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

Shoichi Hirose[1(✉)] and Atsushi Yabumoto[2]

[1] Faculty of Engineering, University of Fukui, Fukui, Japan
hrs_shch@u-fukui.ac.jp
[2] Graduate School of Engineering, University of Fukui, 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 · Provable security · 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:

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

where K is a secret key, M is an input message, $\|$ represents concatenation, $\oplus$ represents bitwise XOR, $\mathtt{ipad} = \mathtt{0x3636} \cdots \mathtt{36}$ and $\mathtt{opad} = \mathtt{0x5c5c} \cdots \mathtt{5c}$.

Due to the length extension property of standardized hash functions such as SHA-1, SHA-256 and SHA-512 [14], 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.

Recently, an approach attracts a lot of interest to construct symmetric-key schemes using a public permutation. It is emerged from the sponge construction [7], which is the basis of the SHA-3 hash function [15]. Following the approach, methods to construct authenticated encryption schemes and pseudorandom generators are proposed [8]. The Even-Mansour cipher [12,13], which is constructed from a public permutation, also attracts renewed interest, and schemes

I. Bica and R. Reyhanitabar (Eds.): SECITC 2016, LNCS 10006, pp. 103–114, 2016.
DOI: 10.1007/978-3-319-47238-6_7

for encryption, message authentication and authenticated encryption are proposed based on it [19–21,27]. Chaskey is a recently proposed MAC function based on a permutation [23].

The approach to construct secret-key schemes using a compression function is not new. In the context of multi-property preservation [6], some schemes are proposed such as EMD [6] and MDP [16], which may produce PRFs with some appropriate keying strategies. Yasuda [28] also presents a novel PRF mode of a compression function, which almost maximizes the efficiency of the Merkle-Damgård iteration. The recent proposal OMD [11] for authenticated encryption is constructed with a compression function.

Our Contribution. This paper extends the MDP domain extension [16] 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 [30] 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.

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].

Yasuda's PRF mode of a compression function in [28] 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 [29].

Minimum padding is already common among block-cipher-based MAC functions such as CMAC [25] and PMAC [10]. CMAC, which is based on OMAC (One-key CBC-MAC) [17], originated from XCBC [9]. The idea to finalize the iteration with multiple permutations is used in the secure CBC-MAC variants GCBC1 and GCBC2 [24].

Rogaway and Shrimpton [26] 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 [22] also proposed a vPRF using his universal hash function based on bit rotation.

Organization. Sect. 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 the manner of provable security in Sect. 4. Section 5 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. Σ^1 is identified with Σ. 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 $s \twoheadleftarrow S$.

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

2.2 Pseudorandom Functions

For $f : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$, 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 $\boldsymbol{F}(\mathcal{D},\mathcal{R})$, 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

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

where $K \twoheadleftarrow \mathcal{K}$ and $\rho \twoheadleftarrow \boldsymbol{F}(\mathcal{D}, \mathcal{R})$. 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

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

where $(K_1, \ldots, K_m) \twoheadleftarrow \mathcal{K}^m$ and $(\rho_1, \ldots, \rho_m) \twoheadleftarrow \boldsymbol{F}(\mathcal{D}, \mathcal{R})^m$.

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*

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

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

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

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

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

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

where $(K_1, \ldots, K_m) \twoheadleftarrow \mathcal{K}^m$ and $(\rho_1, \ldots, \rho_m) \twoheadleftarrow \boldsymbol{F}(\mathcal{K} \times \mathcal{D}, \mathcal{R})^m$.

2.4 MDP Domain Extension

The MDP domain extension is a variant of the plain Merkle-Damgård iteration of a compression function [16]. It finalizes the iteration of the compression function by permuting the chaining variable fed into the final compression function with a permutation.

Let $F : \Sigma^n \times \Sigma^w \to \Sigma^n$ 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 $I^{F,\pi} : \Sigma^n \times (\Sigma^w)^+ \to \Sigma^n$ such that

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

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

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

$X_1, X_2, \ldots, X_x$ are called blocks. $I^{F,\pi}$ is also depicted in Fig. 1.

