IEICE TRANSACTIONS

on Information and Systems

VOL. E104-D NO. 11
NOVEMBER 2021

A PUBLICATION OF THE INFORMATION AND SYSTEMS SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER Special Section on Next-generation Security Applications and Practice

Provable-Security Analysis of Authenticated Encryption Based on Lesamnta-LW in the Ideal Cipher Model

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

SUMMARY Hirose, Kuwakado and Yoshida proposed a nonce-based authenticated encryption scheme Lae0 based on Lesamnta-LW in 2019. Lesamnta-LW is a block-cipher-based iterated hash function included in the ISO/IEC 29192-5 lightweight hash-function standard. They also showed that Lae0 satisfies both privacy and authenticity if the underlying block cipher is a pseudorandom permutation. Unfortunately, their result implies only about 64-bit security for instantiation with the dedicated block cipher of Lesamnta-LW. In this paper, we analyze the security of Lae0 in the ideal cipher model. Our result implies about 120-bit security for instantiation with the block cipher of Lesamnta-LW.

key words: *authenticated encryption, hash function, Lesamnta-LW, ideal cipher model*

1. Introduction

1.1 Background

Authenticated encryption (AE) is symmetric cryptography providing both privacy and authenticity. Informally, privacy is confidentiality of plaintexts and authenticity is integrity of ciphertexts. AE schemes often take additional input called associated data which only require authenticity. Such AE schemes are referred to as authenticated encryption with associated data (AEAD).

There are some kinds of approaches for AEAD construction. Among them, one of the most common approaches is to construct it as a mode of operation of a block cipher such as AES [1]. The other is to construct it based on the sponge construction [2]. The sponge construction [3] was invented originally for cryptographic hash functions as well as for MAC functions and stream ciphers. The sponge-based hash function Keccak [4] was selected for the SHA-3 standard [5]. The sponge construction is also popular for lightweight hashing.

The ISO/IEC 29192-5 lightweight hash function standard [6] was released in 2016, which specifies three lightweight cryptographic hash functions: PHOTON [7], SPONGENT [8], and Lesamnta-LW [9]. PHOTON and SPONGENT follow the sponge construction, and the sponge-based AEAD mode can be applied to them. On the other hand, Lesamnta-LW is a Merkle-Damgård [10], [11] hash function using a dedicated block cipher whose key size is half the block size as a compression function. In addition, Lesamnta-LW is optimized for software implementation, while both PHOTON and SPONGENT are optimized for hardware implementation. In fact, a software result [9] shows that Lesmanta-LW provides 120-bit collision resistance with 54 bytes of RAM, achieving 20% faster short-message performance over SHA-256, while hardware results show that SPONGENT provides 80-bit collision resistance with 1329 GE and PHOTON provides the same security level with 1396 GE.

In 2019, Hirose, Kuwakado and Yoshida [12] proposed a nonce-based AEAD scheme based on Lesamnta-LW, which they called Lae0. It can be implemented with the block cipher of Lesamnta-LW. Thus, it is an efficient option for lightweight AEAD on low-cost 8-bit microcontrollers where RAM requirement is critical for cryptographic functionality.

1.2 Our Contribution

Hirose, Kuwakado and Yoshida [12] also showed that Lae0 is secure in the standard model: Lae0 satisfies both privacy and authenticity if the block cipher of the Lesamnta-LW hashing mode is a pseudorandom permutation (PRP). Unfortunately, their result is not entirely satisfactory in that it implies only about 64-bit security for instantiation of Lae0 with the block cipher of Lesamnta-LW. Their upper bound on the advantage of any adversary **A** against Lae0 has the term $\ell q\,\mathrm{adv}_E^{\mathrm{prp}}$, where $\mathrm{adv}_E^{\mathrm{prp}}$ is the advantage of an adversary constructed from **A** against the underlying block cipher E, ℓ is the maximum length of the queries made by **A**, and q is the number of the queries made by **A**. Due to the simple key-guessing attack on E, $\mathrm{adv}_E^{\mathrm{prp}} = \Omega(t/2^w)$, where t is the run time of **A** and w is the key length of E. Thus, the upper bound is $\Omega(1)$ if both ℓq and t are $\Omega(2^{w/2})$. For the block cipher of Lesamnta-LW, $w = 128$.

In this paper, we analyze the security of Lae0 in the ideal cipher model. In terms of both privacy and authenticity, our result implies about 120-bit security for instantiation of Lae0 with the block cipher of Lesamnta-LW. We discuss the authenticity of Lae0 under two typical misuses: nonce repetition (NR) and releasing unverified plaintexts (RUP).

Manuscript received February 9, 2020.
Manuscript revised June 4, 2021.
Manuscript publicized July 8, 2021.

[†]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, Tokyo, 135–0064 Japan.
a) E-mail: hrs_shch@u-fukui.ac.jp
b) E-mail: kuwakado@kansai-u.ac.jp
c) E-mail: hirotaka.yoshida@aist.go.jp

DOI: 10.1587/transinf.2021NGP0008

Though our analysis assumes an ideal cipher, our result is still significant in that it implies security of Lae0 against generic attacks regarding the underlying block cipher just as a black box.

