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

Shoichi Hirose[1] Hidenori Kuwakado[2] Hirotaka Yoshida[3]

[1]University of Fukui, Japan

[2]Kansai University, Japan

[3]National Institute of Advanced Industrial Science and Technology, Japan

NIST LWC 2016 (2016/10/17-18, Gaithersburg)

Introduction

Pseudorandom function (PRF)

- Indistinguishable from a uniform random function

Applications

- Message authentication
- Pseudorandom number generation

Widely used constructions

- Block-cipher-based: CMAC
- Hash-function-based: HMAC

Motivation

HMAC may not be suitable for lightweight cryptography

- Inefficient for short messages due to
  - length-extension property
  - injective padding with strengthened MD

  of an underlying hash function

More efficient PRF can be constructed using a compression function.

Compression-function-based modes for

- hashing
- PRF
- AEAD (OMD among CAESAR submissions)

Cf.) Sponge construction provides permutation-based modes for

- hashing
- PRF
- AEAD

Target IoT System: Automotives

V2X (Vehicle-to-X) system

- Over-the-air programming (OTA) gets a lot of attention.
- ITU-T SG17 is developing a protocol for remote software update.
- Hash, MAC and PRF play core roles in this protocol.

In-vehicle system

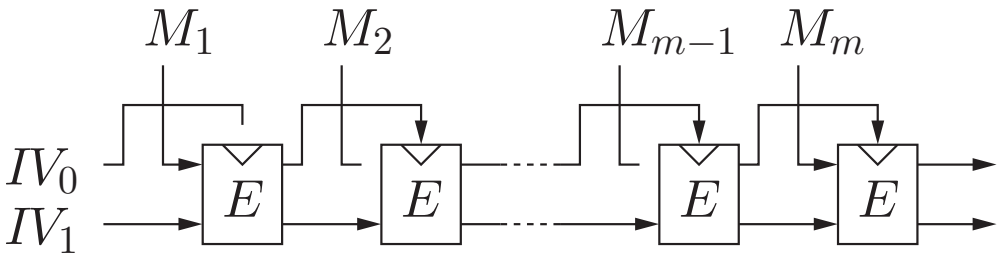
- Short-message performance important:
  - Packets are as short as 8 bytes (CAN) to 64 bytes (CAN-FD).
  - Realtime req. is severe: 1–100ms periodic tasks are processed.
- 50–100 ECUs are employed in a car:
  - Limited cost can be paid for each ECU.
  - Cost comes from circuit size in HW and RAM/ROM size in SW.

Lesamnta-LW

Lightweight hash functions in ISO/IEC 29192-5

- Optimized for hardware: PHOTON and SPONGENT
- Optimized for software: Lesamnta-LW
  - Software implementation using 54-byte of RAM is possible.

Lesamnta-LW [HIKOPY12]



E is a dedicated block cipher with

- block length $= 256$ bits
- key length $= 128$ bits

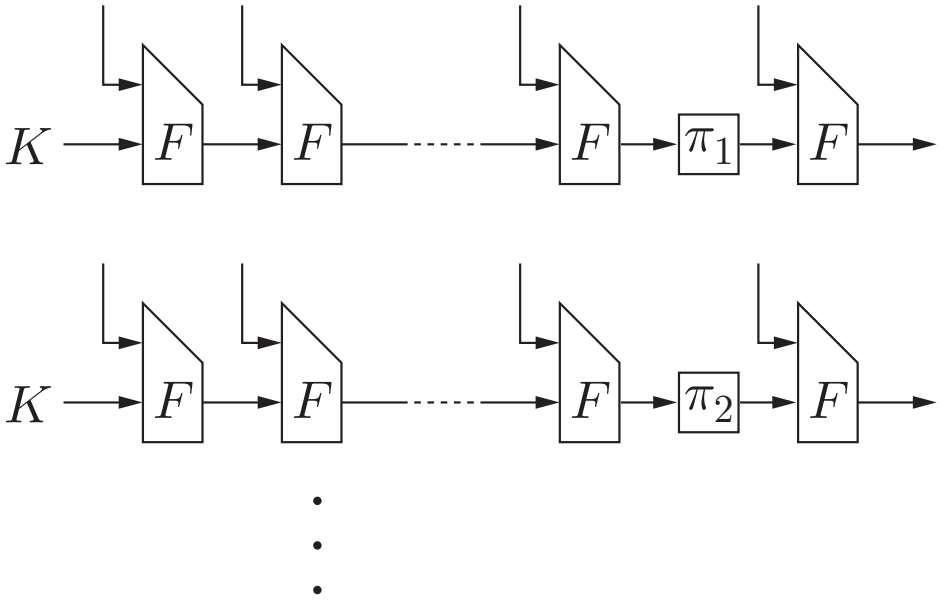
Related Work [Hirose, Yabumoto 2016]

