required to be a PRF against related-key attacks with respect to `ipad` and `opad`.

Yasuda [36] presented a secure HMAC variant without the second key, which is called H^2 -MAC. It is shown to be a PRF on the assumption that the underlying compression function is a PRF even if an adversary is allowed to obtain a piece of information on the secret key.

AMAC [2] is a MAC function using a hash function encapsulated with an unkeyed output function. Typical candidates for the output function are truncation and the mod function. AMAC is more efficient than HMAC especially for short messages. It is shown that AMAC is a PRF if the underlying compression function remains a PRF under leakage of the key by the output function.

PRF modes of a compression function other than those mentioned above are also known. Yasuda [32] presented a novel PRF mode of a compression function, which almost maximizes the efficiency of the Merkle-Damgård iteration. It is shown to be a PRF if the underlying compression function is a PRF against a kind of related-key attacks. Sandwich construction for an iterated hash function is shown to produce a PRF if the underlying compression function is a PRF with respect to two keying strategies [33].

PRF modes for keyed compression functions were also proposed. XOR MAC [5] was the first proposal, which was followed by the protected counter sum construction [9]. It is shown that various hashing modes preserve the PRF security of keyed compression functions [8]. Yasuda proposed PRF modes for keyed compression functions with security beyond birthday [34, 35, 37, 38].

Minimum padding is already common among block-cipher-based MAC functions such as CMAC [29] and PMAC [13]. CMAC, which is based on OMAC (One-key CBC-MAC) [20],

originated from XCBC [12]. The idea to finalize the iteration with multiple non-cryptographic transformations for domain separation is used in the secure CBC-MAC variants GCBC1 and GCBC2 [28].

Rogaway and Shrimpton [30] introduced the notion of vPRF. They also presented a generic scheme to construct a vPRF from a common PRF taking a single string as input. Minematsu [26] also proposed a vPRF using his universal hash function based on bit rotation.

Organization. Section 2 gives notations and definitions used in the remaining parts of the paper. It is shown in Sect. 3 that the MDP domain extension may produce multiple independent PRFs with a single secret key and multiple permutations. Based on the result in Sect. 3, FMAC and vFMAC is presented and their security is confirmed in Sect. 4. Section 5 gives short discussion on the proposed constructions. Section 6 concludes the paper.

2 Preliminaries

2.1 Notations and Definitions

Let $\Sigma = \{0, 1\}$. For any non-negative integer l , Σ^l is identified with the set of all Σ -sequences of length l . Σ^0 is the set of the empty sequence ε . For $l \geq 1$, let $(\Sigma^l)^* = \bigcup_{i \geq 0} (\Sigma^l)^i$ be the set of all Σ -sequences whose lengths are multiples of l . Let $(\Sigma^l)^+ = (\Sigma^l)^* \setminus \{\varepsilon\}$. For $k_1 \leq k_2$, let $(\Sigma^l)^{[k_1, k_2]} = \bigcup_{i=k_1}^{k_2} (\Sigma^l)^i$.

For $x \in \Sigma^*$, the length of x is denoted by $|x|$. The concatenation of x_1 and x_2 in Σ^* is denoted by $x_1 \| x_2$.

The operation of selecting element s from set S uniformly at random is denoted by $s \leftarrow S$.

Let $f : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ be a family of functions from \mathcal{D} to \mathcal{R} indexed by keys in \mathcal{K} . Then, $f(K, \cdot)$ is a function from \mathcal{D} to \mathcal{R} for each key $K \in \mathcal{K}$ and is often denoted by $f_K(\cdot)$.

Let $\mathbf{F}(\mathcal{D}, \mathcal{R})$ denote the set of all functions from \mathcal{D} to \mathcal{R} . Let $\mathbf{P}(\mathcal{D})$ denote the set of all permutations on \mathcal{D} . id represents an identity permutation.

2.2 Pseudorandom Functions

For $f : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$, let A be an adversary trying to distinguish f_K from a function ρ , where K and ρ are chosen uniformly at random from \mathcal{K} and $\mathbf{F}(\mathcal{D}, \mathcal{R})$, respectively. A is given access to f_K or ρ as an oracle and makes adaptive queries in \mathcal{D} and obtains the corresponding outputs. The prf-advantage of A against f is defined as

$$\text{Adv}_f^{\text{prf}}(A) = \left| \Pr \left[A^{f_K} = 1 \right] - \Pr \left[A^\rho = 1 \right] \right| ,$$

where $K \leftarrow \mathcal{K}$ and $\rho \leftarrow \mathbf{F}(\mathcal{D}, \mathcal{R})$. In this notation, adversary A is regarded as a random variable.

f is called a pseudorandom function, or PRF in short, if no efficient adversary A can have any significant prf-advantage against f .

The definition of the prf-advantage can naturally be extended to adversaries with multiple oracles. The prf-advantage of adversary A with access to m oracles is defined as

$$\text{Adv}_f^{m\text{-prf}}(A) = \left| \Pr \left[A^{F_{K_1}, \dots, F_{K_m}} = 1 \right] - \Pr \left[A^{\rho_1, \dots, \rho_m} = 1 \right] \right| ,$$

where $(K_1, \dots, K_m) \leftarrow \mathcal{K}^m$ and $(\rho_1, \dots, \rho_m) \leftarrow \mathbf{F}(\mathcal{D}, \mathcal{R})^m$.

The following lemma is a paraphrase of Lemma 3.3 in [4]:

Lemma 1. *Let A be any adversary against f with access to m oracles. Then, there exists an adversary B against f such that*

$$\text{Adv}_f^{m\text{-prf}}(A) \leq m \cdot \text{Adv}_f^{\text{prf}}(B) .$$

The run time of B is approximately total of that of A and the time required to compute f to answer to the queries made by A . The number of the queries made by B is at most $\max\{q_i \mid 1 \leq i \leq m\}$, where q_i is the number of the queries made by A to its i -th oracle.

