PAPER *Special Section on Cryptography and Information Security*

A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Applications

Shoichi HIROSE[†a)], ***Member***, **Hidenori KUWAKADO**[††], ***Senior Member***, ***and*** **Hirotaka YOSHIDA**[†††], ***Member***

SUMMARY This paper discusses a mode for pseudorandom functions (PRFs) based on the hashing mode of Lesamnta-LW and the domain extension called Merkle-Damgård with permutation (MDP). The hashing mode of Lesamnta-LW is a plain Merkle-Damgård iteration of a block cipher with its key size half of its block size. First, a PRF mode is presented which produces multiple independent PRFs with multiple permutations and initialization vectors if the underlying block cipher is a PRP. Then, two applications of the PRF mode are presented. One is a PRF with minimum padding. Here, padding is said to be minimum if the produced message blocks do not include message blocks only with the padded sequence for any non-empty input message. The other is a vector-input PRF using the PRFs with minimum padding.

key words: *compression function, MAC, provable security, pseudorandom function, vector-input PRF*

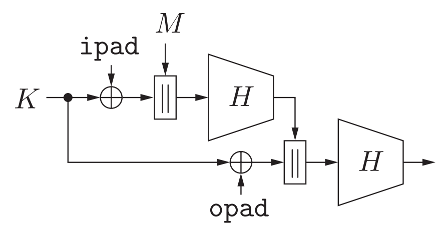

Fig. 1 HMAC. H is a cryptographic hash function. K is a secret key. M is an input message. $\oplus$ represents bitwise XOR operation. $\|$ represents concatenation of sequences. ipad = 0x3636 · · · 36 and opad = 0x5c5c · · · 5c.

1. Introduction

1.1 Background

A pseudorandom function (PRF) is one of the most important elements in cryptography. Informally, it is a keyed function indistinguishable from a random function if the key is chosen uniformly at random and kept secret. It is often used as a function for message authentication (MAC function). It is also used for pseudorandom number generation. A PRF is usually constructed using a block cipher or a cryptographic hash function. We are interested in the latter approach.

Continuing advances of pervasive computing have greatly been increasing the demand for security of devices with constrained resources. To answer to such demand, for cryptographic hash functions, the international standard ISO/IEC 29192-5 [22] has been published, which includes three lightweight hash functions: PHOTON [18], SPONGENT [15] and Lesamnta-LW [19].

In the coming IoT era, many "things" will get connected to the internet and we will enjoy the great amount of benefits, while the risk of cyber attacks will be significantly increased. Examples of the fastest evolving IoT systems can be seen in automotive industry and smart factory (Industry 4.0). Recently, for vehicles, remote software update attracts a lot of attention, and therefore, the international standard ITU-T SG17 [1] referring to ISO/IEC 29192-5 has been published. To ensure security for IoT devices such as electronic control units in a vehicle, cryptographic solutions such as PRFs need to be lightweight in terms of implementation resources, especially for short messages.

HMAC [5] is a widely deployed 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, ipad = 0x3636 · · · 36 and opad = 0x5c5c · · · 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 [16], HMAC invokes the underlying hash function twice. The drawback of this structure is inefficiency for short messages. Such inefficiency may also come from the padding of the underlying hash function based on the Merkle-Damgård strengthening.

1.2 Our Contribution

This paper discusses a keyed mode based on the hashing mode of Lesamnta-LW and the MDP domain extension [20], which is depicted in Fig. 2. It is first shown that the keyed mode produces multiple independent PRFs with multiple permutations and initialization vectors if the underlying block cipher is a PRP. Then, two applications of the mode are presented. First, a PRF with minimum padding is presented. We say that padding is minimum if the produced message blocks do not include message blocks only with the padded sequence for any non-empty input message.

Manuscript received March 21, 2017.
[†]The author is with Faculty of Engineering, University of Fukui, Fukui-shi, 910-8507 Japan.
[††]The author is with Faculty of Informatics, Kansai University, Takatsuki-shi, 569-1095 Japan.
[†††]The author is with National Institute of Advanced Industrial Science and Technology, Tsukuba-shi, 305-8560 Japan.
a) E-mail: hrs_shch@u-fukui.ac.jp
DOI: 10.1587/transfun.E101.A.110

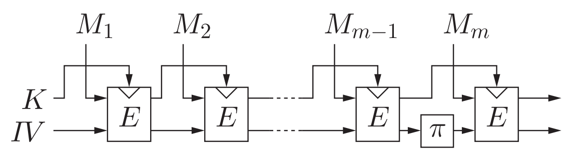

Fig. 2 A keyed mode based on Lesamnta-LW and the MDP domain extension. E is the underlying block cipher, K is a secret key, IV is an initialization vector, and π is a permutation. The input of E from the top is its key input.

Second, a vector-input PRF (vPRF) is constructed using the PRFs with minimum padding. A vPRF is a PRF which takes as input a vector of strings. The presented vPRF is an instantiation of the protected counter sum construction [10] with a variable-input-length PRF based on Lesamnta-LW and MDP.

The basic idea to obtain multiple independent PRFs using the MDP domain extension is from the precedent paper [21] as well as its two applications described above. It is shown that the keyed mode in [21] may produce multiple PRFs if the underlying compression function is a PRF against related-key attacks with respect to the permutations used in the mode. On the other hand, by adjusting the idea in [21] to the hashing mode of Lesamnta-LW, we show that our keyed mode does not require the security against related-key attacks of the underlying block cipher.

1.3 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 [3]. 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 [33] 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 [4] 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.

Various PRF modes of a compression function are also known. The plain Merkle-Damgård cascade is a PRF against adversaries making prefix-free queries if the underlying compression function is a PRF [6]. In the context of multi-property preservation [8], PRF modes such as EMD [8] and MDP [20] are proposed. Yasuda's PRF mode of a compression function in [29] 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 [30].

PRF modes using keyed compression functions were also proposed. The first proposal was XOR MAC [7], which was followed by the protected counter sum construction [10]. It is shown that various hashing modes preserve the PRF security of keyed compression functions [9]. Yasuda proposed PRF modes for keyed compression functions with security beyond birthday [31], [32], [34], [35].

The most related schemes to our proposal are recent keyed sponge constructions [2], [11], [12], [17] and Chaskey [25]. The advantage of our proposal over them is that the PRF property of our proposal requires a weaker security assumption on the underlying primitive. The keyed sponge constructions are shown to be indistinguishable from a uniform random function in the ideal permutation model, that is, on the assumption that the underlying permutation is chosen uniformly at random. Chaskey is also shown to be indistinguishable from a uniform random function in the ideal permutation model. Chaskey-B is shown to be a PRF if the underlying block cipher is a PRP against related key-attacks.

Minimum padding is already common among block-cipher-based MAC functions such as CMAC [27] and PMAC [14]. CMAC, which is based on OMAC (One-key CBC-MAC) [23], originated from XCBC [13]. The idea to finalize the iteration with multiple permutations is used in the secure CBC-MAC variants GCBC1 and GCBC2 [26].