MDP may produce multiple independent PRFs with

- a single key
- multiple permutations

Applications

- PRF with minimum padding
- Vector-input PRF only with CF and XOR



Summary of Our Results

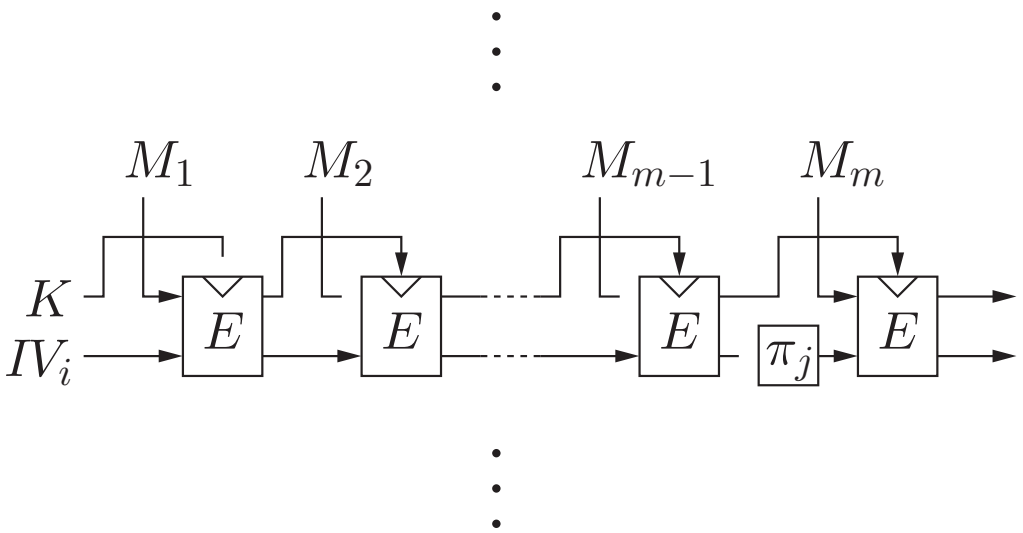
Apply [HY16] to Lesamnta-LW

Lesamnta-LW with MDP may produce multiple independent PRFs with

- a single key
- multiple IVs
- multiple permutations

Applications

- PRF with minimum padding
- Vector-input PRF



Related Work

Hash-function-based PRF

- HMAC [Bellare, Canetti, Krawczyk 1996]
- HMAC without the second key [Yasuda 2009]
- AMAC [Bellare, Bernstein, Tessaro 2016]

Compression-function-based PRF

- Plain Merkle-Damgård (MD) with prefix-free encoding [BCK1996]
- EMD (Enveloped MD) [Bellare, Ristenpart 2006]
- MDP (MD with Permutation) [Hirose, Park, Yun 2007]
- Boosting MD [Yasuda 2007]
- Sandwich MD [Yasuda 2007]

Vector-input PRF

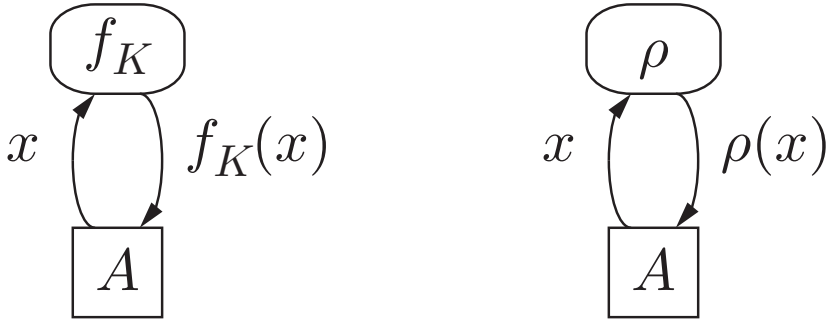
- S2V [Rogaway, Shrimpton 2006]
- S2V-R [Minematsu 2013]

Definition of PRF and PRP

A keyed function $f : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ is PRF

if f is indistinguishable from uniform random function $\rho : \mathcal{D} \to \mathcal{R}$