2.3 PRFs under Related-Key Attacks

The notion of PRF under related-key attacks is formalized by Bellare and Kohno [6]. Let $\Phi \subset \mathbf{F}(\mathcal{K}, \mathcal{K})$. Let $\text{key} \in \mathbf{F}(\Phi \times \mathcal{K}, \mathcal{K})$ be a function such that $\text{key}(\varphi, K) = \varphi(K)$. Adversary A has oracle access to $g(\text{key}(\cdot, K), \cdot)$, where $g \in \mathbf{F}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$. The oracle accepts $(\varphi, x) \in \Phi \times \mathcal{D}$ as a query and returns $g(\varphi(K), x)$. To simplify the notation, $g(\text{key}(\cdot, K), \cdot)$ is denoted by $g[K]$. The prf-rka-advantage of A against $f \in \mathbf{F}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$ with a Φ -restricted related-key attack (Φ -RKA) is given by

$$\text{Adv}_{\Phi, f}^{\text{prf-rka}}(A) = \left| \Pr[A^{f[K]} = 1] - \Pr[A^{\rho[K]} = 1] \right| ,$$

where $K \leftarrow \mathcal{K}$ and $\rho \leftarrow \mathbf{F}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$.

The prf-rka-advantage can naturally be extended to adversaries with multiple oracles as well as the prf-advantage. The prf-rka-advantage of adversary A with access to m oracles launching a Φ -RKA is defined as

$$\text{Adv}_{\Phi, f}^{m\text{-prf-rka}}(A) = \left| \Pr[A^{f[K_1], \dots, f[K_m]} = 1] - \Pr[A^{\rho_1[K_1], \dots, \rho_m[K_m]} = 1] \right| ,$$

where $(K_1, \dots, K_m) \leftarrow \mathcal{K}^m$ and $(\rho_1, \dots, \rho_m) \leftarrow \mathbf{F}(\mathcal{K} \times \mathcal{D}, \mathcal{R})^m$.

2.4 MDP domain extension

The MDP domain extension is a variant of the plain Merkle-Damgård iteration of a compression function [19]. It finalizes the iteration of the compression function by permuting the chaining variable fed into the final compression function with a permutation.

Let $F : \Sigma^n \times \Sigma^w \rightarrow \Sigma^n$ be a compression function. Let π be a permutation on Σ^n . The MDP domain extension of F with π is defined by the function $I^{F, \pi} : \Sigma^n \times (\Sigma^w)^+ \rightarrow \Sigma^n$ such that

$$I^{F, \pi}(Y_0, X_1 \| X_2 \| \dots \| X_x) = Y_x$$

for any $Y_0 \in \Sigma^n$ and $X_1, X_2, \dots, X_x \in \Sigma^w$, where

$$Y_i \leftarrow \begin{cases} F(Y_{i-1}, X_i) & \text{if } 1 \leq i \leq x-1 \\ F(\pi(Y_{x-1}), X_x) & \text{if } i = x . \end{cases}$$

X_1, X_2, \dots, X_x are called blocks. $I^{F, \pi}$ is also depicted in Fig. 2.

3 Multiple PRFs based on MDP

It is shown in this section that the MDP domain extension may produce multiple independent PRFs with a single compression function, a single secret key and multiple permutations.

For compression function $F : \Sigma^n \times \Sigma^w \rightarrow \Sigma^n$ and set of permutations $\Pi = \{\pi_1, \pi_2, \dots, \pi_d\} \subset \mathbf{P}(\Sigma^n) \setminus \{id\}$, let $I^{F, \Pi} = \{I^{F, \pi_1}, I^{F, \pi_2}, \dots, I^{F, \pi_d}\}$.

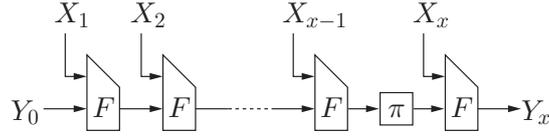


Fig. 2: MDP domain extension $I^{F,\pi}(Y_0, X_1 \| X_2 \| \dots \| X_x) = Y_x$

Let A be an adversary against $I^{F,\Pi}$. The advantage of A is defined by

$$\text{Adv}_{I^{F,\Pi}}^{\text{prfs}}(A) = \left| \Pr \left[A^{I_K^{F,\pi_1}, I_K^{F,\pi_2}, \dots, I_K^{F,\pi_d}} = 1 \right] - \Pr \left[A^{\rho_1, \rho_2, \dots, \rho_d} = 1 \right] \right| ,$$

where $K \leftarrow \Sigma^n$ and $(\rho_1, \rho_2, \dots, \rho_d) \leftarrow \mathbf{F}((\Sigma^w)^+, \Sigma^n)^d$. Notice that the setting is different from that of PRF for an adversary with multiple oracles in Sect. 2.2. $I_K^{F,\pi_1}, I_K^{F,\pi_2}, \dots, I_K^{F,\pi_d}$ use a single key K .

For Π , let

$$p_\Pi = \Pr \left[\pi(X) = \pi'(X) \text{ for some distinct } \pi, \pi' \in \Pi \cup \{id\} \right] ,$$

where X is a random variable with uniform distribution over Σ^n .

The following theorem states that $I^{F,\Pi}$ may produce multiple independent PRFs with a single key under the assumption that F is a PRF against related-key attacks restricted by $\Pi \cup \{id\}$.

Theorem 1. *Let A be any adversary against $I^{F,\Pi}$ running in time at most t and making at most q queries in total. Suppose that each query consists of at most ℓ blocks. Then, there exists an adversary B against F such that*

$$\text{Adv}_{I^{F,\Pi}}^{\text{prfs}}(A) \leq \ell q \left(\text{Adv}_{\Pi \cup \{id\}, F}^{\text{prf-rka}}(B) + p_\Pi \right) .$$

B runs in time at most $t + O(\ell q T_F)$, and makes at most q queries. T_F is the time required to compute F .

Remark 1. Theorem 1 extends Theorem 2 in [19] in two ways. First, Theorem 1 deals with multiple instances of $I^{F,\pi}$, while the latter shows the PRF security of a single instance. Second, Theorem 1 covers the case that $p_\Pi \neq 0$. Theorem 2 in [19] only covers the case that $p_{\{\pi\}} = 0$ for $\pi \in \mathbf{P}(\Sigma^n) \setminus \{id\}$.

Remark 2. The probability p_Π should be negligibly small for $\Pi = \{\pi_1, \pi_2, \dots, \pi_d\}$. Let c_1, c_2, \dots, c_d be distinct nonzero constants in Σ^n .

- Suppose that $\pi_i(x) = x \oplus c_i$ for $1 \leq i \leq d$. Then, $p_\Pi = 0$.
- Suppose that $\pi_i(x) = c_i \cdot x$ and $c_i \neq 1$ for $1 \leq i \leq d$. Then, $p_\Pi = 1/2^n$.

Theorem 1 immediately follows from Lemma 2 and Lemma 3.