Rogaway and Shrimpton [28] 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 [24] also proposed a vPRF using his universal hash function based on bit rotation.

1.4 Organization

Section 2 gives notations and definitions used in the remaining parts of the paper. It is shown in Sect. 3 that the keyed mode based on Lesamnta-LW and MDP may produce multiple independent PRFs with multiple permutations and multiple initialization vectors. Based on the result in Sect. 3, the PRF with minimum padding and the vPRF are presented and their security is confirmed in the manner of provable security in Sect. 4 and Sect. 5, respectively. 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. Let $(\Sigma^l)^* = \bigcup_{i \ge 0}(\Sigma^l)^i$ and $(\Sigma^l)^+ = \bigcup_{i \ge 1}(\Sigma^l)^i$. For $k_1 \le k_2$, 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 $K \in \mathcal{K}$. $f(K,x)$ is often denoted by $f_K(x)$.

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. Let $\boldsymbol{C}(\kappa,n)$ be the set of all block ciphers with key size κ and block size n. A block cipher in $\boldsymbol{C}(\kappa,n)$ is called a (κ,n) block cipher.

Let $\Pi \subset \boldsymbol{P}(\mathcal{D})$. We say that Π is pairwise everywhere distinct if, for any pair of distinct permutations $\pi,\pi' \in \Pi$, $\pi(x) \neq \pi'(x)$ for every $x \in \mathcal{D}$.

2.2 Pseudorandom Functions and Permutations

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 $\rho \twoheadleftarrow \boldsymbol{F}(\mathcal{D},\mathcal{R})$. The prp-advantage of A against f is defined as

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

where $K \twoheadleftarrow \mathcal{K}$ and $\rho \twoheadleftarrow \boldsymbol{P}(\mathcal{D})$. In these notations, adversary A is regarded as a random variable.

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

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

$$\mathrm{Adv}_f^{m\text{-prf}}(A) = \left|\Pr[A^{f_{K_1},f_{K_2},\ldots,f_{K_m}}=1] - \Pr[A^{\rho_1,\rho_2,\ldots,\rho_m}=1]\right| ,$$

where $(K_1,K_2,\ldots,K_m) \twoheadleftarrow \mathcal{K}^m$ and $(\rho_1,\rho_2,\ldots,\rho_m) \twoheadleftarrow \boldsymbol{F}(\mathcal{D},\mathcal{R})^m$. $\mathrm{Adv}_f^{m\text{-prp}}$ can be defined similarly.

The following lemma is a paraphrase of Lemma 3.3 in [6]:

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 of 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.

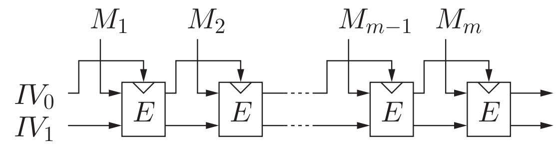

Fig. 3 The hashing mode of Lesamnta-LW.

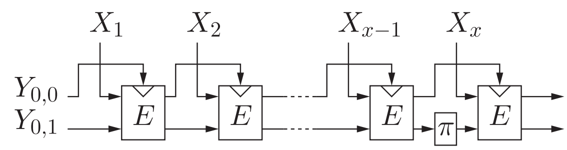

Fig. 4 $J^{E,\pi}(Y_0, X_1\|X_2\|\cdots\|X_x)$.

2.3 The Hashing Mode of Lesamnta-LW and Its Variant with MDP

The hashing mode of Lesamnta-LW [19] is given in Fig. 3. It is the plain Merkle-Damgård iteration of a block cipher E in $\boldsymbol{C}(n/2,n)$, where n is a positive even integer. The input of E from the top is its key input. $IV_0\|IV_1 \in \Sigma^n$ is an initialization vector, where $|IV_0| = |IV_1| = n/2$. $M_1,M_2,\ldots,M_m$ are message blocks, where $M_i \in \Sigma^{n/2}$ for $i=1,2,\ldots,m$.

Now, let us introduce the variant of the hashing mode of Lesamnta-LW with the MDP domain extension [20]. Hereafter, it is assumed that the underlying block cipher E is in $\boldsymbol{C}(w,n)$, where $w < n$. The MDP variant with a permutation π on Σ^{n-w} is the function $J^{E,\pi} : \Sigma^n \times (\Sigma^w)^+ \to \Sigma^n$, which is defined as follows: For $X_1,X_2,\ldots,X_x \in \Sigma^w$ and $Y_0 \in \Sigma^n$,

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

such that

$$Y_i \leftarrow \begin{cases} E_{Y_{i-1,0}}(X_i\|Y_{i-1,1}) & (1 \leq i \leq x-1) \\ E_{Y_{i-1,0}}(X_i\|\pi(Y_{i-1,1})) & (i = x) \end{cases} ,$$

where $Y_j = Y_{j,0}\|Y_{j,1} \in \Sigma^n$ and $|Y_{j,0}| = w$ for $0 \leq j \leq x$. It is depicted in Fig. 4. As it will be seen later, π need not be a cryptographic primitive. Thus, the computational overhead of π can be small.

3. Multiple PRFs based on Lesamnta-LW

In this section, it is shown that the MDP variant of the Lesamnta-LW hashing mode may produce multiple independent PRFs with a single secret key using multiple permutations and initialization vectors.

Let $J_{IV}^{E,\pi} : \Sigma^w \times (\Sigma^w)^+ \to \Sigma^n$ be a keyed function such that $J_{IV}^{E,\pi}(K,X) = J^{E,\pi}(K\|IV, X)$, where $K \in \Sigma^w$, $IV \in \Sigma^{n-w}$ and $X \in (\Sigma^w)^+$. K is a secret key and IV is an initialization vector. $J_{IV}^{E,\pi}(K,\cdot)$ is also denoted by $J_{IV,K}^{E,\pi}(\cdot)$. For $\Pi \subset \boldsymbol{P}(\Sigma^{n-w})$ and $\mathcal{V} \subset \Sigma^{n-w}$, let

$$J_{\mathcal{V}}^{E,\Pi} = \left\{ J_{IV}^{E,\pi} \,\middle|\, IV \in \mathcal{V} \wedge \pi \in \Pi \right\} .$$