1.3 Related Work

Authenticated encryption received the first formal treatments from Katz and Yung [13] and Bellare and Namprempre [14], which are followed by Jutla [15].

There are many block-cipher modes of operation for AEAD. OCB [16] is one of the earliest but most efficient modes, and it is inspired by IAPM [15]. CCM [17] and GCM [18] are specified by NIST and ISO/IEC 19772 [19].

As far as we know, there is only one proposal for AEAD based on cryptographic hashing except for the sponge-based proposals. It is OMD (Offset Merkle-Damgård) by Cogliani et al. [20], which is a mode of operation of a compression function for the Merkle-Damgård hashing such as SHA-2 [21].

Nonce-based symmetric encryption was introduced with its formalization by Rogaway [22]. The generic composition of nonce-based AEAD was discussed by Namprempre et al. [23].

For misuse resistance of authenticated encryption, security under NR was formalized by Rogaway and Shrimpton [24]. Security under RUP was formalized by Andreeva et al. [25]. Robust authenticated encryption was introduced and formalized by Hoang et al. [26], which is secure under NR and RUP.

Improved and/or new security analyses of the Lesamnta-LW block cipher have recently been conducted by Hirose, Sasaki and Yoshida [27] and by Shiba et al. [28].

1.4 Organization

Notations and definitions used in the remaining parts are given in Sect. 2. Syntax and security are formalized for AEAD in Sect. 3. The nonce-based AEAD scheme Lae0 is described in Sect. 4. Lae0 is shown to satisfy both privacy and authenticity in Sect. 5. A brief concluding remark is given in Sect. 6.

2. Preliminaries

2.1 Notations

Let $\Sigma = \{0, 1\}$. For any integer $l \geq 0$, let Σ^l be identified with the set of all Σ-sequences of length l. $\Sigma^0 = \{\varepsilon\}$, where ε is the empty sequence. $\Sigma^1 = \Sigma$. Let $(\Sigma^l)^* = \bigcup_{i\geq 0}(\Sigma^l)^i$ and $(\Sigma^l)^+ = \bigcup_{i\geq 1}(\Sigma^l)^i$.

For $x \in \Sigma^*$, the length of x is denoted by $|x|$. For $x_1, x_2 \in \Sigma^*$, $x_1\|x_2$ represents their concatenation. For $x \in \Sigma^*$ and an integer $0 \leq l \leq |x|$, $\mathsf{msb}_l(x)$ represents the most significant l bits of x, and $\mathsf{lsb}_l(x)$ represents the least significant l bits of x.

For $x, y \in \Sigma^*$ such that $|x| \geq |y|$, let $x \oplus y$ and $y \oplus x$ represent bitwise XOR of x and $y\|0^{|x|-|y|}$.

Selecting an element s from a set $\mathcal{S}$ uniformly at random is denoted by $s \twoheadleftarrow \mathcal{S}$.

The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted by $\mathcal{F}(\mathcal{X}, \mathcal{Y})$. The set of all permutations on $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$. ι represents an identity permutation. The set of all block ciphers with a key size κ and a block size n is denoted by $\mathcal{B}(\kappa, n)$. A block cipher in $\mathcal{B}(\kappa, n)$ is called a (κ, n) block cipher. For a keyed function $f : \mathcal{K}\times\mathcal{X} \to \mathcal{Y}$, $f(K, \cdot)$ is often denoted by $f_K(\cdot)$.

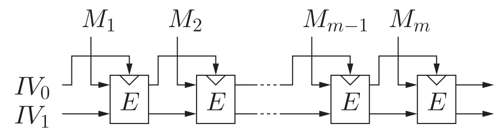

Fig. 1 The hashing mode of Lesamnta-LW. The input of the block cipher E from the top is its key input.

2.2 Hashing Mode of Lesamnta-LW

The hashing mode of Lesamnta-LW [9] is the plain Merkle-Damgård iteration of a block cipher E in $\mathcal{B}(n/2, n)$, where n is a positive even integer. E works as a compression function with domain $\Sigma^{3n/2}$ and range Σ^n. It is depicted in Fig. 1. $IV_0\|IV_1 \in \Sigma^n$ 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 $i = 1, 2, \ldots, m$.

The dedicated block cipher of Lesamnta-LW is in $\mathcal{B}(128, 256)$.