- Adversary makes queries to f_K or ρ
- Secret key $K \in \mathcal{K}$ is chosen uniformly at random



real world ideal world

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

If f_K and ρ are permutations,

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

Independent PRFs Based on Lesamnta-LW & MDP

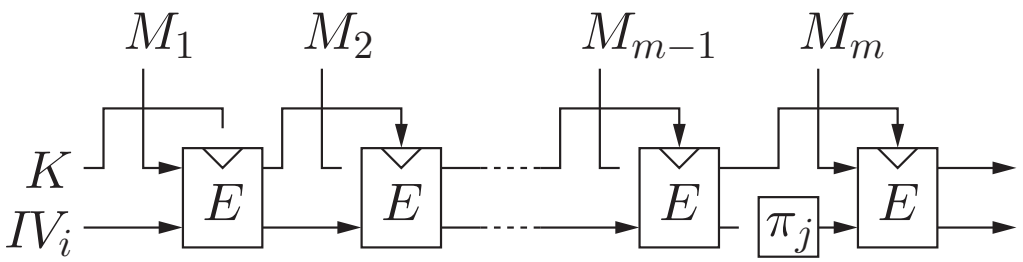
Theorem

Lesamnta-LW with MDP produces multiple independent PRFs with

- *a single key* K
- *multiple IVs* $\mathcal{V} = \{IV_1, IV_2, \ldots, IV_a\}$
- *multiple permutations* $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\}$

$\Longleftarrow$ E *is PRP and*

1. $\pi(x) \neq \pi'(x)$ *for every* $\pi, \pi' \in \Pi \cup \{id\}$ *and every* $x \in \Sigma^{n-w}$
2. $\pi(IV) \neq \pi'(IV')$ *for every* $(\pi, IV), (\pi', IV') \in (\Pi \cup \{id\}) \times \mathcal{V}$



Security

Theorem

For $\mathcal{V}$ and Π, suppose that

- $\pi(x) \neq \pi'(x)$ *for every* $\pi, \pi' \in \Pi \cup \{id\}$ *and every* $x \in \Sigma^{n-w}$
- $\pi(IV) \neq \pi'(IV')$ *for every* $(\pi, IV), (\pi', IV') \in (\Pi \cup \{id\}) \times \mathcal{V}$

Let A be any adversary against $J_{\mathcal{V}}^{E,\Pi}$ s.t.

- *run time* $\leq t$
- *number of queries* $\leq q$
- *length of each query* $\leq \ell$ *message blocks*

Then, there exists an adversary B against E s.t.

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

- *run time* $\leq t + O(\ell q T_E)$
- *number of queries* $\leq q$

Example

$\mathcal{V}$ and Π have to satisfy

1. $\pi(x) \neq \pi'(x)$ for every $\pi, \pi' \in \Pi \cup \{id\}$ and every $x \in \Sigma^{n-w}$
2. $\pi(IV) \neq \pi'(IV')$ for every $(\pi, IV), (\pi', IV') \in (\Pi \cup \{id\}) \times \mathcal{V}$

Example

Let $\mathcal{V} = \{IV_1, IV_2, \ldots, IV_a\}$ and $\Pi = \{\pi_1, \pi_2, \ldots, \pi_d\}$

$$IV_i = \boxed{v_i}\boxed{00\cdots0}$$

$$\pi_j(x) = \boxed{\quad x \quad} \oplus \boxed{00\cdots0}\boxed{c_j}$$

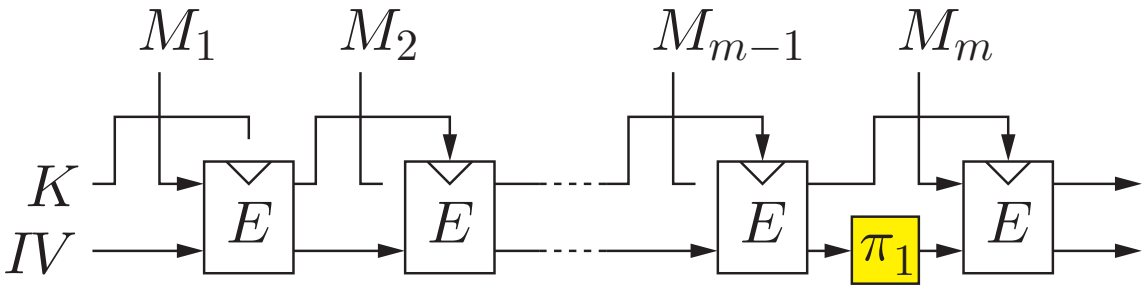
$$\pi_j(IV_i) = \boxed{v_i}\boxed{c_j}$$