Let $\mathcal{V} = \{IV_i \mid 1 \le j \le a\}$ and $\Pi = \{\pi_j \mid 1 \le j \le d\}$. Let A be an adversary against $J^{E,\Pi}_{\mathcal{V}}$. The advantage of A is defined by

$$\mathrm{Adv}^{\mathrm{prfs}}_{J^{E,\Pi}_{\mathcal{V}}}(A) = \left|\Pr\left[A^{\langle J^{E,\pi_j}_{IV_i,K}\rangle^{1\le j\le d}_{1\le i\le a}} = 1\right] - \Pr\left[A^{\langle \rho_{i,j}\rangle^{1\le j\le d}_{1\le i\le a}} = 1\right]\right|$$

for $K \twoheadleftarrow \Sigma^w$ and $\left\langle \rho_{i,j}\right\rangle^{1\le j\le d}_{1\le i\le a} \twoheadleftarrow \boldsymbol{F}((\Sigma^w)^+, \Sigma^n)^{a\times d}$, where

$$\left\langle J^{E,\pi_j}_{IV_i,K}\right\rangle^{1\le j\le d}_{1\le i\le a} = \left(J^{E,\pi_1}_{IV_1,K}, J^{E,\pi_2}_{IV_1,K}, \ldots, J^{E,\pi_d}_{IV_1,K}, J^{E,\pi_1}_{IV_2,K}, \ldots, J^{E,\pi_d}_{IV_a,K}\right)$$

and

$$\left\langle \rho_{i,j}\right\rangle^{1\le j\le d}_{1\le i\le a} = (\rho_{1,1}, \rho_{1,2}, \ldots, \rho_{1,d}, \rho_{2,1}, \ldots, \rho_{a,d}) \quad .$$

Notice that the setting is different from that of PRF for an adversary with multiple oracles in Sect. 2.2. Only a single key K is used for $\left\langle J^{E,\pi_j}_{IV_i,K}\right\rangle^{1\le j\le d}_{1\le i\le a}$.

The following theorem states that $J^{E,\Pi}_{\mathcal{V}}$ produces multiple independent PRFs with a single key if E is a PRP.

Theorem 1 Let $\mathcal{V} \subset \Sigma^{n-w}$ and $\Pi \subset \boldsymbol{P}(\Sigma^{n-w})$. Suppose that $\Pi \cup \{id\}$ is pairwise everywhere distinct and that $\pi(IV) \ne \pi'(IV')$ for any $\pi, \pi' \in \Pi \cup \{id\}$ and $IV, IV' \in \mathcal{V}$ such that $(\pi, IV) \ne (\pi', IV')$. Let A be any adversary against $J^{E,\Pi}_{\mathcal{V}}$ 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 E such that

$$\mathrm{Adv}^{\mathrm{prfs}}_{J^{E,\Pi}_{\mathcal{V}}}(A) \le \ell q \cdot \mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{\ell q(q-1)}{2^{n+1}} \quad .$$

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

Remark 1 Let t_{v} and t_{p} be integers such that $t_{\mathrm{v}} + t_{\mathrm{p}} = n - w$. Let $\mathcal{V} = \{IV_1, IV_2, \ldots, IV_a\}$ and $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\}$. Let $v_1, v_2, \ldots, v_a$ be distinct constants in $\Sigma^{t_{\mathrm{v}}}$. Let $c_1, c_2, \ldots, c_d$ be distinct nonzero constants in $\Sigma^{t_{\mathrm{p}}}$. Suppose that $IV_i = v_i \| 0^{t_{\mathrm{p}}}$ for $1 \le i \le a$ and that $\pi_j(x) = x \oplus (0^{t_{\mathrm{v}}} \| c_j)$ for $1 \le j \le d$. Then,

- $\Pi \cup \{id\}$ is pairwise everywhere distinct, and
- since $\pi_j(IV_i) = v_i \| c_j$, $\pi_j(IV_i) \ne \pi_{j'}(IV_{i'})$ if $(i,j) \ne (i',j')$.

Theorem 1 immediately follows from Lemma 2 and Lemma 3.

Lemma 2 Let $\mathcal{V} \subset \Sigma^{n-w}$ and $\Pi \subset \boldsymbol{P}(\Sigma^{n-w})$. Suppose that $\Pi \cup \{id\}$ is pairwise everywhere distinct and that $\pi(IV) \ne \pi'(IV')$ for any $\pi, \pi' \in \Pi \cup \{id\}$ and $IV, IV' \in \mathcal{V}$ such that $(\pi, IV) \ne (\pi', IV')$. Let A be any adversary against $J^{E,\Pi}_{\mathcal{V}}$ 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 E with access to q oracles such that

$$\mathrm{Adv}^{\mathrm{prfs}}_{J^{E,\Pi}_{\mathcal{V}}}(A) \le \ell \cdot \mathrm{Adv}^{q\text{-prf}}_{E}(B) \quad .$$

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

Proof Let $\mathcal{V} = \{IV_1, IV_2, \ldots, IV_a\}$ and $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\}$. Let $X = X_1 \| X_2 \| \cdots \| X_x$, where $1 \le x \le \ell$ and $|X_i| = w$ for $1 \le i \le x$. For $1 \le i_1 \le i_2 \le x$, let $X_{[i_1,i_2]} = X_{i_1} \| X_{i_1+1} \| \cdots \| X_{i_2}$. For $l \in \{0, 1, \ldots, \ell\}$ and two functions $\mu : (\Sigma^w)^{[1,\ell]} \to \Sigma^n$ and $\xi : (\Sigma^w)^{[0,\ell-1]} \to \Sigma^n$, let $R[l]^{E,\pi}_{\mu,\xi} : (\Sigma^w)^{[1,\ell]} \to \Sigma^n$ be a function such that

$$R[l]^{E,\pi}_{\mu,\xi}(X) = \begin{cases} \mu(X) & \text{if } x \le l, \\ J^{E,\pi}(\xi(X_{[1,l]}), X_{[l+1,x]}) & \text{if } x \ge l+1, \end{cases}$$

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

$$P_l = \Pr\left[A^{\langle R[l]^{E,\pi_j}_{\mu_{i,j},\xi_i}\rangle^{1\le j\le d}_{1\le i\le a}} = 1\right] \ ,$$

where $(\mu_{1,1}, \ldots, \mu_{a,d}) \twoheadleftarrow \boldsymbol{F}((\Sigma^w)^{[1,\ell]}, \Sigma^n)^{a\times d}$ and

$$\xi_i(X_{[1,l]}) = \begin{cases} K \| IV_i & \text{if } l = 0 \\ \tilde{\xi}_i(X_{[1,l]}) & \text{otherwise} \end{cases}$$

for $K \twoheadleftarrow \Sigma^w$ and $(\tilde{\xi}_1, \ldots, \tilde{\xi}_a) \twoheadleftarrow \boldsymbol{F}((\Sigma^w)^{[1,\ell-1]}, \Sigma^n)^a$. Then, the advantage of A is

$$\mathrm{Adv}^{\mathrm{prfs}}_{J^{E,\Pi}_{\mathcal{V}}}(A) = |P_0 - P_\ell| \ .$$

The algorithm of an adversary B against E with q oracles is described below. Let $(g_1, \ldots, g_q)$ be the oracles of B. They are either $(E_{K_1}, E_{K_2}, \ldots, E_{K_q})$ or $(\rho_1, \rho_2, \ldots, \rho_q)$ such that $(K_1, \ldots, K_q) \twoheadleftarrow (\Sigma^n)^q$ and $(\rho_1, \ldots, \rho_q) \twoheadleftarrow \boldsymbol{F}(\Sigma^n, \Sigma^n)^q$, respectively. B uses A as a subroutine.