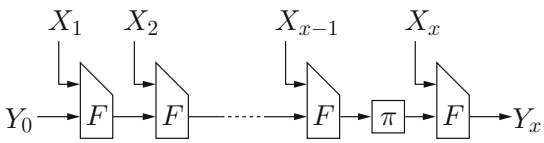

Fig. 1. MDP domain extension $I^{F,\pi}(Y_0, X_1 \| X_2 \| \cdots \| X_x) = Y_x$

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 $F : \Sigma^n \times \Sigma^w \to \Sigma^n$ and set of permutations $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\} \subset \boldsymbol{P}(\Sigma^n) \setminus \{id\}$, let $I^{F,\Pi} = \{I^{F,\pi_1}, I^{F,\pi_2}, \ldots, I^{F,\pi_d}\}$.

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

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

where $K \twoheadleftarrow \Sigma^n$ and $(\rho_1, \rho_2, \ldots, \rho_d) \twoheadleftarrow \boldsymbol{F}((\Sigma^w)^+, \Sigma^n)^d$. Notice that the setting is different from that of PRF for an adversary with multiple oracles in Sect. 2.2. $I_K^{F,\pi_1}, I_K^{F,\pi_2}, \ldots, I_K^{F,\pi_d}$ 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*

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

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 [16] 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 [16] only covers the case that $p_{\{\pi\}} = 0$ for $\pi \in \boldsymbol{P}(\Sigma^n)$.

Remark 2. The probability p_{Π} should be negligibly small for $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\}$. Let $c_1, c_2, \ldots, c_d$ 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 Lemmas 2 and 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*

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

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

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

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

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

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

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

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

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

1. B selects r from $\{1,\ldots,\ell\}$ uniformly at random.
2. If $r \geq 2$, then B selects functions $(\tilde{\mu}_1,\ldots,\tilde{\mu}_d)$ from $\boldsymbol{F}((\Sigma^w)^{[1,r-1]},\Sigma^n)^d$ 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 $X = X_1\|X_2\|\cdots\|X_l$ 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 $idx : \{1,\ldots,q\} \to \{1,\ldots,q\}$ 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

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

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

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

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

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

Suppose that B is given oracles $(\tilde{\rho}_1,\ldots,\tilde{\rho}_q)$. 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 $\tilde{\rho}_{idx(k)}(\pi_1, \cdot), \ldots, \tilde{\rho}_{idx(k)}(\pi_d, \cdot)$ and $\tilde{\rho}_{idx(k)}(id, \cdot)$ are independent of each other. Thus, B provides A with the oracle $R[r]^{F,\pi_j}_{\mu_j,\xi}$, and

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

Thus,

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

Now, let $(\rho_1, \rho_2, \ldots, \rho_q) \twoheadleftarrow \boldsymbol{F}(\Sigma^n \times \Sigma^w, \Sigma^n)^q$. Then,

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

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

$$\left|\Pr\left[B^{\rho_1[K_1],\ldots,\rho_q[K_q]} = 1\right] - \Pr\left[B^{\tilde{\rho}_1,\ldots,\tilde{\rho}_q} = 1\right]\right| \le q p_\Pi \ .$$

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

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*

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

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 [16], 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 [16].

4 Applications

4.1 PRF with Minimum Padding

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

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

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

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

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

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

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

$C^{F,\{\pi_1,\pi_2\}}$ 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. The proof is omitted due to the page limit.

Corollary 1. *Let π_1 and π_2 be permutations on Σ^n. 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*

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

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.

4.2 Vector-Input PRF

A scheme is proposed to construct a vector-input PRF (vPRF) using instances of FMAC. In the original formalization [26], 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 $F : \Sigma^n \times \Sigma^w \to \Sigma^n$ and $\Pi = \{\pi_1, \pi_2, \ldots, \pi_{2d+2}\} \subset \boldsymbol{P}(\Sigma^n)$. The proposed vector-input function vFMAC $V^{F,\Pi} : \Sigma^n \times (\Sigma^*)^{[0,d]} \to$

Σ^n is defined as follows: For an s-component vector $(S_1, S_2, \ldots, S_s)$ such that $0 \le s \le d$,

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

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 $\Pi = \{\pi_1, \pi_2, \ldots, \pi_{2d+2}\} \subset \boldsymbol{P}(\Sigma^n) \setminus \{id\}$. 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 $\sigma (\ge q - 1)$. Then, there exists an adversary B against F such that*

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

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 Lemmas 4 and 5. The proofs are omitted.

Lemma 4. *Let $\Pi = \{\pi_1, \pi_2, \ldots, \pi_{2d+2}\} \subset \boldsymbol{P}(\Sigma^n) \setminus \{id\}$. Let A be any adversary against $\left\{ C^{F,\{\pi_{2i-1}, \pi_{2i}\}} \,\middle|\, 1 \le i \le d+1 \right\}$ 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*

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

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.