3. Authenticated Encryption with Associated Data

3.1 Syntax

A scheme of nonce-based authenticated encryption with associated data (AEAD) consists of a pair of functions for encryption and decryption. The encryption function is $\mathsf{Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ and the decryption function is $\mathsf{Dec} : \mathcal{K}\times\mathcal{N}\times\mathcal{A}\times\mathcal{C}\times\mathcal{T} \to \mathcal{M}\cup\{\perp\}$, where $\mathcal{K}$ is a key space, $\mathcal{N}$ is a nonce space, $\mathcal{A}$ is an associated-data space, $\mathcal{M}$ is a message space, $\mathcal{C}$ is a ciphertext space, and $\mathcal{T}$ is a tag space. $\mathcal{M} \subset \Sigma^*$, $\perp \notin \mathcal{M}$ and $\mathcal{A} \subset \Sigma^*$. If $M \in \mathcal{M}$, then $\Sigma^{|M|} \subset \mathcal{M}$. For any $K \in \mathcal{K}$, if $(C, T) \leftarrow \mathsf{Enc}_K(N, A, M)$ for some $(N, A, M) \in \mathcal{N}\times\mathcal{A}\times\mathcal{M}$, then $M \leftarrow \mathsf{Dec}_K(N, A, C, T)$. Otherwise, $\perp \leftarrow \mathsf{Dec}_K(N, A, C, T)$, which means that (N, A, C, T) is invalid with respect to $K \in \mathcal{K}$.

3.2 Security

The security requirements for AEAD are privacy and authenticity. Informally, privacy is confidentiality of encrypted messages, and authenticity is integrity of ciphertexts and associated data.

(1) Privacy

Let \$ be a random function taking $(N, A, M) \in \mathcal{N} \times \mathcal{A} \times$

$\mathcal{M}$ as input and returning a binary sequence of length $|\mathsf{Enc}_K(N, A, M)|$, which is chosen uniformly at random. The privacy of an AEAD scheme $(\mathsf{Enc}, \mathsf{Dec})$ is defined by the indistinguishability between Enc_K and \$:

$$\mathrm{Adv}^{\mathrm{priv}}_{(\mathsf{Enc},\mathsf{Dec})}(\mathbf{A}) = \left|\Pr[\mathbf{A}^{\mathsf{Enc}_K} = 1] - \Pr[\mathbf{A}^{\$} = 1]\right|,$$

where $K \twoheadleftarrow \mathcal{K}$. $\mathbf{A}$ is assumed to be nonce-respecting. Namely, $\mathbf{A}$ is not allowed to make multiple encryption queries with the same nonce.

(2) Authenticity

The authenticity of an AEAD scheme $(\mathsf{Enc}, \mathsf{Dec})$ is defined by the unforgeability:

$$\mathrm{Adv}^{\mathrm{auth}}_{(\mathsf{Enc},\mathsf{Dec})}(\mathbf{A}) = \Pr[\mathbf{A}^{\mathsf{Enc}_K,\mathsf{Dec}_K} \text{ succeeds in forgery}],$$

where $K \twoheadleftarrow \mathcal{K}$. $\mathbf{A}$ succeeds in forgery if it succeeds in making a decryption query such that its corresponding reply from Dec_K is not $\perp$. $\mathbf{A}$ is not allowed to make a trivial decryption query. Namely, if $\mathbf{A}$ gets (C, T) as an answer to some encryption query (N, A, M), then it is not allowed to ask (N, A, C, T) as a decryption query.

4. AEAD Based on Lesamnta-LW: Lae0

Let E be a block cipher in $\mathcal{B}(n/2, n)$, where n is an even integer. Hereafter, let $n/2 = w$ just for simplicity.

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

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

where t is the minimum non-negative integer satisfying $|X| + 1 + t \equiv 0 \pmod{w}$. For any $X \in \Sigma^*$, $|\mathsf{pad}(X)|$ is the minimum positive multiple of w, which is greater than or equal to $|X|$. Notice that pad is not injective. For example, $\mathsf{pad}(\varepsilon) = \mathsf{pad}(10^{w-1}) = 10^{w-1}$.

Let $\mathsf{pad}(X) = (X_1, X_2, \ldots, X_x)$, where $|X_i| = w$ for every i such that $1 \le i \le x$. $x = 1$ if $|X| = 0$, and $x = \lceil |X|/w \rceil$ if $|X| > 0$. X_i is called the i-th block of $\mathsf{pad}(X)$.

For $E \in \mathcal{B}(w, n)$ and $\pi_0, \pi_1 \in \mathcal{P}(\Sigma^w)$, the nonce-based AEAD scheme $\mathsf{Lae0} = (\mathsf{E0}, \mathsf{D0})$ is presented by Algorithm 1. The encryption function $\mathsf{E0}$ is also depicted in Fig. 2. For $\mathsf{Lae0}$, the key space is Σ^w, the nonce space is Σ^n, and the tag space is Σ^τ, where $0 < \tau \le n$. The associated-data space, the message space and the ciphertext space are Σ^*. If $(C, T) \leftarrow \mathsf{E0}_K(N, A, M)$, then $|C| = |M|$.