1. B selects r from $\{1, \ldots, \ell\}$ uniformly at random.
2. If $r \ge 2$, then B selects functions $(\tilde{\mu}_{1,1}, \ldots, \tilde{\mu}_{a,d})$ from $\boldsymbol{F}((\Sigma^w)^{[1,r-1]}, \Sigma^n)^{a\times d}$ uniformly at random. Actually, B simulates $\tilde{\mu}_{i,j}$ with lazy evaluation.
3. B runs A. Finally, B outputs the output of A.

For $1 \le k \le q$ and $1 \le x \le \ell$, let $X = X_1 \| X_2 \| \cdots \| X_x$ be the k-th query made by A during the execution of A. Suppose that X is a query to the (i,j)-th oracle of A. If $x \ge r$, then B makes a query to the $idx(k)$-th oracle $g_{idx(k)}$, where $idx : \{1, \ldots, q\} \to \{1, \ldots, q\}$ is a function defined below:

- If $r = 1$, then $idx(k) = 1$ for $1 \le k \le q$.
- If $r \ge 2$, then
  - $idx(k) = idx(k')$ if there exists a previous k'-th query X' $(k' < k)$ such that it is a query to the (i, j')-th oracle for some $1 \le j' \le d$ and $X'_{[1,r-1]} =$

$X_{[1,r-1]}$, and
– $idx(k) = k$ otherwise.

For the query to the $idx(k)$-th oracle, B also chooses $\nu(k)$ as follows:

- If $r = 1$, then $\nu(k) = IV_i$.
- If $r \geq 2$, then $\nu(k) = \nu(k')$ if $idx(k) = idx(k')$ for some $k' < k$ and $\nu(k) \twoheadleftarrow \Sigma^{n-w}$ if $idx(k) = k$.

The query made by B is $(X_r \| \pi_j(\nu(k)))$ if $x = r$ and $(X_r \| \nu(k))$ if $x \geq r+1$. The answer of B to X is

$$\begin{cases} \tilde{\mu}_{i,j}(X) & \text{if } x \leq r-1, \\ g_{idx(k)}(X_r \| \pi_j(\nu(k))) & \text{if } x = r, \\ J^{E,\pi_j}(g_{idx(k)}(X_r \| \nu(k)), X_{[r+1,x]}) & \text{if } x \geq r+1. \end{cases}$$

Now, suppose that B is given $(E_{K_1}, \ldots, E_{K_q})$ as oracles. Then, the answer of B to X is

$$\begin{cases} \tilde{\mu}_{i,j}(X) & \text{if } x \leq r-1, \\ E_{K_{idx(k)}}(X_r \| \pi_j(\nu(k))) & \text{if } x = r, \\ J^{E,\pi_j}(E_{K_{idx(k)}}(X_r \| \nu(k)), X_{[r+1,x]}) & \text{if } x \geq r+1. \end{cases}$$

If $r = 1$, then $idx(k) = 1$ and $\nu(k) = IV_i$ for $1 \leq k \leq q$. If $r \geq 2$, then $K_{idx(k)} \| \nu(k)$ is chosen uniformly at random from Σ^n for a new pair of i and $X_{[1,r-1]}$. Thus, B provides A with the oracle $R[r-1]^{E,\pi_j}_{\mu_{i,j},\xi_i}$, and

$$\begin{aligned} &\Pr\left[B^{E_{K_1},\ldots,E_{K_q}} = 1\right] \\ &= \sum_{u=1}^{\ell} \Pr\left[r = u \wedge B^{E_{K_1},\ldots,E_{K_q}} = 1\right] \\ &= \frac{1}{\ell} \sum_{u=1}^{\ell} \Pr\left[B^{E_{K_1},\ldots,E_{K_q}} = 1 \,\middle|\, r = u\right] \\ &= \frac{1}{\ell} \sum_{u=1}^{\ell} \Pr\left[A^{\left\langle R[u-1]^{E,\pi_j}_{\mu_{i,j},\xi_i} \right\rangle^{1\leq j\leq d}_{1\leq i\leq a}} = 1\right] \\ &= \frac{1}{\ell} \sum_{u=1}^{\ell} P_{u-1} \ . \end{aligned}$$

Suppose that B is given oracles $(\rho_1, \ldots, \rho_q)$. Then, the answer of B to X is

$$\begin{cases} \tilde{\mu}_{i,j}(X) & \text{if } x \leq r-1, \\ \rho_{idx(k)}(X_r \| \pi_j(\nu(k))) & \text{if } x = r, \\ J^{E,\pi_j}(\rho_{idx(k)}(X_r \| \nu(k)), X_{[r+1,x]}) & \text{if } x \geq r+1. \end{cases}$$

If $r = 1$, then $idx(k) = 1$ and $\nu(k) = IV_i$ for $1 \leq k \leq q$. The functions in $\{\rho_1(\cdot \| \pi(IV)) \,|\, \pi \in \Pi \cup \{id\},\ IV \in \mathcal{V}\}$ are independent of each other since $\pi(IV) \neq \pi'(IV')$ for any $\pi, \pi' \in \Pi \cup \{id\}$ and $IV, IV' \in \mathcal{V}$ such that $(\pi, IV) \neq (\pi', IV')$. If $r \geq 2$, then $idx(k)$ is fixed only by $(i, X_{[1,r-1]})$ and $\nu(k)$ is chosen uniformly at random only when $idx(k) = k$. In addition, $\Pi \cup \{id\}$ is pairwise everywhere distinct. Thus, B provides A with the oracle $R[r]^{E,\pi_j}_{\mu_{i,j},\xi_i}$, and

$$\Pr[B^{\rho_1,\ldots,\rho_q} = 1] = \frac{1}{\ell} \sum_{i=1}^{\ell} P_i \ .$$

Thus,

$$\begin{aligned} &\mathrm{Adv}^{q\text{-prf}}_{E}(B) \\ &= \left|\Pr\left[B^{E_{K_1},\ldots,E_{K_q}} = 1\right] - \Pr\left[B^{\rho_1,\ldots,\rho_q} = 1\right]\right| \\ &= \left|\frac{1}{\ell}\sum_{i=1}^{\ell} P_{i-1} - \frac{1}{\ell}\sum_{i=1}^{\ell} P_i\right| = \frac{|P_0 - P_\ell|}{\ell} \\ &= \frac{1}{\ell}\,\mathrm{Adv}^{\mathrm{prfs}}_{J^{E,\Pi}_{\mathcal{V}}}(A) \ . \end{aligned}$$

There may exist an adversary with the same amounts of resources as B and larger advantage. Let us call it B again. □

Lemma 3 (Lemma 3 of [19]) Let A be any adversary with m oracles against E running in time at most t, and making at most q queries. Then, there exists an adversary B against E such that

$$\mathrm{Adv}^{m\text{-prf}}_{E}(A) \leq m \cdot \mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{q(q-1)}{2^{n+1}} \ .$$

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

4. PRF with Minimum Padding

Based on the result in the previous section, a PRF mode with minimum padding is proposed and its security is confirmed in this section. Then, the proposed scheme is compared with two PRF modes based on Lesamnta-LW in [19] in terms of efficiency.