Lemma 5. *Let $\Pi = \{\pi_1, \pi_2, \ldots, \pi_{2d+2}\} \subset \boldsymbol{P}(\Sigma^n) \setminus \{id\}$. 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 $\left\{ C^{F,\{\pi_{2i-1}, \pi_{2i}\}} \,\middle|\, 1 \le i \le d+1 \right\}$ such that*

$$\mathrm{Adv}^{\mathrm{prf}}_{V^{F,\Pi}}(A) \le \mathrm{Adv}^{\mathrm{prfs}}_{\left\{ C^{F,\{\pi_{2i-1}, \pi_{2i}\}} \,\middle|\, 1 \le i \le d+1 \right\}}(B) + \frac{q(q-1)}{2^{n+1}} \ .$$

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.

5 Conclusion

We have presented a MAC function called FMAC, which is cascade of a compression function based on the MDP domain extension. 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.

Acknowledgements. 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 2006. LNCS, vol. 4117, pp. 602–619. Springer, Heidelberg (2006). doi:10.1007/11818175_36
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: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 1–15. Springer, Heidelberg (1996). doi:10.1007/3-540-68697-5_1
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., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003). doi:10.1007/3-540-39200-9_31
6. Bellare, M., Ristenpart, T.: Multi-property-preserving hash domain extension and the EMD transform. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 299–314. Springer, Heidelberg (2006). doi:10.1007/11935230_20
7. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Sponge functions. In: ECRYPT Hash Workshop (2007)
8. Bertoni, G., Daemen, J., Peeters, M., Assche, G.: Duplexing the sponge: single-pass authenticated encryption and other applications. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 320–337. Springer, Heidelberg (2012). doi:10.1007/978-3-642-28496-0_19
9. Black, J., Rogaway, P.: CBC MACs for arbitrary-length messages: the three-key constructions. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 197–215. Springer, Heidelberg (2000). doi:10.1007/3-540-44598-6_12
10. Black, J., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 384–397. Springer, Heidelberg (2002). doi:10.1007/3-540-46035-7_25
11. 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 [18], pp. 112–128

12. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993). doi:10.1007/3-540-57332-1_17
13. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptology **10**(3), 151–162 (1997)
14. FIPS PUB 180–4: secure hash standard (SHS), March 2012
15. FIPS PUB 202: SHA-3 standard: permutation-based hash and extendable-output functions (2015)
16. Hirose, S., Park, J.H., Yun, A.: A simple variant of the Merkle-Damgård scheme with a permutation. J. Cryptology **25**(2), 271–309 (2012)
17. Iwata, T., Kurosawa, K.: OMAC: one-key CBC MAC. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 129–153. Springer, Heidelberg (2003). doi:10.1007/978-3-540-39887-5_11
18. Joux, A., Youssef, A. (eds.): SAC 2014. LNCS, vol. 8781. Springer, Heidelberg (2014)
19. 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/
20. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. IEEE Trans. Inf. Theory **56**(10), 5366–5374 (2010)
21. Mennink, B.: XPX: Generalized tweakable Even-Mansour with improved security guarantees. Cryptology ePrint Archive, Report 2015/476 (2015). http://eprint.iacr.org/
22. Minematsu, K.: A short universal hash function from bit rotation, and applications to blockcipher modes. In: Susilo, W., Reyhanitabar, R. (eds.) ProvSec 2013. LNCS, vol. 8209, pp. 221–238. Springer, Heidelberg (2013). doi:10.1007/978-3-642-41227-1_13
23. Mouha, N., Mennink, B., Herrewege, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: an efficient MAC algorithm for 32-bit microcontrollers. In: Joux and Youssef [18], pp. 306–323
24. Nandi, M.: Fast and secure CBC-type MAC algorithms. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 375–393. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03317-9_23
25. NIST Special Publication 800-38B: Recommendation for block cipher modes of operation: The CMAC mode for authentication (2005)
26. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 373–390. Springer, Heidelberg (2006). doi:10.1007/11761679_23
27. 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)
28. Yasuda, K.: Boosting Merkle-Damgård hashing for message authentication. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 216–231. Springer, Heidelberg (2007). doi:10.1007/978-3-540-76900-2_13
29. Yasuda, K.: "Sandwich" is indeed secure: how to authenticate a message with just one hashing. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 355–369. Springer, Heidelberg (2007)
30. Yasuda, K.: HMAC without the "second" key. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 443–458. Springer, Heidelberg (2009)