Lemma 2. *Let A be any adversary against $I^{F,\Pi}$ running in time at most t and making at most q queries in total. Suppose that each query consists of at most ℓ blocks. Then, there exists an adversary B against F with access to q oracles such that*

$$\text{Adv}_{I^{F,\Pi}}^{\text{prfs}}(A) \leq \ell \left(\text{Adv}_{\Pi \cup \{id\}, F}^{q\text{-prf-rka}}(B) + q p_\Pi \right) .$$

B runs in time at most $t + O(\ell q T_F)$ and makes at most q queries.

Proof. Let $X = X_1 \| X_2 \| \cdots \| X_\ell$, where $|X_i| = w$ for $1 \leq i \leq \ell$ and $l \leq \ell$. For $1 \leq i_1 \leq i_2 \leq \ell$, let $X_{[i_1, i_2]} = X_{i_1} \| X_{i_1+1} \| \cdots \| X_{i_2}$. For $i \in \{0, 1, \dots, \ell\}$ and two functions $\mu : (\Sigma^w)^{[1, \ell]} \rightarrow \Sigma^n$ and $\xi : (\Sigma^w)^{[0, \ell]} \rightarrow \Sigma^n$, let $R[i]_{\mu, \xi}^{F, \pi} : (\Sigma^w)^{[1, \ell]} \rightarrow \Sigma^n$ be a function such that

$$R[i]_{\mu, \xi}^{F, \pi}(X) = \begin{cases} \mu(X) & \text{if } l \leq i, \\ I^{F, \pi}(\xi(X_{[1, i]}), X_{[i+1, \ell]}) & \text{if } l \geq i + 1, \end{cases}$$

where $X_{[1, i]} = \varepsilon$ if $i = 0$. We define

$$P_i = \Pr \left[A^{R[i]_{\mu_1, \xi}^{F, \pi_1}, R[i]_{\mu_2, \xi}^{F, \pi_2}, \dots, R[i]_{\mu_d, \xi}^{F, \pi_d}} = 1 \right],$$

where $(\mu_1, \dots, \mu_d) \leftarrow \mathbf{F}((\Sigma^w)^{[1, \ell]}, \Sigma^n)^d$ and $\xi \leftarrow \mathbf{F}((\Sigma^w)^{[0, \ell]}, \Sigma^n)$. Then, the advantage of A is

$$\text{Adv}_{I^{F, \Pi}}^{\text{prfs}}(A) = |P_0 - P_\ell|.$$

The algorithm of an adversary B against F with q oracles is described below. Let the oracles (g_1, \dots, g_q) of B be either $(F[K_1], F[K_2], \dots, F[K_q])$ or $(\tilde{\rho}_1, \tilde{\rho}_2, \dots, \tilde{\rho}_q)$ such that $(K_1, \dots, K_q) \leftarrow (\Sigma^n)^q$ and $(\tilde{\rho}_1, \tilde{\rho}_2, \dots, \tilde{\rho}_q) \leftarrow \mathbf{F}((\Pi \cup \{id\}) \times \Sigma^w, \Sigma^n)^q$. B uses A as a subroutine.

1. B selects r from $\{1, \dots, \ell\}$ uniformly at random.
2. If $r \geq 2$, then B selects functions $(\tilde{\mu}_1, \dots, \tilde{\mu}_d)$ from $\mathbf{F}((\Sigma^w)^{[1, r-1]}, \Sigma^n)^d$ uniformly at random.
3. B runs A . Finally, B outputs the output of A .

For $1 \leq k \leq q$ and $1 \leq l \leq \ell$, let $X = X_1 \| X_2 \| \cdots \| X_\ell$ be the k -th query made by A during the execution of A . Suppose that X is given to the j -th oracle. If $l \geq r$, then B makes a query to the $idx(k)$ -th oracle, where $idx : \{1, \dots, q\} \rightarrow \{1, \dots, q\}$ is a function such that

- $idx(k) = idx(k')$ if there exists a previous k' -th query X' ($k' < k$) such that $X'_{[1, r-1]} = X_{[1, r-1]}$, and
- $idx(k) = k$ otherwise.

The query made by B is (π_j, X_r) if $l = r$ and (id, X_r) if $l \geq r + 1$. The answer of B to X is

$$\begin{cases} \tilde{\mu}_j(X) & \text{if } l \leq r - 1, \\ g_{idx(k)}(\pi_j, X_r) & \text{if } l = r, \\ I^{F, \pi_j}(g_{idx(k)}(id, X_r), X_{[r+1, \ell]}) & \text{if } l \geq r + 1. \end{cases}$$

Now, suppose that B is given oracles $(F[K_1], \dots, F[K_q])$. Then, the answer of B to X is

$$\begin{cases} \tilde{\mu}_j(X) & \text{if } l \leq r - 1, \\ F_{\pi_j(K_{idx(k)})}(X_r) & \text{if } l = r, \\ I^{F, \pi_j}(F_{K_{idx(k)}}(X_r), X_{[r+1, \ell]}) & \text{if } l \geq r + 1. \end{cases}$$

$K_{idx(k)}$ can be regarded as an output of a function chosen uniformly at random from $\mathbf{F}((\Sigma^w)^{r-1}, \Sigma^n)$ since $idx(k)$ is a function of $X_{[1, r-1]}$ and $K_{idx(k)}$ is chosen uniformly at random from Σ^n . Thus, B provides A with the oracle $R[r-1]_{\mu_j, \xi}^{F, \pi_j}$, and

$$\begin{aligned} & \Pr \left[B^{F[K_1], \dots, F[K_q]} = 1 \right] \\ &= \sum_{i=1}^{\ell} \Pr \left[r = i \wedge B^{F[K_1], \dots, F[K_q]} = 1 \right] = \frac{1}{\ell} \sum_{i=1}^{\ell} \Pr \left[B^{F[K_1], \dots, F[K_q]} = 1 \mid r = i \right] \\ &= \frac{1}{\ell} \sum_{i=1}^{\ell} \Pr \left[A^{R[i-1]_{\mu_1, \xi}^{F, \pi_1}, R[i-1]_{\mu_2, \xi}^{F, \pi_2}, \dots, R[i-1]_{\mu_d, \xi}^{F, \pi_d}} = 1 \right] = \frac{1}{\ell} \sum_{i=1}^{\ell} P_{i-1}. \end{aligned}$$