4.1 The Proposed Scheme

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

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

where t is the minimum non-negative integer such that $|M| + 1 + t \equiv 0 \pmod{w}$. 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 $1 \leq i \leq m$. $m = 1$ if $|M| = 0$, and $m = \lceil |M|/w \rceil$ if $|M| > 0$. $\bar{M}_i$ is called the i-th block of $\mathsf{pad}(M)$.

The proposed function $L^{E,\{\pi_1,\pi_2\}}_{IV} : \Sigma^w \times \Sigma^* \to \Sigma^n$ based on Lesamnta-LW and MDP is defined by

$$L^{E,\{\pi_1,\pi_2\}}_{IV}(K, M) =$$

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

$L_{IV}^{E,\{\pi_1,\pi_2\}}$ is shown to be a PRF if the underlying block cipher E is a PRP.

Theorem 2 Let $IV \in \Sigma^{n-w}$. Let $\{\pi_1, \pi_2\} \subset \boldsymbol{P}(\Sigma^{n-w})$ and suppose that $\{\pi_1, \pi_2, id\}$ is pairwise everywhere distinct. Let A be any adversary against $L_{IV}^{E,\{\pi_1,\pi_2\}}$ 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 E such that

$$\mathrm{Adv}^{\mathrm{prf}}_{L_{IV}^{E,\{\pi_1,\pi_2\}}}(A) \leq \ell q \cdot \mathrm{Adv}^{\mathrm{prp}}_E(B) + \frac{\ell q(q-1)}{2^{n+1}} \ .$$

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

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

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

Notice that

$$\Pr[\hat{A}^{J_{IV,K}^{E,\pi_1}, J_{IV,K}^{E,\pi_2}} = 1] = \Pr[A^{L_{IV,K}^{E,\{\pi_1,\pi_2\}}} = 1]$$

and

$$\Pr[\hat{A}^{\rho_1,\rho_2} = 1] = \Pr[A^{\rho} = 1] \ ,$$

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

$$\begin{aligned} \mathrm{Adv}^{\mathrm{prf}}_{L_{IV}^{E,\{\pi_1,\pi_2\}}}(A) &= \mathrm{Adv}^{\mathrm{prfs}}_{J_{IV}^{E,\{\pi_1,\pi_2\}}}(\hat{A}) \\ &\leq \ell q \cdot \mathrm{Adv}^{\mathrm{prp}}_E(B) + \frac{\ell q(q-1)}{2^{n+1}} \ . \end{aligned}$$

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

Remark 2 A PRF with minimum padding can also be constructed with a single permutation and two distinct initialization vectors. However, $L_{IV}^{E,\{\pi_1,\pi_2\}}$ is much better than this construction. For the PRF with a single permutation and two distinct initialization vectors, users have to know the length of an input message in advance since it determines which initialization vector should be chosen.

4.2 Discussion

In [19], the authors presented two PRF modes based on Lesamnta-LW, which are called a keyed-via-IV (KIV) mode and a key-prefix (KP) mode.

Let $n = 256$ and $w = 128$ for $J^{E,\pi}$, as is specified for Lesamnta-LW. Let $\mathsf{pad}_{\mathrm{L}}$ is the padding function of Lesamnta-LW and $IV_{\mathrm{L}} \in \Sigma^{256}$ is the initialization vector of Lesamnta-LW. Let $\mathsf{chop} : \Sigma^{256} \to \Sigma^{128}$ be the function which simply outputs the latter half of the input. Then, the KIV mode of Lesamnta-LW is $\mathsf{chop}(J^{E,\pi}(K, \mathsf{pad}_{\mathrm{L}}(M)))$ and the KP mode is $\mathsf{chop}(J^{E,\pi}(IV_{\mathrm{L}}, \mathsf{pad}_{\mathrm{L}}(K' \| M)))$, where $K \in \Sigma^{256}$ and $K' \in \Sigma^{128}$ are secret keys and $M \in \Sigma^*$ is a message input of length at most $2^{64} - 1$.

For $X \in \Sigma^*$ such that $|X| \leq 2^{64} - 1$, $\mathsf{pad}_{\mathrm{L}}(X) = X \| 10^{t+63} \| \mathsf{len}_{64}(X)$, where $\mathsf{len}_{64}(X)$ is the 64-bit binary representation of $|X|$ and t is the minimum non-negative integer such that $|X| + t \equiv 0 \pmod{128}$.

Suppose that input M is not the empty sequence. Then, the number of invocations of E is $\lceil |M|/128 \rceil + 1$ for the KIV mode, $\lceil |M|/128 \rceil + 2$ for the KP mode, and $\lceil |M|/128 \rceil$ for the proposed mode $L_{IV}^{E,\{\pi_1,\pi_2\}}$. Thus, $L_{IV}^{E,\{\pi_1,\pi_2\}}$ is the most efficient, especially for short messages.

The advantage of the KP mode is that it uses the hash function Lesamnta-LW as it is.

The output of $L_{IV}^{E,\{\pi_1,\pi_2\}}$ is twice as long as those of the KIV mode and the KP mode. It may be advantageous when used for pseudorandom bit generation.

5. Vector-Input PRF

5.1 The Proposed Scheme

A scheme is proposed to construct a vector-input PRF (vPRF) using instances of the PRF presented in Sect. 4. In the original formalization [28], 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 a be a positive integer, which is the maximum number of the components in an input vector. Let $\Pi = \{\pi_1, \pi_2\} \subset \boldsymbol{P}(\Sigma^{n-w})$ and $\mathcal{V} = \{IV_0, IV_1, \ldots, IV_a\} \subset \Sigma^{n-w}$. The proposed vector-input function based on Lesamnta-LW $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}} : \Sigma^w \times (\Sigma^*)^{[0,a]} \to \Sigma^n$ is defined as follows: For an s-component vector $(S_1, \ldots, S_s)$ such that $0 \leq s \leq a$,

$$\begin{aligned} &vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}(K, (S_1, S_2, \ldots, S_s)) \\ &= \begin{cases} L_{IV_0}^{E,\{\pi_1,\pi_2\}}(K, \varepsilon) & \text{if } s = 0, \\ L_{IV_0}^{E,\{\pi_1,\pi_2\}}\Big(K, \bigoplus_{i=1}^{s} L_{IV_i}^{E,\{\pi_1,\pi_2\}}(K, S_i)\Big) & \text{if } s \geq 1. \end{cases} \end{aligned}$$

It is shown that $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ is a vPRF if E is a PRP.