Algorithm 1 Encryption E0 and decryption D0 of Lae0

function $\mathsf{E0}_K(N, A, M)$
  $(A_1, A_2, \ldots, A_a) \leftarrow \mathsf{pad}(A)$;
  $(M_1, M_2, \ldots, M_m) \leftarrow \mathsf{pad}(M)$;
  $Y_0 \leftarrow E_K(N)$;
  for $i = 1$ **to** $a - 1$ **do** ▹ $Y_{i-1,0} = \mathsf{msb}_w(Y_{i-1}), Y_{i-1,1} = \mathsf{lsb}_w(Y_{i-1})$
    $Y_i \leftarrow E_{Y_{i-1,0}}(A_i\|Y_{i-1,1})$;
  if $|A| > 0 \wedge |A| \equiv 0 \pmod{w}$ **then**
    $Y_a \leftarrow E_{Y_{a-1,0}}(A_a\|\pi_0(Y_{a-1,1}))$;
  else
    $Y_a \leftarrow E_{Y_{a-1,0}}(A_a\|\pi_1(Y_{a-1,1}))$;
  for $i = 1$ **to** $m - 1$ **do**
    $C_i \leftarrow M_i \oplus Y_{a+i-1,1}$;
    $Y_{a+i} \leftarrow E_{Y_{a+i-1,0}}(M_i\|Y_{a+i-1,1})$;
  $C_m \leftarrow M_m \oplus Y_{a+m-1,1}$;
  if $|M| > 0 \wedge |M| \equiv 0 \pmod{w}$ **then**
    $T \leftarrow E_{Y_{a+m-1,0}}(M_m\|\pi_0(Y_{a+m-1,1}))$;
  else
    $T \leftarrow E_{Y_{a+m-1,0}}(M_m\|\pi_1(Y_{a+m-1,1}))$;
  $C \leftarrow C_1\|\cdots\|C_{m-1}\|\mathsf{msb}_{|M|-(m-1)w}(C_m)$;
  return C, T;

function $\mathsf{D0}_K(N, A, C, T)$
  $(A_1, A_2, \ldots, A_a) \leftarrow \mathsf{pad}(A)$;
  $(C_1, C_2, \ldots, C_m) \leftarrow \mathsf{pad}(C)$;
  $Y_0 \leftarrow E_K(N)$;
  for $i = 1$ **to** $a - 1$ **do**
    $Y_i \leftarrow E_{Y_{i-1,0}}(A_i\|Y_{i-1,1})$;
  if $|A| > 0 \wedge |A| \equiv 0 \pmod{w}$ **then**
    $Y_a \leftarrow E_{Y_{a-1,0}}(A_a\|\pi_0(Y_{a-1,1}))$;
  else
    $Y_a \leftarrow E_{Y_{a-1,0}}(A_a\|\pi_1(Y_{a-1,1}))$;
  for $i = 1$ **to** $m - 1$ **do**
    $M_i \leftarrow C_i \oplus Y_{a+i-1,1}$;
    $Y_{a+i} \leftarrow E_{Y_{a+i-1,0}}(M_i\|Y_{a+i-1,1})$;
  $M_m \leftarrow C_m \oplus \mathsf{msb}_{|C|-(m-1)w}(Y_{a+m-1,1})$;
  if $|C| > 0 \wedge |C| \equiv 0 \pmod{w}$ **then**
    $T' \leftarrow E_{Y_{a+m-1,0}}(M_m\|\pi_0(Y_{a+m-1,1}))$;
  else
    $T' \leftarrow E_{Y_{a+m-1,0}}(M_m\|\pi_1(Y_{a+m-1,1}))$;
  $M \leftarrow M_1\|\cdots\|M_{m-1}\|\mathsf{msb}_{|C|-(m-1)w}(M_m)$;
  if $T' = T$ **then**
    return M;
  else
    return $\perp$;

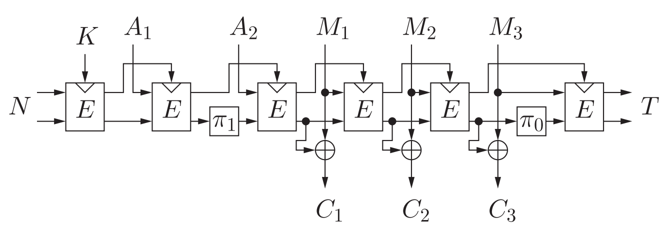

Fig. 2 The encryption function $\mathsf{E0}$ of the nonce-based AEAD scheme $\mathsf{Lae0}$. $(C, T) \leftarrow \mathsf{E0}_K(N, A, M)$, where $\mathsf{pad}(A) = (A_1, A_2)$, $\mathsf{pad}(M) = (M_1, M_2, M_3)$, and $C = C_1\|C_2\|C_3$. This figure assumes that $|A| \not\equiv 0 \pmod{w}$, $|M| \equiv 0 \pmod{w}$ and $\tau = n$.

5. Security of Lae0 in the Ideal Cipher Model

The security of $\mathsf{Lae0} = (\mathsf{E0}, \mathsf{D0})$ is analyzed in the ideal cipher model. Thus, adversaries are given oracle access to encryption E and decryption E^{-1} of the block cipher used in Lae0. Without loss of generality, it is assumed that adversaries do not make trivial queries to E and E^{-1}. Namely, once an adversary obtains a triplet (S, U, V) such that $E_S(U) = V$ by a query to E or E^{-1}, it makes no new queries on the triplet.

A combinatorial theorem used in the analysis is first presented:

Lemma 1 (Theorem 3.1 in [29]) Suppose that there are t balls and t bins and that each ball is placed in a bin chosen independently and uniformly at random. Then, with probability at least $1 - 1/t$, no bin has more than $\mathrm{e} \ln t / \ln \ln t$ balls in it.