Suppose that B is given oracles $(\tilde{\rho}_1, \dots, \tilde{\rho}_q)$. Then, the answer of B to X is

$$\begin{cases} \tilde{\mu}_j(X) & \text{if } l \leq r-1, \\ \tilde{\rho}_{idx(k)}(\pi_j, X_r) & \text{if } l = r, \\ I^{F, \pi_j}(\tilde{\rho}_{idx(k)}(id, X_r), X_{[r+1, l]}) & \text{if } l \geq r+1. \end{cases}$$

Notice that $\tilde{\rho}_{idx(k)}(\pi_1, \cdot), \dots, \tilde{\rho}_{idx(k)}(\pi_d, \cdot)$ and $\tilde{\rho}_{idx(k)}(id, \cdot)$ are independent of each other. Thus, B provides A with the oracle $R[r]_{\mu_j, \xi}^{F, \pi_j}$, and

$$\Pr[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1] = \frac{1}{\ell} \sum_{i=1}^{\ell} P_i .$$

Thus,

$$\begin{aligned} \left| \Pr \left[B^{F[K_1], \dots, F[K_q]} = 1 \right] - \Pr \left[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1 \right] \right| &= \left| \frac{1}{\ell} \sum_{i=1}^{\ell} P_{i-1} - \frac{1}{\ell} \sum_{i=1}^{\ell} P_i \right| \\ &= \frac{|P_0 - P_\ell|}{\ell} = \frac{1}{\ell} \text{Adv}_{I^{F, \Pi}}^{\text{prfs}}(A) . \end{aligned}$$

Now, let $(\rho_1, \rho_2, \dots, \rho_q) \leftarrow \mathbf{F}(\Sigma^n \times \Sigma^w, \Sigma^n)^q$. Then,

$$\begin{aligned} &\left| \Pr \left[B^{F[K_1], \dots, F[K_q]} = 1 \right] - \Pr \left[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1 \right] \right| \\ &\leq \left| \Pr \left[B^{F[K_1], \dots, F[K_q]} = 1 \right] - \Pr \left[B^{\rho_1[K_1], \dots, \rho_q[K_q]} = 1 \right] \right| \\ &\quad + \left| \Pr \left[B^{\rho_1[K_1], \dots, \rho_q[K_q]} = 1 \right] - \Pr \left[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1 \right] \right| \\ &= \text{Adv}_{\Pi \cup \{id\}, F}^{q\text{-prf-rka}}(B) + \left| \Pr \left[B^{\rho_1[K_1], \dots, \rho_q[K_q]} = 1 \right] - \Pr \left[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1 \right] \right| . \end{aligned}$$

$(\rho_1[K_1], \dots, \rho_q[K_q])$ and $(\tilde{\rho}_1, \dots, \tilde{\rho}_q)$ are identical as long as $\pi(K_i) \neq \pi'(K_i)$ for any distinct $\pi, \pi' \in \Pi \cup \{id\}$ for $1 \leq i \leq q$. Thus,

$$\left| \Pr \left[B^{\rho_1[K_1], \dots, \rho_q[K_q]} = 1 \right] - \Pr \left[B^{\tilde{\rho}_1, \dots, \tilde{\rho}_q} = 1 \right] \right| \leq qp\Pi .$$

To answer to the queries made by A , B may compute $I^{F, \pi_1}, \dots, I^{F, \pi_d}$ and simulate $\tilde{\mu}$. It approximately costs at most ℓq evaluations of F . \square

Lemma 3. *Let A be any adversary with m oracles against F running in time at most t , and making at most q queries. Then, there exists an adversary B against F such that*

$$\text{Adv}_{\Pi \cup \{id\}, F}^{m\text{-prf-rka}}(A) \leq m \cdot \text{Adv}_{\Pi \cup \{id\}, F}^{\text{prf-rka}}(B) .$$

B runs in time at most $t + O(qT_F)$ and makes at most q queries, where T_F represents the time required to compute F .

Lemma 3 is a generalized version of Lemma 4 in [19], which only covers the case that $|\Pi| = 1$. The proof of Lemma 3 is omitted since it is standard and similar to that of Lemma 4 in [19].

4 Applications

4.1 PRF with minimum padding

The proposed MAC function FMAC consists of a compression function $F : \Sigma^n \times \Sigma^w \rightarrow \Sigma^n$ and distinct permutations π_1 and π_2 on Σ^n .

The padding function used in FMAC is defined as follows: For any $M \in \Sigma^*$,

$$\text{pad}(M) = \begin{cases} M & \text{if } |M| > 0 \text{ and } |M| \equiv 0 \pmod{w} \\ M \| 10^l & \text{if } |M| = 0 \text{ or } |M| \not\equiv 0 \pmod{w} \end{cases},$$

where l is the minimum non-negative integer such that $|M| + 1 + l \equiv 0 \pmod{w}$. In particular, $\text{pad}(\varepsilon) = 10^{w-1}$.

For any M , $|\text{pad}(M)|$ is the minimum positive multiple of w , which is greater than or equal to $|M|$. Let $\text{pad}(M) = \bar{M}_1 \| \bar{M}_2 \| \cdots \| \bar{M}_m$, where $|\bar{M}_i| = w$ for every i such that $1 \leq i \leq m$. $m = 1$ if $|M| = 0$, and $m = \lceil |M|/w \rceil$ if $|M| > 0$. \bar{M}_i is called the i -th block of $\text{pad}(M)$.

FMAC is the MAC function $C^{F, \{\pi_1, \pi_2\}} : \Sigma^n \times \Sigma^* \rightarrow \Sigma^n$ defined by

$$C^{F, \{\pi_1, \pi_2\}}(K, M) = \begin{cases} I^{F, \pi_1}(K, \text{pad}(M)) & \text{if } |M| > 0 \text{ and } |M| \equiv 0 \pmod{w} \\ I^{F, \pi_2}(K, \text{pad}(M)) & \text{if } |M| = 0 \text{ or } |M| \not\equiv 0 \pmod{w} \end{cases}.$$

$C^{F, \{\pi_1, \pi_2\}}$ is shown to be a PRF under the assumptions that F is a PRF against related-key attacks with respect to permutations π_1 and π_2 and that $p_{\{\pi_1, \pi_2\}}$ is negligibly small.

Corollary 1. *Let π_1 and π_2 be permutations in $\mathbf{P}(\Sigma^n) \setminus \{id\}$. Let A be any adversary against $C^{F, \{\pi_1, \pi_2\}}$ running in time at most t and making at most q queries. Suppose that the length of each query is at most ℓw . Then, there exists an adversary B against F such that*

$$\text{Adv}_{C^{F, \{\pi_1, \pi_2\}}}^{\text{prf}}(A) \leq \ell q \left(\text{Adv}_{\{id, \pi_1, \pi_2\}, F}^{\text{prf-rka}}(B) + p_{\{\pi_1, \pi_2\}} \right).$$

B runs in time at most $t + O(\ell q T_F)$, and makes at most q queries. T_F is the time required to compute F .