Theorem 3 Let $\mathcal{V} = \{IV_0, IV_1, \ldots, IV_a\} \subset \Sigma^{n-w}$. Let $\{\pi_1, \pi_2\} \subset \boldsymbol{P}(\Sigma^{n-w})$ and suppose that $\{\pi_1, \pi_2, id\}$ is pairwise everywhere distinct. Let A be any adversary against $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ 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 the total number of the vector components in all of the queries is at most σ. Then, there exists an adversary B against E such that

$$\mathrm{Adv}^{\mathrm{prf}}_{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V}}}(A) \le \ell(\sigma+q)\,\mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{\ell(\sigma+q)(\sigma+q-1)+q(q-1)}{2^{n+1}} \ .$$

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

Theorem 3 directly follows from Lemmas 4 and 5.

Lemma 4 Let $\mathcal{V} = \{IV_0, IV_1, \dots, IV_a\} \subset \Sigma^{n-w}$. Let $\{\pi_1,\pi_2\} \subset \boldsymbol{P}(\Sigma^{n-w})$ and suppose that $\{\pi_1,\pi_2,id\}$ is pairwise everywhere distinct. Let A be any adversary against $vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V}}$ 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 the total number of the vector components in all of the queries is at most σ. Then, there exists an adversary B against $\{L^{E,\{\pi_1,\pi_2\}}_{IV_i} \mid 0 \le i \le a\}$ such that

$$\mathrm{Adv}^{\mathrm{prf}}_{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V}}}(A) \le \mathrm{Adv}^{\mathrm{prfs}}_{\{L^{E,\{\pi_1,\pi_2\}}_{IV_i} \mid 0\le i\le a\}}(B) + \frac{q(q-1)}{2^{n+1}} \ .$$

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

$$\mathrm{Adv}^{\mathrm{prf}}_{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V}}}(A) = \left|\Pr[A^{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V},K}} = 1] - \Pr[A^{\rho} = 1]\right| \ ,$$

where $K \twoheadleftarrow \Sigma^w$ and $\rho \twoheadleftarrow \boldsymbol{F}((\Sigma^*)^{[0,a]}, \Sigma^n)$.

Let $\rho_i : \Sigma^* \to \Sigma^n$ for $0 \le i \le a$. Let $Q^{\rho_0,\dots,\rho_a} : (\Sigma^*)^{[0,a]} \to \Sigma^n$ be a vector-input function such that

$$Q^{\rho_0,\dots,\rho_a}(S_1,\dots,S_s) = \begin{cases} \rho_0(\varepsilon) & \text{if } s=0,\\ \rho_0\left(\bigoplus_{i=1}^{s} \rho_i(S_i)\right) & \text{if } s \ge 1.\end{cases}$$

$Q^{\rho_0,\dots,\rho_a}$ is obtained from $vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V},K}$ simply by replacing $L^{E,\{\pi_1,\pi_2\}}_{IV_i,K}$ with ρ_i for $0 \le i \le a$. Then,

$$\mathrm{Adv}^{\mathrm{prf}}_{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V}}}(A) \le \left|\Pr[A^{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V},K}} = 1] - \Pr[A^{Q^{\rho_0,\dots,\rho_a}} = 1]\right| + \left|\Pr[A^{Q^{\rho_0,\dots,\rho_a}} = 1] - \Pr[A^{\rho} = 1]\right| \ , \quad (1)$$

where $K \twoheadleftarrow \Sigma^w$, $(\rho_0,\dots,\rho_a) \twoheadleftarrow \boldsymbol{F}(\Sigma^*, \Sigma^n)^{a+1}$ and $\rho \twoheadleftarrow \boldsymbol{F}((\Sigma^*)^{[0,a]}, \Sigma^n)$.

For the first term of the upper bound of Eq. (1), let B be an adversary against $\{L^{E,\{\pi_1,\pi_2\}}_{IV_i} \mid 0 \le i \le a\}$. Let $(g_0, g_1, \dots, g_a)$ be the oracles given to B, which are either $(L^{E,\{\pi_1,\pi_2\}}_{IV_0,K}, L^{E,\{\pi_1,\pi_2\}}_{IV_1,K}, \dots, L^{E,\{\pi_1,\pi_2\}}_{IV_a,K})$ or $(\rho_0, \rho_1, \dots, \rho_a)$. B runs A. For each query $(S_1, S_2, \dots, S_s)$ by A, B returns $g_0(\varepsilon)$ if $s = 0$ and $g_0\left(\bigoplus_{i=1}^{s} g_i(S_i)\right)$ if $s \ge 1$. Finally, B outputs the output of A. Thus,

$$\left|\Pr[A^{vL^{E,\{\pi_1,\pi_2\}}_{\mathcal{V},K}} = 1] - \Pr[A^{Q^{\rho_0,\dots,\rho_a}} = 1]\right| = \mathrm{Adv}^{\mathrm{prfs}}_{\{L^{E,\{\pi_1,\pi_2\}}_{IV_i,K} \mid 0\le i\le a\}}(B) \ .$$

The run time of B approximately equals that of A. The number of queries made by B to its oracles is at most $(\sigma+q)$ and the length of each query is at most ℓw.

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 $1 \le i \le q$ and $1 \le j \le a$,
   - $Z_i \twoheadleftarrow \Sigma^n$ for $1 \le i \le q$, and
   - $bad \leftarrow 0$.
2. During the interaction with A, return Z_i to the i-th query made by A.
3. For $1 \le i \le q$, let $\boldsymbol{S}_i = (S_{i,1}, S_{i,2}, \dots, S_{i,s_i})$ be the i-th query made by A, where $0 \le s_i \le a$. For $1 \le j \le s_i$,
   - $Y_{i,j} \twoheadleftarrow \Sigma^n$ if $S_{i,j}$ is new, that is, $S_{i,j} \ne S_{i',j}$ for any i' such that $i' < i$, and
   - $Y_{i,j} \leftarrow Y_{i',j}$ if $S_{i,j}$ is not new.
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, $\Pr\left[A^R = 1\right] = \Pr[A^{\rho} = 1]$. As long as $bad = 0$, R is also identical to $Q^{\rho_0,\dots,\rho_a}$. Notice that

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

Thus,

$$\left|\Pr[A^{Q^{\rho_0,\dots,\rho_a}} = 1] - \Pr[A^{\rho} = 1]\right| \le \frac{q(q-1)}{2^{n+1}} \ .$$