For Lemma 1, let $t = 2^w$. Then,

$$\mathrm{e} \ln t / \ln \ln t = \mathrm{e}w/(\log_2 w - \log_2 \log_2 \mathrm{e}),$$

which is denoted by $\gamma(w)$ in the remaining part.

Example 1 $\gamma(128) \approx 53.77$.

5.1 Privacy

From the theorem given below, for privacy, Lae0 is secure against nonce-respecting adversaries causing at most $O(2^w/\gamma(w))$ evaluations of its underlying block cipher. For $w = 128$, $2^w/\gamma(w) \approx 2^{122.25}$.

The main idea of the proof of the following theorem is simple: The outputs of E0 look random to an adversary if the set of the triplets (S, U, V) such that $E_S(U) = V$ used by the process of E0 and the set of them obtained by the queries to E and E^{-1} made by the adversary are disjoint.

Theorem 1 Let $\mathbf{A}$ be any adversary against Lae0 for privacy. Suppose that $\mathbf{A}$ makes at most q_e and q_d queries to E and E^{-1}, respectively. Suppose that σ is the total number of the queries to E induced by the queries to E0 and D0 made by $\mathbf{A}$. Let $q = q_\mathrm{e} + q_\mathrm{d}$ and suppose that $q + \sigma \le 2^w$. Then,

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{Lae0}}(\mathbf{A}) \le \frac{\gamma(w)q_\mathrm{e} + q_\mathrm{d} + q + \sigma + 1}{2^w} + \frac{(q+\sigma)^2}{2^{n-1}}$$

in the ideal cipher model.

Proof This proof uses the game transformation technique. In the game PGr1 given in Fig. 3, BCenc and BCdec implement E and E^{-1} using lazy evaluation, respectively, and AEenc implements E0. Thus,

$$\Pr[\mathbf{A}^{\mathsf{E0}_K} = 1] = \Pr[\mathbf{A}^{\mathrm{PGr1}} = 1].$$

PGr2 differs from PGr1 only in $\mathscr{E}$ and $\mathscr{D}$, which are given in Fig. 4. PGr2 is equivalent to PGr1 until *bad* gets `true` in $\mathscr{E}$ or $\mathscr{D}$. Thus,

$$\left|\Pr[\mathbf{A}^{\mathrm{PGr1}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGr2}} = 1]\right| \le (q+\sigma)^2/2^{n+1}.$$

PGr3 differs from PGr2 only in **Initialization**, $\mathscr{E}$ and $\mathscr{D}$, which are given in Fig. 5. The differences are minor, and

$$\Pr[\mathbf{A}^{\mathrm{PGr3}} = 1] = \Pr[\mathbf{A}^{\mathrm{PGr2}} = 1].$$

PGr4 differs from PGr3 only in $\mathscr{E}$ and $\mathscr{D}$, which are

Initialization:
$K \twoheadleftarrow \Sigma^w$;
$\mathtt{E}[S,U] \leftarrow \perp$ for every (S,U);
$\mathtt{D}[S,V] \leftarrow \perp$ for every (S,V);
$P_S \leftarrow \{\}$ for every S; $C_S \leftarrow \{\}$ for every S;
$bad \leftarrow$ `false`;

Function $\mathscr{E}(S,U)$:
if $\mathtt{E}[S,U] = \perp$ **then**
  $V \twoheadleftarrow \Sigma^n \setminus C_S$
  $P_S \leftarrow P_S \cup \{U\}$
  $C_S \leftarrow C_S \cup \{V\}$
  $\mathtt{E}[S,U] \leftarrow V$
  $\mathtt{D}[S,V] \leftarrow U$
return $\mathtt{E}[S,U]$

Function $\mathscr{D}(S,V)$:
if $\mathtt{D}[S,V] = \perp$ **then**
  $U \twoheadleftarrow \Sigma^n \setminus P_S$
  $P_S \leftarrow P_S \cup \{U\}$
  $C_S \leftarrow C_S \cup \{V\}$
  $\mathtt{E}[S,U] \leftarrow V$
  $\mathtt{D}[S,V] \leftarrow U$
return $\mathtt{D}[S,V]$