Proof. Let \hat{A} be an adversary against $I^{F, \pi_1}, I^{F, \pi_2}$ using A as a subroutine. Let (h_1, h_2) be the oracles of \hat{A} . Then, (h_1, h_2) are either $(I_K^{F, \pi_1}, I_K^{F, \pi_2})$ with $K \leftarrow \Sigma^n$ or $(\rho_1, \rho_2) \leftarrow \mathbf{F}((\Sigma^w)^+, \Sigma^n)^2$.

\hat{A} simply runs A . Let M be a query made by A . If $|M| > 0$ and $|M| \equiv 0 \pmod{w}$, then \hat{A} returns $h_1(\text{pad}(M))$ to A . Otherwise, \hat{A} returns $h_2(\text{pad}(M))$ to A . Finally, \hat{A} outputs the output of A . The run time of \hat{A} is almost equal to that of A and \hat{A} makes at most q queries in total.

Notice that

$$\Pr \left[\hat{A}_{I_K^{F, \pi_1}, I_K^{F, \pi_2}} = 1 \right] = \Pr \left[A_{C_K^{F, \{\pi_1, \pi_2\}}} = 1 \right]$$

and

$$\Pr \left[\hat{A}_{\rho^1, \rho^2} = 1 \right] = \Pr [A^\rho = 1],$$

where $\rho \leftarrow \mathbf{F}(\Sigma^*, \Sigma^n)$. Thus, from Theorem 1, there exists an adversary B against F such that

$$\text{Adv}_{C^{F, \{\pi_1, \pi_2\}}}^{\text{prf}}(A) = \text{Adv}_{I^{F, \{\pi_1, \pi_2\}}}^{\text{prfs}}(\hat{A}) \leq \ell q \left(\text{Adv}_{\{id, \pi_1, \pi_2\}, F}^{\text{prf-rka}}(B) + p_{\{\pi_1, \pi_2\}} \right).$$

B runs in time at most $t + O(\ell q T_F)$, and makes at most q queries. \square

4.2 Vector-Input PRF

A scheme is proposed to construct a vector-input PRF (vPRF) using instances of FMAC. In the original formalization [30], a vPRF accepts vectors with any number of components as inputs. In contrast, the proposed scheme has a parameter which specifies the maximum number of the components in an input vector.

Let d be a positive integer, which is the maximum number of the components in an input vector. Let $F : \Sigma^n \times \Sigma^w \rightarrow \Sigma^n$ and $\Pi = \{\pi_1, \pi_2, \dots, \pi_{2d+2}\} \subset \mathbf{P}(\Sigma^n) \setminus \{id\}$. The proposed vector-input function vFMAC $V^{F,\Pi} : \Sigma^n \times (\Sigma^*)^{[0,d]} \rightarrow \Sigma^n$ is defined as follows: For an s -component vector (S_1, S_2, \dots, S_s) such that $0 \leq s \leq d$,

$$V^{F,\Pi}(K, (S_1, S_2, \dots, S_s)) = \begin{cases} C_K^{F, \{\pi_{2d+1}, \pi_{2d+2}\}}(\varepsilon) & \text{if } s = 0, \\ C_K^{F, \{\pi_{2d+1}, \pi_{2d+2}\}} \left(\bigoplus_{i=1}^s C_K^{F, \{\pi_{2i-1}, \pi_{2i}\}}(S_i) \right) & \text{if } s \geq 1. \end{cases}$$

It is shown that $V^{F,\Pi}$ is a vPRF if F is a PRF against related-key attacks with respect to permutations in Π and p_Π is negligibly small.

Corollary 2. *Let $\Pi = \{\pi_1, \pi_2, \dots, \pi_{2d+2}\} \subset \mathbf{P}(\Sigma^n) \setminus \{id\}$. Let A be any adversary against $V^{F,\Pi}$ running in time at most t and making at most q queries. Suppose that the length of each vector component in queries is at most ℓw and that the total number of the vector components in all of the queries is at most $\sigma (\geq q - 1)$. Then, there exists an adversary B against F such that*

$$\text{Adv}_{V^{F,\Pi}}^{\text{prf}}(A) \leq \ell(\sigma + q) \left(\text{Adv}_{\Pi \cup \{id\}, F}^{\text{prf-rka}}(B) + p_\Pi \right) + \frac{q(q-1)}{2^{n+1}}.$$

B runs in time at most $t + O(\ell \sigma T_F)$, and makes at most $(\sigma + q)$ queries. T_F is the time required to compute F .

Corollary 2 directly follows from Lemmata 4 and 5.

Lemma 4. *Let $\Pi = \{\pi_1, \pi_2, \dots, \pi_{2d+2}\} \subset \mathbf{P}(\Sigma^n) \setminus \{id\}$. Let A be any adversary against $\{C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1\}$ running in time at most t and making at most q queries in total. Suppose that the length of each query is at most ℓw . Then, there exists an adversary B against F such that*

$$\text{Adv}_{\{C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1\}}^{\text{prfs}}(A) \leq \ell q \left(\text{Adv}_{\Pi \cup \{id\}, F}^{\text{prf-rka}}(B) + p_\Pi \right).$$

B runs in time at most $t + O(\ell q T_F)$, and makes at most q queries. T_F is the time required to compute F .

Proof. Let \hat{A} be an adversary against $\{I^{F, \pi_1}, I^{F, \pi_2}, \dots, I^{F, \pi_{2d+2}}\}$ using A as a subroutine. Then, \hat{A} is given $(2d+2)$ oracles $(h_1, h_2, \dots, h_{2d+2})$, which are either $(I_K^{F, \pi_1}, \dots, I_K^{F, \pi_{2d+2}})$ with $K \leftarrow \Sigma^n$ or $(\hat{\rho}_1, \dots, \hat{\rho}_{2d+2}) \leftarrow \mathbf{F}((\Sigma^w)^+, \Sigma^n)^{2d+2}$.

\hat{A} simply runs A . Let M be a query made by A to its j -th oracle. If $|M| > 0$ and $|M| \equiv 0 \pmod{w}$, then \hat{A} returns $h_{2j-1}(\text{pad}(M))$ to A . Otherwise, \hat{A} returns $h_{2j}(\text{pad}(M))$ to A . Finally, \hat{A} outputs the output of A . The run time of \hat{A} is almost equal to that of A and \hat{A} makes at most q queries in total.