□

Lemma 5 Let $\mathcal{V} = \{IV_0, IV_1, \dots, IV_a\} \subset \Sigma^{n-w}$. Let $\{\pi_1,\pi_2\} \subset \boldsymbol{P}(\Sigma^{n-w})$ and suppose that $\{\pi_1,\pi_2,id\}$ is pairwise everywhere distinct. Let A be any adversary against $\{L^{E,\{\pi_1,\pi_2\}}_{IV_i} \mid 0 \le i \le a\}$ 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 E such that

$$\mathrm{Adv}^{\mathrm{prfs}}_{\{L^{E,\{\pi_1,\pi_2\}}_{IV_i} \mid 0\le i\le a\}}(A) \le$$

$$\ell q \, \mathrm{Adv}_E^{\mathrm{prp}}(B) + \frac{\ell q(q-1)}{2^{n+1}} \ .$$

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

Proof Let $\hat{A}$ be an adversary against $\{J_{IV_0}^{E,\pi_1}, J_{IV_0}^{E,\pi_2}, J_{IV_1}^{E,\pi_1}, \ldots, J_{IV_a}^{E,\pi_1}, J_{IV_a}^{E,\pi_2}\}$ using A as a subroutine. $\hat{A}$ is given access to $2(a+1)$ oracles $(h_{0,1}, h_{0,2}, h_{1,1}, h_{1,2}, \ldots, h_{a,1}, h_{a,2})$, which are either $(J_{IV_0,K}^{E,\pi_1}, J_{IV_0,K}^{E,\pi_2}, J_{IV_1,K}^{E,\pi_1}, \ldots, J_{IV_a,K}^{E,\pi_1}, J_{IV_a,K}^{E,\pi_2})$ with $K \twoheadleftarrow \Sigma^w$ or $(\hat{\rho}_{0,1}, \hat{\rho}_{0,2}, \hat{\rho}_{1,1}, \ldots, \hat{\rho}_{a,1}, \hat{\rho}_{a,2}) \twoheadleftarrow \boldsymbol{F}((\Sigma^w)^+, \Sigma^n)^{2(a+1)}$.

$\hat{A}$ simply runs A. Let M be a query made by A to its i-th oracle for $0 \le i \le a$. If $|M| > 0$ and $|M| \equiv 0 \pmod w$, then $\hat{A}$ returns $h_{i,1}(\mathsf{pad}(M))$ to A. Otherwise, $\hat{A}$ returns $h_{i,2}(\mathsf{pad}(M))$ 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

$$\Pr[\hat{A}^{J_{IV_0,K}^{E,\pi_1}, J_{IV_0,K}^{E,\pi_2}, \ldots, J_{IV_a,K}^{E,\pi_2}} = 1] = \Pr[A^{L_{IV_0,K}^{E,\{\pi_1,\pi_2\}}, \ldots, L_{IV_a,K}^{E,\{\pi_1,\pi_2\}}} = 1] \ ,$$

$$\Pr[\hat{A}^{\hat{\rho}_{0,1}, \hat{\rho}_{0,2}, \ldots, \hat{\rho}_{a,2}} = 1] = \Pr[A^{\rho_0, \ldots, \rho_a} = 1] \ ,$$

where $(\rho_0, \ldots, \rho_a) \twoheadleftarrow \boldsymbol{F}(\Sigma^*, \Sigma^n)^{a+1}$. Thus, from Theorem 1, there exists an adversary B against F such that

$$\mathrm{Adv}^{\mathrm{prfs}}_{\left\{L_{IV_i}^{E,\{\pi_1,\pi_2\}} \,\middle|\, 0 \le i \le a\right\}}(A) \le \ell q \, \mathrm{Adv}_E^{\mathrm{prp}}(B) + \frac{\ell q(q-1)}{2^{n+1}} \ .$$

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

5.2 Discussion

Some generic constructions of vPRF using any string-input PRF such as S2V [28] and S2V-R [24] can also be applied to $L_{IV}^{E,\{\pi_1,\pi_2\}}$. S2V and S2V-R require finite field multiplications and bit rotations, respectively, as well as bitwise XOR operations. On the other hand, $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ only requires bitwise XOR operations if the permutations π_1 and π_2 are bitwise XOR operations with constants.

$vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ can be regarded as an instantiation of the protected counter sum construction with a variable-input-length PRF. It is not a straightforward application, however, in that $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ does not require any encoding of an input to add counter values. The domain separation and the ordering of vector components are achieved by the initialization vectors in $\mathcal{V}$.

6. Conclusion

This paper has first presented a PRF mode based on Lesamnta-LW and MDP which may produce multiple independent PRFs with a single key and multiple permutations and initialization vectors. Then, it has used this mode to construct a PRF with minimum padding and a vector-input PRF. It is expected that the proposed PRF mode will find some other applications. Future work is to provide security analysis for the proposed schemes in multi-user settings.

Acknowledgments

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

References

[1] Recommendation ITU-T X.1373, "Secure software update capability for intelligent transportation system communication devices," 2017.
[2] E. Andreeva, J. Daemen, B. Mennink, and G.V. Assche, "Security of keyed sponge constructions using a modular proof approach," FSE 2015, Proceedings, G. Leander, ed., Lecture Notes in Computer Science, vol.9054, pp.364–384, Springer, 2015.
[3] M. Bellare, "New proofs for NMAC and HMAC: Security without collision-resistance," CRYPTO 2006, Proceedings, C. Dwork, ed., Lecture Notes in Computer Science, vol.4117, pp.602–619, Springer, 2006.
[4] M. Bellare, D.J. Bernstein, and S. Tessaro, "Hash-function based PRFs: AMAC and its multi-user security," EUROCRYPT 2016, Proceedings, Part I, M. Fischlin and J. Coron, eds., Lecture Notes in Computer Science, vol.9665, pp.566–595, Springer, 2016.
[5] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," CRYPTO '96, Proceedings, N. Koblitz, ed., Lecture Notes in Computer Science, vol.1109, pp.1–15, Springer, 1996.
[6] M. Bellare, R. Canetti, and H. Krawczyk, "Pseudorandom functions revisited: The cascade construction and its concrete security," Proc. 37th IEEE Symposium on Foundations of Computer Science, pp.514–523, 1996.
[7] M. Bellare, R. Guérin, and P. Rogaway, "XOR MACs: New methods for message authentication using finite pseudorandom functions," CRYPTO'95, Proceedings, D. Coppersmith, ed., Lecture Notes in Computer Science, vol.963, pp.15–28, Springer, 1995.
[8] M. Bellare and T. Ristenpart, "Multi-property-preserving hash domain extension and the EMD transform," ASIACRYPT 2006, Proceedings, X. Lai and K. Chen, eds., Lecture Notes in Computer Science, vol.4284, pp.299–314, Springer, 2006.
[9] M. Bellare and T. Ristenpart, "Hash functions in the dedicated-key setting: Design choices and MPP transforms," ICALP 2007, Proceedings, L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, eds., Lecture Notes in Computer Science, vol.4596, pp.399–410, Springer, 2007.
[10] D.J. Bernstein, "How to stretch random functions: The security of protected counter sums," J. Cryptology, vol.12, no.3, pp.185–192, 1999.
[11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "On the security of the keyed sponge construction," Symmetric Key Encryption Workshop, 2011.
[12] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Permutation-based encryption, authentication and authenticated encryption," Directions in Authenticated Ciphers (DIAC) Workshop, 2012.
[13] J. Black and P. Rogaway, "CBC MACs for arbitrary-length messages: The three-key constructions," CRYPTO 2000, Proceedings, M. Bellare, ed., Lecture Notes in Computer Science, vol.1880, pp.197–215, Springer, 2000.
[14] J. Black and P. Rogaway, "A block-cipher mode of operation for parallelizable message authentication," EUROCRYPT 2002, Proceedings,