Oracle $\mathsf{AEenc}(N, A, M)$:
$(A_1, A_2, \ldots, A_a) \leftarrow \mathsf{pad}(A)$;
$(M_1, M_2, \ldots, M_m) \leftarrow \mathsf{pad}(M)$;
$Y_0 \leftarrow \mathscr{E}(K, N)$;
for $i = 1$ **to** $a-1$ **do**
  $Y_i \leftarrow \mathscr{E}(Y_{i-1,0}, A_i \| Y_{i-1,1})$;
if $|A| > 0 \wedge |A| \equiv 0 \pmod{w}$ **then**
  $Y_a \leftarrow \mathscr{E}(Y_{a-1,0}, A_a \| \pi_0(Y_{a-1,1}))$;
else
  $Y_a \leftarrow \mathscr{E}(Y_{a-1,0}, A_a \| \pi_1(Y_{a-1,1}))$;
for $i = 1$ **to** $m-1$ **do**
  $C_i \leftarrow M_i \oplus Y_{a+i-1,1}$;
  $Y_{a+i} \leftarrow \mathscr{E}(Y_{a+i-1,0}, M_i \| Y_{a+i-1,1})$;
$C_m \leftarrow M_m \oplus Y_{a+m-1,1}$;
if $|M| > 0 \wedge |M| \equiv 0 \pmod{w}$ **then**
  $T \leftarrow \mathscr{E}(Y_{a+m-1,0}, M_m \| \pi_0(Y_{a+m-1,1}))$;
else
  $T \leftarrow \mathscr{E}(Y_{a+m-1,0}, M_m \| \pi_1(Y_{a+m-1,1}))$;
$C \leftarrow C_1 \| \cdots \| C_{m-1} \| \mathsf{msb}_{|M|-(m-1)w}(C_m)$;
return C, T;

Oracle $\mathsf{BCenc}(S,U)$:
return $\mathscr{E}(S,U)$;

Oracle $\mathsf{BCdec}(S,V)$:
return $\mathscr{D}(S,V)$;

Fig. 3 Game PGr1

Function $\mathscr{E}(S,U)$:
if $\mathtt{E}[S,U] = \perp$ **then**
  $V \twoheadleftarrow \Sigma^n$
  if $V \in C_S$ **then**
    $bad \leftarrow$ `true`
  $P_S \leftarrow P_S \cup \{U\}$
  $C_S \leftarrow C_S \cup \{V\}$
  $\mathtt{E}[S,U] \leftarrow V$
  $\mathtt{D}[S,V] \leftarrow U$
return $\mathtt{E}[S,U]$

Function $\mathscr{D}(S,V)$:
if $\mathtt{D}[S,V] = \perp$ **then**
  $U \twoheadleftarrow \Sigma^n$
  if $U \in P_S$ **then**
    $bad \leftarrow$ `true`
  $P_S \leftarrow P_S \cup \{U\}$
  $C_S \leftarrow C_S \cup \{V\}$
  $\mathtt{E}[S,U] \leftarrow V$
  $\mathtt{D}[S,V] \leftarrow U$
return $\mathtt{D}[S,V]$

Fig. 4 Game PGr2

```
Initialization:
K ←$ Σ^w;
E[S, U] ← ⊥ for every (S, U);
D[S, V] ← ⊥ for every (S, V);
bad ← false;

Function 𝓔(S, U):                 Function 𝓓(S, V):
if E[S, U] = ⊥ then               if D[S, V] = ⊥ then
    V ←$ Σ^n                          U ←$ Σ^n
    E[S, U] ← V                       E[S, U] ← V
    D[S, V] ← U                       D[S, V] ← U
return E[S, U]                    return D[S, V]
```

Fig. 5 Game PGr3

```
Function 𝓔(S, U):                 Function 𝓓(S, V):
if E[S, U] ≠ ⊥ then               if D[S, V] ≠ ⊥ then
    bad ← true                        bad ← true
else                              else
    V ←$ Σ^n                          U ←$ Σ^n
    E[S, U] ← V                       E[S, U] ← V
    D[S, V] ← U                       D[S, V] ← U
return E[S, U]                    return D[S, V]
```

Fig. 6 Game PGr4

given in Fig. 6. The differences are also minor, and

$$\Pr[\mathbf{A}^{\mathrm{PGr4}} = 1] = \Pr[\mathbf{A}^{\mathrm{PGr3}} = 1].$$

In the game PGi1 given in Fig. 7, BCenc and BCdec implement E and E^{-1} using lazy evaluation, respectively, and AEenc implements \$. Thus,

$$\Pr[\mathbf{A}^{\$} = 1] = \Pr[\mathbf{A}^{\mathrm{PGi1}} = 1].$$

PGi2 differs from PGi1 only in $\mathscr{E}$ and $\mathscr{D}$, which are given in Fig. 8. Similar to the transformation from PGr1 to PGr3,

$$\left|\Pr[\mathbf{A}^{\mathrm{PGi1}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGi2}} = 1]\right| \le q^2/2^{n+1}.$$

Notice that $\mathscr{E}$ and $\mathscr{D}$ are called only by BCenc and BCdec, respectively.