Notice that

$$\Pr \left[\hat{A}^{I_K^{F, \pi_1}, \dots, I_K^{F, \pi_{2d+2}}} = 1 \right] = \Pr \left[A^{C_K^{F, \{\pi_1, \pi_2\}}, \dots, C_K^{F, \{\pi_{2d+1}, \pi_{2d+2}\}}} = 1 \right]$$

and

$$\Pr \left[\hat{A}^{\hat{\rho}_1, \dots, \hat{\rho}_{2d+2}} = 1 \right] = \Pr \left[A^{\rho_1, \dots, \rho_{d+1}} = 1 \right] ,$$

where $(\rho_1, \dots, \rho_{d+1}) \leftarrow \mathbf{F}(\Sigma^*, \Sigma^n)^{d+1}$. Thus, from Theorem 1, there exists an adversary B against F such that

$$\text{Adv}_{\left\{ C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1 \right\}}^{\text{prfs}}(A) = \text{Adv}_{IF, \Pi}^{\text{prfs}}(\hat{A}) \leq \ell q \left(\text{Adv}_{\Pi \cup \{id\}, F}^{\text{prf-rka}}(B) + p_{\Pi} \right) .$$

B runs in time at most $t + O(\ell q T_F)$, and makes at most q queries. \square

Lemma 5. *Let $\Pi = \{\pi_1, \pi_2, \dots, \pi_{2d+2}\} \subset \mathbf{P}(\Sigma^n) \setminus \{id\}$. Let A be any adversary against $V^{F, \Pi}$ running in time at most t and making at most q queries. Suppose that the length of each vector component in queries is at most ℓw and that the total number of the vector components in all of the queries is at most σ . Then, there exists an adversary B against $\{C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1\}$ such that*

$$\text{Adv}_{VF, \Pi}^{\text{prf}}(A) \leq \text{Adv}_{\left\{ C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1 \right\}}^{\text{prfs}}(B) + \frac{q(q-1)}{2^{n+1}} .$$

B runs in time at most t and makes at most $(\sigma + q)$ queries in total. The length of each query is at most ℓw .

Proof. Notice that

$$\text{Adv}_{VF, \Pi}^{\text{prf}}(A) = \left| \Pr \left[A^{V_K^{F, \Pi}} = 1 \right] - \Pr \left[A^{\rho} = 1 \right] \right| ,$$

where $\rho \leftarrow \mathbf{F}((\Sigma^*)^{[0, d]}, \Sigma^n)$.

Let $\rho_i : \Sigma^* \rightarrow \Sigma^n$ for $1 \leq i \leq d+1$. Let $V^{\rho_1, \dots, \rho_{d+1}} : (\Sigma^*)^{[0, d]} \rightarrow \Sigma^n$ be a vector-input function such that

$$V^{\rho_1, \dots, \rho_{d+1}}(S_1, S_2, \dots, S_s) = \begin{cases} \rho_{d+1}(\varepsilon) & \text{if } s = 0, \\ \rho_{d+1}(\bigoplus_{i=1}^s \rho_i(S_i)) & \text{if } s \geq 1. \end{cases}$$

$V^{\rho_1, \dots, \rho_{d+1}}$ is obtained from $V_K^{F, \Pi}$ simply by replacing $C^{F, \{\pi_{2i-1}, \pi_{2i}\}}$ with ρ_i for $1 \leq i \leq d+1$. Then,

$$\text{Adv}_{VF, \Pi}^{\text{prf}}(A) \leq \left| \Pr \left[A^{V_K^{F, \Pi}} = 1 \right] - \Pr \left[A^{V^{\rho_1, \dots, \rho_{d+1}}} = 1 \right] \right| + \left| \Pr \left[A^{V^{\rho_1, \dots, \rho_{d+1}}} = 1 \right] - \Pr \left[A^{\rho} = 1 \right] \right| , \quad (1)$$

where $K \leftarrow \Sigma^n$, $(\rho_1, \dots, \rho_{d+1}) \leftarrow \mathbf{F}(\Sigma^*, \Sigma^n)^{d+1}$ and $\rho \leftarrow \mathbf{F}((\Sigma^*)^{[0, d]}, \Sigma^n)$.

For the first term of the upper bound of Eq. (1), let B be an adversary against $C^{F, \{\pi_1, \pi_2\}}, C^{F, \{\pi_3, \pi_4\}}, \dots, C^{F, \{\pi_{2d+1}, \pi_{2d+2}\}}$. Let $(g_1, g_2, \dots, g_{d+1})$ be the oracles of B , which are either $(C^{F, \{\pi_1, \pi_2\}}, C^{F, \{\pi_3, \pi_4\}}, \dots, C^{F, \{\pi_{2d+1}, \pi_{2d+2}\}})$ or $(\rho_1, \rho_2, \dots, \rho_{d+1})$. B runs A . For each query (S_1, S_2, \dots, S_s) made by A , B returns $g_{d+1}(\bigoplus_{i=1}^s g_i(S_i))$. Finally, B outputs the output of A . Thus,

$$\left| \Pr \left[A^{V_K^{F, \Pi}} = 1 \right] - \Pr \left[A^{V^{\rho_1, \dots, \rho_{d+1}}} = 1 \right] \right| = \text{Adv}_{\left\{ C^{F, \{\pi_{2i-1}, \pi_{2i}\}} \mid 1 \leq i \leq d+1 \right\}}^{\text{prfs}}(B) .$$

The run time of B approximately equals that of A . The number of queries made by B to its oracles is at most $(d+1)q$.