- $v_1, v_2, \ldots, v_a$ are nonzero and distinct
- $c_1, c_2, \ldots, c_d$ are nonzero and distinct

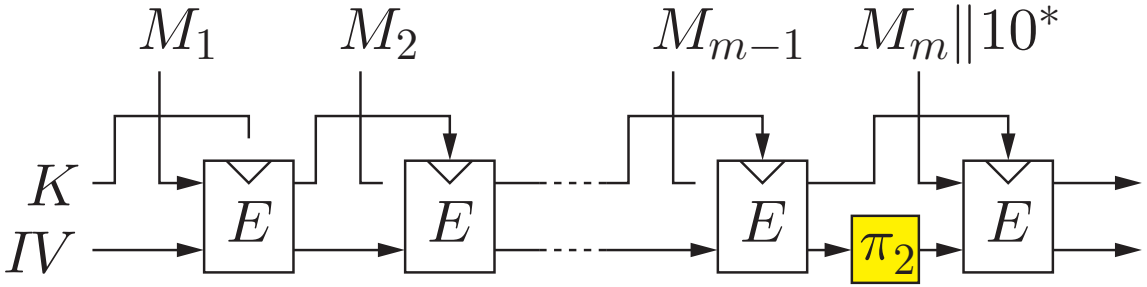
PRF with Minimum Padding

For message M such that

- $|M| > 0$ and $|M| \equiv 0 \pmod{w}$,



- $|M| = 0$ or $|M| \not\equiv 0 \pmod{w}$,



Distinct permutations are used for domain separation.

No message blocks only with the padding sequence (10^*)

Security

Theorem

$$L_{IV}^{E,\{\pi_1,\pi_2\}} \textit{ is PRF} \Longleftarrow E \textit{ is PRP}$$

Let A be any adversary against $L_{IV}^{E,\{\pi_1,\pi_2\}}$ s.t.

- run time $\leq t$
- number of queries $\leq q$
- length of each query $\leq \ell$ message blocks

Then, there exists an adversary B against E s.t.

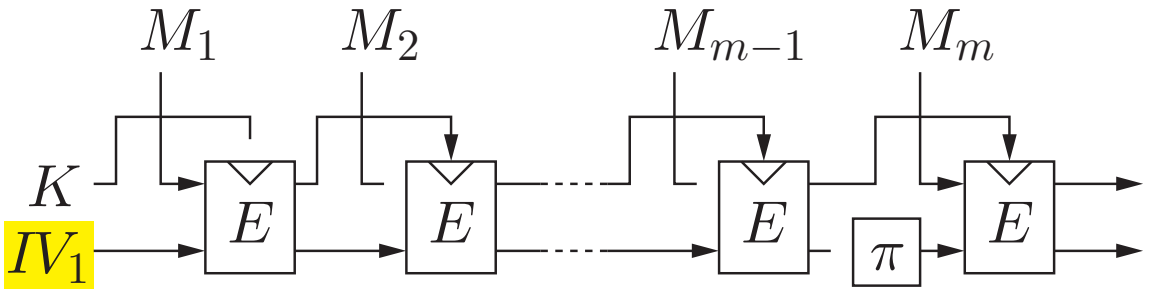
$$\mathrm{Adv}^{\mathrm{prf}}_{L_{IV}^{E,\{\pi_1,\pi_2\}}}(A) \leq \ell q \cdot \mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{\ell q(q-1)}{2^{n+1}}$$

- run time $\leq t + O(\ell q T_E)$
- number of queries $\leq q$

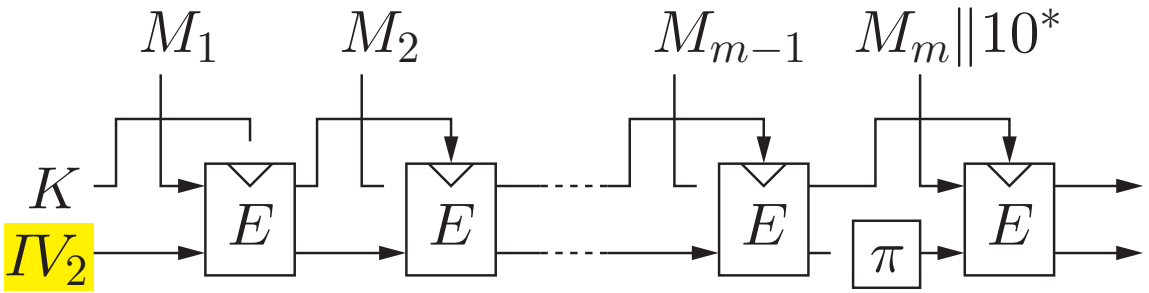
Another Secure but Inefficient Construction