PGr4 is equivalent to PGi2 until *bad* gets `true` in PGr4. Let Bad be the event that $\mathbf{A}^{\mathrm{PGr4}}$ sets *bad* `true`. Then,

$$\left|\Pr[\mathbf{A}^{\mathrm{PGr4}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGi2}} = 1]\right| \le \Pr[\mathsf{Bad}].$$

For PGr4, let Hit be the event that $\mathscr{E}$ receives a query (K, U) for some U except for the cases that (K, N) is the first query made by AEenc to respond to a query (N, A, M) made by $\mathbf{A}$, or $\mathscr{D}$ receives a query (K, V) for some V. Then,

$$\Pr[\mathsf{Bad}] \le \Pr[\mathsf{Hit}] + \Pr[\mathsf{Bad} \mid \overline{\mathsf{Hit}}]$$

and

$$\Pr[\mathsf{Hit}] \le (q + \sigma)/2^w.$$

For Bad, let $\mathsf{Bad}_{\mathsf{AE}}$ be the event that a query from AEenc to $\mathscr{E}$ sets *bad* `true` for the first time and $\mathsf{Bad}_{\mathsf{BC}}$ be the event that a query from BCenc or BCdec sets *bad* `true` for the first time. Then,

$$\Pr[\mathsf{Bad} \mid \overline{\mathsf{Hit}}] \le \Pr[\mathsf{Bad}_{\mathsf{AE}} \mid \overline{\mathsf{Hit}}] + \Pr[\mathsf{Bad}_{\mathsf{BC}} \mid \overline{\mathsf{Hit}}].$$

$$\Pr[\mathsf{Bad}_{\mathsf{AE}} \mid \overline{\mathsf{Hit}}] \le \sigma(q + \sigma)/2^n.$$

Further, for $\mathsf{Bad}_{\mathsf{BC}}$, let $\mathsf{Bad}_{\mathsf{BCe}}$ and $\mathsf{Bad}_{\mathsf{BCd}}$ be the events that a query from BCenc and BCdec sets *bad* `true` for the first time, respectively. Then,

$$\Pr[\mathsf{Bad}_{\mathsf{BC}} \mid \overline{\mathsf{Hit}}] \le \Pr[\mathsf{Bad}_{\mathsf{BCe}} \mid \overline{\mathsf{Hit}}] + \Pr[\mathsf{Bad}_{\mathsf{BCd}} \mid \overline{\mathsf{Hit}}].$$

For $\mathsf{Bad}_{\mathsf{BCe}}$, from Lemma 1,

$$\Pr[\mathsf{Bad}_{\mathsf{BCe}} \mid \overline{\mathsf{Hit}}] \le \gamma(w) q_{\mathrm{e}}/2^w + 1/2^w.$$

For $\mathsf{Bad}_{\mathsf{BCd}}$, considering the probability of collision among the replies from $\mathscr{E}$, we obtain

$$\Pr[\mathsf{Bad}_{\mathsf{BCd}} \mid \overline{\mathsf{Hit}}] \le q_{\mathrm{d}}/2^w + (q + \sigma)^2/2^{n+1}.$$

Thus,

$$\left|\Pr[\mathbf{A}^{\mathrm{PGr4}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGi2}} = 1]\right| \le \frac{\gamma(w) q_{\mathrm{e}} + q_{\mathrm{d}} + q + \sigma + 1}{2^w} + \frac{\sigma(q + \sigma)}{2^n} + \frac{(q + \sigma)^2}{2^{n+1}}.$$

Consequently,

$$\begin{aligned}\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{Lae0}}(\mathbf{A}) \le &\left|\Pr[\mathbf{A}^{\mathrm{PGr4}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGi2}} = 1]\right| \\ &+ \left|\Pr[\mathbf{A}^{\mathrm{PGr1}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGr2}} = 1]\right| \\ &+ \left|\Pr[\mathbf{A}^{\mathrm{PGi1}} = 1] - \Pr[\mathbf{A}^{\mathrm{PGi2}} = 1]\right|\end{aligned}$$

```
Initialization:
E[S, U] ← ⊥ for every (S, U);
D[S, V] ← ⊥ for every (S, V);
P_S ← {} for every S; C_S ← {} for every S;

Function 𝓔(S, U):                 Function 𝓓(S, V):
if E[S, U] = ⊥ then               if D[S, V] = ⊥ then
    V ←$ Σ^n \ C_S                    U ←$ Σ^n \ P_S
    P_S ← P_S ∪ {U}                   P_S ← P_S ∪ {U}
    C_S ← C_S ∪ {V}                   C_S ← C_S ∪ {V}
    E[S, U] ← V                       E[S, U] ← V
    D[S, V] ← U                       D[S, V] ← U
return E[S, U]                    return D[S, V]

Oracle AEenc(N, A, M):
C ←$ Σ^|M|; T ←$ Σ^n;
return C, T;

Oracle BCenc(S, U):               Oracle BCdec(S, V):
return 𝓔(S, U);                   return 𝓓(S, V);
```

Fig. 7 Game PGi1

```
Function 𝓔(S, U):                 Function 𝓓(S, V):
V ←$ Σ^n                          U ←$ Σ^n
E[S, U] ← V                       E[S, U] ← V
D[S, V] ← U                       D[S, V] ← U
return E[S, U]                    return D[S, V]
```

Fig. 8 Game PGi2

$$\leq \frac{\gamma(w)q_{\mathrm{e}} + q_{\mathrm{d}} + q + \sigma + 1}{2^w} + \frac{\sigma(q+\sigma)}{2^n} + \frac{(q+\sigma)^2}{2^n} + \frac{q^2}{2^{n+1}},$$

where

$$\frac{\sigma(q+\sigma)}{2^n} + \frac{(q+\sigma)^2}{2^n} + \frac{q^2}{2^{n+1}} \leq \frac{(q+\sigma)^2}{2^{n-1}}.$$

□

5.2 Authenticity

We discuss the authenticity of Lae0 under misuses. Namely, we assume NR and RUP in the following analysis.