L.R. Knudsen, ed., Lecture Notes in Computer Science, vol.2332, pp.384–397, Springer, 2002.
[15] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "SPONGENT: A lightweight hash function," CHES 2011, Proceedings, B. Preneel and T. Takagi, eds., Lecture Notes in Computer Science, vol.6917, pp.312–325, Springer, 2011.
[16] FIPS PUB 180-4, "Secure hash standard (SHS)," Aug. 2015.
[17] P. Gazi, K. Pietrzak, and S. Tessaro, "The exact PRF security of truncation: Tight bounds for keyed sponges and truncated CBC," CRYPTO 2015, Proceedings, Part I, R. Gennaro and M. Robshaw, eds., Lecture Notes in Computer Science, vol.9215, pp.368–387, Springer, 2015.
[18] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," CRYPTO 2011, Proceedings, P. Rogaway, ed., Lecture Notes in Computer Science, vol.6841, pp.222–239, Springer, 2011.
[19] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, and H. Yoshida, "An AES based 256-bit hash function for lightweight applications: Lesamnta-LW," IEICE Trans. Fundamentals, vol.E95-A, no.1, pp.89–99, Jan. 2012.
[20] S. Hirose, J.H. Park, and A. Yun, "A simple variant of the Merkle-Damgård scheme with a permutation," J. Cryptology, vol.25, no.2, pp.271–309, 2012.
[21] S. Hirose and A. Yabumoto, "A tweak for a PRF mode of a compression function and its applications," SECITC 2016, Proceedings, I. Bica and R. Reyhanitabar, eds., Lecture Notes in Computer Science, vol.10006, pp.103–114, 2016.
[22] ISO/IEC 29192-5, "Information technology – security techniques – lightweight cryptography – part 5: Hash-functions," 2016.
[23] T. Iwata and K. Kurosawa, "OMAC: One-key CBC MAC," FSE 2003, Proceedings, T. Johansson, ed., Lecture Notes in Computer Science, vol.2887, pp.129–153, Springer, 2003.
[24] K. Minematsu, "A short universal hash function from bit rotation, and applications to blockcipher modes," ProvSec 2013, Proceedings, W. Susilo and R. Reyhanitabar, eds., Lecture Notes in Computer Science, vol.8209, pp.221–238, Springer, 2013.
[25] N. Mouha, B. Mennink, A.V. Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, "Chaskey: An efficient MAC algorithm for 32-bit microcontrollers," SAC 2014, Proceedings, A. Joux and A.M. Youssef, eds., Lecture Notes in Computer Science, vol.8781, pp.306–323, Springer, 2014.
[26] M. Nandi, "Fast and secure CBC-type MAC algorithms," FSE 2009, Proceedings, O. Dunkelman, ed., Lecture Notes in Computer Science, vol.5665, pp.375–393, Springer, 2009.
[27] NIST Special Publication 800-38B, "Recommendation for block cipher modes of operation: The CMAC mode for authentication," 2005.
[28] P. Rogaway and T. Shrimpton, "A provable-security treatment of the key-wrap problem," EUROCRYPT 2006, Proceedings, S. Vaudenay, ed., Lecture Notes in Computer Science, vol.4004, pp.373–390, Springer, 2006.
[29] K. Yasuda, "Boosting Merkle-Damgård hashing for message authentication," ASIACRYPT 2007, Proceedings, K. Kurosawa, ed., Lecture Notes in Computer Science, vol.4833, pp.216–231, Springer, 2007.
[30] K. Yasuda, ""Sandwich" is indeed secure: How to authenticate a message with just one hashing," ACISP 2007, Proceedings, J. Pieprzyk, H. Ghodosi, and E. Dawson, eds., Lecture Notes in Computer Science, vol.4586, pp.355–369, Springer, 2007.
[31] K. Yasuda, "A one-pass mode of operation for deterministic message authentication — Security beyond the birthday barrier," FSE 2008, Proceedings, K. Nyberg, ed., Lecture Notes in Computer Science, vol.5086, pp.316–333, Springer, 2008.
[32] K. Yasuda, "A double-piped mode of operation for MACs, PRFs and PROs: Security beyond the birthday barrier," EUROCRYPT 2009, Proceedings, A. Joux, ed., Lecture Notes in Computer Science, vol.5479, pp.242–259, Springer, 2009.
[33] K. Yasuda, "HMAC without the "second" key," ISC 2009, Proceedings, P. Samarati, M. Yung, F. Martinelli, and C.A. Ardagna, eds., Lecture Notes in Computer Science, vol.5735, pp.443–458, Springer, 2009.
[34] K. Yasuda, "On the full MAC security of a double-piped mode of operation," IEICE Trans. Fundamentals, vol.94-A, no.1, pp.84–91, Jan. 2011.
[35] K. Yasuda, "A parallelizable PRF-based MAC algorithm: Well beyond the birthday bound," IEICE Transactions on Fundamentals, vol.96-A, no.1, pp.237–241, Jan. 2013.

Shoichi Hirose received the B.E., M.E. and D.E. degrees in information science from Kyoto University, Kyoto, Japan, in 1988, 1990 and 1995, respectively. From 1990 to 1998, he was a research associate at Faculty of Engineering, Kyoto University. From 1998 to 2005, he was a lecturer at Graduate School of Informatics, Kyoto University. From 2005 to 2009, he was an associate professor at Faculty of Engineering, University of Fukui. From 2009, he is a professor at Graduate School of Engineering, University of Fukui. His current interests include cryptography and information security. He received Young Engineer Award from IEICE in 1997, and KDDI Foundation Research Award in 2008.

Hidenori Kuwakado received the B.E., M.E. and D.E. degrees from Kobe University in 1990, 1992, and 1999 respectively. He worked for Nippon Telegraph and Telephone Corporation from 1992 to 1996. From 1996 to 2002, he was a research associate in the Faculty of Engineering, Kobe University. From 2002 to 2007, he was an associate professor in the Faculty of Engineering, Kobe University. From 2007 to 2013, he was an associate professor in Graduate School of Engineering, Kobe University. Since 2013, he has been a professor in Faculty of Informatics, Kansai University. His research interests are in cryptography and information security.

Hirotaka Yoshida received the B.S. degree from Meiji University, Japan, in 1999, the M.S. degree from Tokyo Institute of Technology (Japan) in 2001, and the Ph.D. degree in electrical engineering from KU Leuven, Belgium, in 2013. From 2001 to 2016, he was with the Research & Development Group, Hitachi, Ltd. He is currently a senior research scientist at the National Institute of Advanced Industrial Science and Technology (AIST). He is a member of IACR, IPSJ, and JSAE.