For message M such that

- $|M| > 0$ and $|M| \equiv 0 \pmod{w}$,



- $|M| = 0$ or $|M| \not\equiv 0 \pmod{w}$,

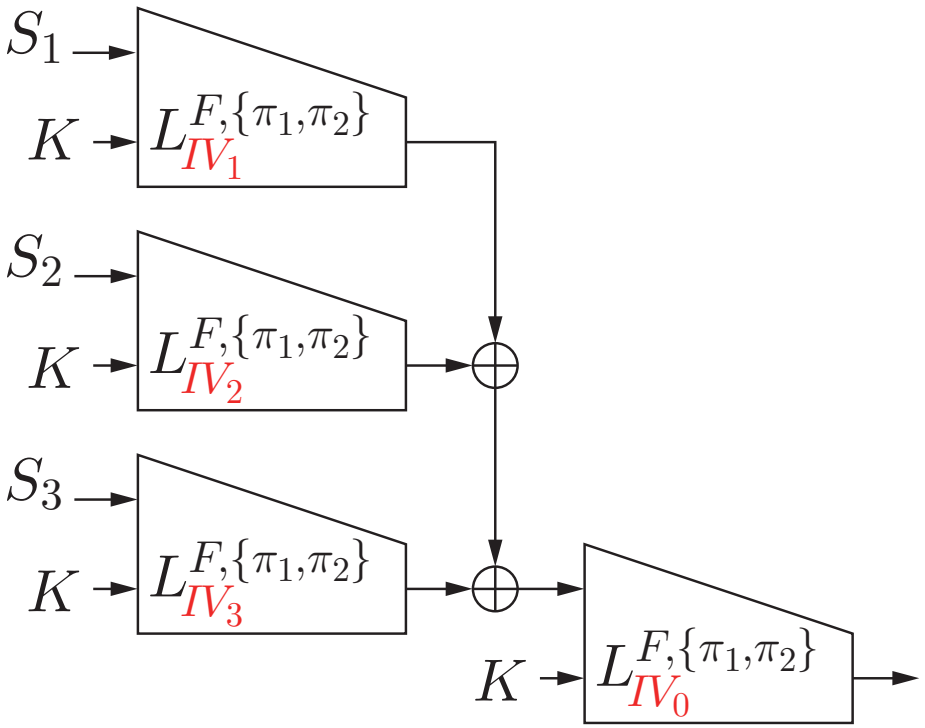


Distinct IVs are used for domain separation instead of permutations.

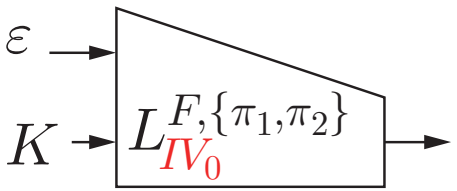
☹ Computation cannot be started until the end of the message.

Vector Input PRF

For vector $(S_1, S_2, \ldots)$ s.t. $S_i \in \{0,1\}^*$



For vector $()$



- An instantiation of protected counter sum construction [Ber99]
  - Uses IV as a counter
  - Does not require any encoding of a message with a counter
- If π_i's are XOR with consts, computed only with F and XOR.

Security

Theorem

$$vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}} \text{ is PRF} \Longleftarrow E \text{ is PRP}$$

Let A be any adversary against $vL_{\mathcal{V}}^{E,\{\pi_1,\pi_2\}}$ s.t.

- run time $\leq t$
- number of queries $\leq q$
- length of each vector component $\leq \ell$ message blocks
- number of vector components in all queries $\leq \sigma$

Then, there exists an adversary B against E s.t.

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

- run time $\leq t + O(\ell(\sigma+q)T_E)$
- number of queries $\leq \sigma + q$

Conclusion

Apply [HY16] to Lesamnta-LW

Lesamnta-LW with MDP may produce multiple independent PRFs with

- a single key
- multiple IVs
- multiple permutations

Applications

- PRF with minimum padding
- Vector-input PRF