For the second term of the upper bound of Eq. (1), let R be the oracle of A such that

1. Prior to the interaction with A ,

- $Y_{i,j} \leftarrow \perp$ for $1 \leq i \leq q$ and $1 \leq j \leq d$,
 - $Z_i \leftarrow \Sigma^n$ for $1 \leq i \leq q$, and
 - $bad \leftarrow 0$.
2. During the interaction with A , return Z_i to the i -th query made by A .
 3. For $1 \leq i \leq q$, let $\mathcal{S}_i = (S_{i,1}, S_{i,2}, \dots, S_{i,s_i})$ be the i -th query made by A , where $0 \leq s_i \leq d$. For $1 \leq j \leq s_i$,
 - $Y_{i,j} \leftarrow \Sigma^n$ if $S_{i,j}$ is new, that is, $S_{i,j} \neq S_{i',j}$ for any i' such that $i' < i$, and
 - $Y_{i,j} \leftarrow Y_{i',j}$ if there exists some i' such that $i' < i$ and $S_{i,j} = S_{i',j}$.
 4. $bad \leftarrow 1$ if, for some distinct i and i' ,

$$\bigoplus_{j=1}^{s_i} Y_{i,j} = \bigoplus_{j=1}^{s_{i'}} Y_{i',j} .$$

Since R is identical to ρ , $\Pr[A^R = 1] = \Pr[A^\rho = 1]$. As long as $bad = 0$, R is also identical to $V^{\rho_1, \dots, \rho_{d+1}}$. Notice that

$$\Pr \left[\bigoplus_{j=1}^{s_i} Y_{i,j} = \bigoplus_{j=1}^{s_{i'}} Y_{i',j} \right] \leq \frac{1}{2^n} .$$

Thus,

$$\left| \Pr \left[A^{V^{\rho_1, \dots, \rho_{d+1}}} = 1 \right] - \Pr[A^\rho = 1] \right| \leq \frac{q(q-1)}{2^{n+1}} .$$

□

5 Discussion

The drawback of our proposals is that it requires the underlying compression function to be a PRF against related-key attacks. However, the related-key-deriving functions, which are the underlying permutations, cannot be chosen by adversaries. They are chosen by the users.

FMAC shares some features with existing MAC functions. The novelty of FMAC is its simplicity.

- The compression-function-based MAC function of OMD [14] already uses minimum padding. The difference between the OMD MAC function and FMAC is that the former uses a keyed compression function as its underlying primitive. OMD is also inspired by tweakable block ciphers [24].
- The idea to finalize the iteration with multiple non-cryptographic transformations was used in the secure CBC-MAC variants GCBC1 and GCBC2 [28]. Due to the structure of CBC-MAC, that is, the addition of a message block to a chaining variable, addition of non-zero constants cannot be used for the non-cryptographic transformations of GCBC1 and GCBC2.

Some generic constructions of vPRF using any string-input PRF are already known. S2V by Rogaway and Shrimpton [30] involves finite field multiplications. S2V-R by Minematsu [26] requires bit rotations. Protected-counter-sum construction by Bernstein [9] can also be used for vPRF, which requires encoding of an input to add counter values. On the other hand, an instantiation of vFMAC only requires additions, though it is not a generic construction.

For vFMAC, the number of the components of an input vector is bounded from above, and the upper bound depends on the number of the underlying permutations. To reduce the number of permutations used for the construction, $I^{F,\pi}$ can be used instead of $C^{F,\{\pi,\pi'\}}$. Let $\{\pi_1, \pi_2, \dots, \pi_{d+1}\} \subset \mathbf{P}(\Sigma^n)$. For any $M \in \Sigma^*$, let

$$\text{pad}'(M) = M \| 10^l ,$$

where l is the minimum non-negative integer such that $|M| + 1 + l \equiv 0 \pmod{w}$. The vPRF $\hat{V}^{F, \{\pi_1, \pi_2, \dots, \pi_{d+1}\}} : \Sigma^n \times (\Sigma^*)^{[0, d]} \rightarrow \Sigma^n$ is defined as follows: For an s -component vector (S_1, S_2, \dots, S_s) such that $0 \leq s \leq d$,

$$\hat{V}^{F, \{\pi_1, \pi_2, \dots, \pi_{d+1}\}}(K, (S_1, S_2, \dots, S_s)) = \begin{cases} I_K^{F, \pi_{d+1}}(\text{pad}'(\varepsilon)) & \text{if } s = 0, \\ I_K^{F, \pi_{d+1}}\left(\text{pad}'\left(\bigoplus_{i=1}^s I_K^{F, \pi_i}(\text{pad}'(S_i))\right)\right) & \text{if } s \geq 1. \end{cases}$$

The security proof is omitted since it is similar to that of $V^{F, \Pi}$ with $\Pi = \{\pi_1, \pi_2, \dots, \pi_{2d+2}\}$.

6 Conclusion

We have shown that the MDP domain extension may produce multiple independent PRFs using a single key and multiple permutations if the underlying compression function is a PRF against related-key attacks with respect to the permutations. Then, based on this result, we have presented a MAC function called FMAC, which is cascade of a compression function based on MDP. We have also extended FMAC so as to take as input a vector of strings. We have confirmed their security as PRF on the assumption that the underlying compression function is PRF under related-key attacks. Future work is to evaluate their security as PRF in the multi-user setting.

Acknowledgments

This work was supported in part by JSPS KAKENHI Grant Number JP16H02828.

References

1. Bellare, M.: New proofs for NMAC and HMAC: Security without collision-resistance. In: Dwork, C. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 4117, pp. 602–619. Springer (2006), the full version is “Cryptology ePrint Archive: Report 2006/043” at <http://eprint.iacr.org/>
2. Bellare, M., Bernstein, D.J., Tessaro, S.: Hash-function based PRFs: AMAC and its multi-user security. Cryptology ePrint Archive, Report 2016/142 (2016), <http://eprint.iacr.org/>
3. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In: Kobitz, N. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 1109, pp. 1–15. Springer (1996)
4. Bellare, M., Canetti, R., Krawczyk, H.: Pseudorandom functions revisited: The cascade construction and its concrete security. In: Proceedings of the 37th IEEE Symposium on Foundations of Computer Science. pp. 514–523 (1996)
5. Bellare, M., Guérin, R., Rogaway, P.: XOR MACs: New methods for message authentication using finite pseudorandom functions. In: Coppersmith, D. (ed.) Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27–31, 1995, Proceedings. Lecture Notes in Computer Science, vol. 963, pp. 15–28. Springer (1995), http://dx.doi.org/10.1007/3-540-44750-4_2
6. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2656, pp. 491–506. Springer (2003), http://dx.doi.org/10.1007/3-540-39200-9_31
7. Bellare, M., Ristenpart, T.: Multi-property-preserving hash domain extension and the EMD transform. In: Lai, X., Chen, K. (eds.) Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3–7, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4284, pp. 299–314. Springer (2006), http://dx.doi.org/10.1007/11935230_20
8. Bellare, M., Ristenpart, T.: Hash functions in the dedicated-key setting: Design choices and MPP transforms. In: ICALP 2007 Proceedings, Lecture Notes in Computer Science 4596. pp. 399–410 (2007)
9. Bernstein, D.J.: How to stretch random functions: The security of protected counter sums. Journal of Cryptology 12(3), 185–192 (1999), <http://dx.doi.org/10.1007/s001459900051>
10. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Sponge functions. ECRYPT Hash Workshop (2007)

11. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Duplexing the sponge: Single-pass authenticated encryption and other applications. In: Miri, A., Vaudenay, S. (eds.) Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 7118, pp. 320–337. Springer (2011), http://dx.doi.org/10.1007/978-3-642-28496-0_19
12. Black, J., Rogaway, P.: CBC MACs for arbitrary-length messages: The three-key constructions. In: Bellare, M. (ed.) Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1880, pp. 197–215. Springer (2000), http://dx.doi.org/10.1007/3-540-44598-6_12
13. Black, J., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2332, pp. 384–397. Springer (2002), http://dx.doi.org/10.1007/3-540-46035-7_25
14. Cogliani, S., Maimut, D., Naccache, D., do Canto, R.P., Reyhanitabar, R., Vaudenay, S., Vizár, D.: OMD: A compression function mode of operation for authenticated encryption. In: Joux and Youssef [21], pp. 112–128, http://dx.doi.org/10.1007/978-3-319-13051-4_7
15. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings. Lecture Notes in Computer Science, vol. 739, pp. 210–224. Springer (1991), http://dx.doi.org/10.1007/3-540-57332-1_17
16. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. *J. Cryptology* 10(3), 151–162 (1997), <http://dx.doi.org/10.1007/s001459900025>
17. FIPS PUB 180-4: Secure hash standard (SHS) (Mar 2012)
18. FIPS PUB 202: SHA-3 standard: Permutation-based hash and extendable-output functions (2015)
19. Hirose, S., Park, J.H., Yun, A.: A simple variant of the Merkle-Damgård scheme with a permutation. *Journal of Cryptology* 25(2), 271–309 (2012), <http://dx.doi.org/10.1007/s00145-010-9095-5>
20. Iwata, T., Kurosawa, K.: OMAC: One-key CBC MAC. In: Johansson, T. (ed.) FSE. Lecture Notes in Computer Science, vol. 2887, pp. 129–153. Springer (2003), an updated version is “Cryptology ePrint Archive: Report 2002/180” at <http://eprint.iacr.org/>
21. Joux, A., Youssef, A.M. (eds.): Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers, Lecture Notes in Computer Science, vol. 8781. Springer (2014), <http://dx.doi.org/10.1007/978-3-319-13051-4>
22. Kurosawa, K.: Power of a public random permutation and its application to authenticated-encryption. Cryptology ePrint Archive, Report 2002/127 (2002), <http://eprint.iacr.org/>
23. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. *IEEE Trans. Information Theory* 56(10), 5366–5374 (2010), <http://dx.doi.org/10.1109/TIT.2010.2059636>
24. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: CRYPT 2002 Proceedings, Lecture Notes in Computer Science 2442. pp. 31–46 (2002)
25. Mennink, B.: XPX: Generalized tweakable Even-Mansour with improved security guarantees. Cryptology ePrint Archive, Report 2015/476 (2015), <http://eprint.iacr.org/>
26. Minematsu, K.: A short universal hash function from bit rotation, and applications to blockcipher modes. In: Susilo, W., Reyhanitabar, R. (eds.) Provable Security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013. Proceedings. Lecture Notes in Computer Science, vol. 8209, pp. 221–238. Springer (2013), http://dx.doi.org/10.1007/978-3-642-41227-1_13
27. Mouha, N., Mennink, B., Herrewewe, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In: Joux and Youssef [21], pp. 306–323, http://dx.doi.org/10.1007/978-3-319-13051-4_19
28. Nandi, M.: Fast and secure CBC-type MAC algorithms. In: Dunkelman, O. (ed.) Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers. Lecture Notes in Computer Science, vol. 5665, pp. 375–393. Springer (2009), http://dx.doi.org/10.1007/978-3-642-03317-9_23
29. NIST Special Publication 800-38B: Recommendation for block cipher modes of operation: The CMAC mode for authentication (2005)
30. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4004, pp. 373–390. Springer (2006), http://dx.doi.org/10.1007/11761679_23

31. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher v1. Submission to CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) (2014)
32. Yasuda, K.: Boosting Merkle-Damgård hashing for message authentication. In: Kurosawa, K. (ed.) *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, Malaysia, December 2-6, 2007, Proceedings. *Lecture Notes in Computer Science*, vol. 4833, pp. 216–231. Springer (2007), http://dx.doi.org/10.1007/978-3-540-76900-2_13
33. Yasuda, K.: “Sandwich” is indeed secure: How to authenticate a message with just one hashing. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) *Information Security and Privacy, 12th Australasian Conference, ACISP 2007*, Townsville, Australia, July 2-4, 2007, Proceedings. *Lecture Notes in Computer Science*, vol. 4586, pp. 355–369. Springer (2007), http://dx.doi.org/10.1007/978-3-540-73458-1_26
34. Yasuda, K.: A one-pass mode of operation for deterministic message authentication- security beyond the birthday barrier. In: Nyberg, K. (ed.) *Fast Software Encryption, 15th International Workshop, FSE 2008*, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers. *Lecture Notes in Computer Science*, vol. 5086, pp. 316–333. Springer (2008), http://dx.doi.org/10.1007/978-3-540-71039-4_20
35. Yasuda, K.: A double-piped mode of operation for macs, prfs and pros: Security beyond the birthday barrier. In: Joux, A. (ed.) *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, April 26-30, 2009. Proceedings. *Lecture Notes in Computer Science*, vol. 5479, pp. 242–259. Springer (2009), http://dx.doi.org/10.1007/978-3-642-01001-9_14
36. Yasuda, K.: HMAC without the “second” key. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) *Information Security, 12th International Conference, ISC 2009*, Pisa, Italy, September 7-9, 2009. Proceedings. *Lecture Notes in Computer Science*, vol. 5735, pp. 443–458. Springer (2009), http://dx.doi.org/10.1007/978-3-642-04474-8_35
37. Yasuda, K.: On the full MAC security of a double-piped mode of operation. *IEICE Transactions on Fundamentals* 94-A(1), 84–91 (2011), http://search.ieice.org/bin/summary.php?id=e94-a_1_84
38. Yasuda, K.: A parallelizable PRF-based MAC algorithm: Well beyond the birthday bound. *IEICE Transactions on Fundamentals* 96-A(1), 237–241 (2013), http://search.ieice.org/bin/summary.php?id=e96-a_1_237