Definition 1 Let $\Pi \subset \mathcal{P}(\mathcal{X})$. We say that Π is pairwise everywhere distinct if, for every $\pi, \pi' \in \Pi$ such that $\pi \neq \pi'$, $\pi(x) \neq \pi'(x)$ for every $x \in \mathcal{X}$.

From the following theorem, for authenticity, Lae0 is secure against adversaries causing at most $O(2^w/\gamma(w))$ evaluations of its underlying block cipher in the setting allowing both NR and RUP.

Theorem 2 For permutations π_0 and π_1 on Σ^w used in Lae0, suppose that $\{\pi_0, \pi_1, \iota\}$ is pairwise everywhere distinct. Let $\mathbf{A}$ be any adversary against Lae0 for authenticity. Suppose that $\mathbf{A}$ makes at most q_{e} and q_{d} queries to E and E^{-1}, respectively, and q_{D} queries to D0. Suppose that σ is the total number of the queries to E induced by the queries to E0 and D0 made by $\mathbf{A}$. Let $q = q_{\mathrm{e}} + q_{\mathrm{d}}$ and suppose that $q + \sigma \leq 2^w$. Then,

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathsf{Lae0}}(\mathbf{A}) \leq \frac{3\gamma(w)q + q_{\mathrm{d}}}{2^w - 1} + \frac{q+\sigma+1}{2^w} + \frac{q_{\mathrm{D}} + 7\sigma^2 + 3q\sigma}{2^n - q - \sigma}$$

in the ideal cipher model.

Proof In this proof, we refer to the game AG1 given in Fig. 9. In this game, BCenc and BCdec implement E and E^{-1} using lazy evaluation, respectively. AEenc and AEdec implement E0 and D0, respectively.

It is assumed that, for each query made by $\mathbf{A}$, AEenc and AEdec give all $Y_{j,1}$'s to $\mathbf{A}$ together with the corresponding reply. Then, they are more informative than in the RUP setting.

Let $\mathcal{E}$ be the set of input-output pairs of the underlying block cipher obtained by the queries to $\mathscr{E}$ induced by the queries to AEenc and AEdec.

Let MCol be the event that

$$\max_{v \in \Sigma^w} \left| \{(S, U, V) \in \mathcal{E} \mid \mathsf{lsb}_w(V) = v\} \right| > \gamma(w).$$

Then, since $\sigma \leq 2^w$, from Lemma 1,

$\Pr[\mathsf{MCol}] \leq 1/2^w$.

For a query to $\mathscr{E}$ or $\mathscr{D}$, let $\mathcal{W}_{\mathsf{AE}}$ be the set of (S, U, V)'s

```
Initialization:
  K ↞ Σ^w;
  E[S,U] ← ⊥ for every (S,U);
  D[S,V] ← ⊥ for every (S,V);
  P_S ← {}; C_S ← {};

Function 𝓔(S,U):
  if E[S,U] = ⊥ then
      V ↞ Σ^n \ C_S
      P_S ← P_S ∪ {U}
      C_S ← C_S ∪ {V}
      E[S,U] ← V
      D[S,V] ← U
  return E[S,U]

Function 𝒟(S,V):
  if D[S,V] = ⊥ then
      U ↞ Σ^n \ P_S
      P_S ← P_S ∪ {U}
      C_S ← C_S ∪ {V}
      E[S,U] ← V
      D[S,V] ← U
  return D[S,V]

Oracle AEenc(N,A,M):
  (A_1, A_2, ..., A_a) ← pad(A);
  (M_1, M_2, ..., M_m) ← pad(M);
  Y_0 ← 𝓔(K,N);
  for i = 1 to a − 1 do
      Y_i ← 𝓔(Y_{i−1,0}, A_i || Y_{i−1,1});
  if |A| > 0 ∧ |A| ≡ 0 (mod w) then
      Y_a ← 𝓔(Y_{a−1,0}, A_a || π_0(Y_{a−1,1}));
  else
      Y_a ← 𝓔(Y_{a−1,0}, A_a || π_1(Y_{a−1,1}));
  for i = 1 to m − 1 do
      C_i ← M_i ⊕ Y_{a+i−1,1};
      Y_{a+i} ← 𝓔(Y_{a+i−1,0}, M_i || Y_{a+i−1,1});
  C_m ← M_m ⊕ Y_{a+m−1,1};
  if |M| > 0 ∧ |M| ≡ 0 (mod w) then
      T ← 𝓔(Y_{a+m−1,0}, M_m || π_0(Y_{a+m−1,1}));
  else
      T ← 𝓔(Y_{a+m−1,0}, M_m || π_1(Y_{a+m−1,1}));
  C ← C_1 || ··· || C_{m−1} || msb_{|M|−(m−1)w}(C_m);
  return C, T;

Oracle AEdec(N,A,C,T):
  (A_1, A_2, ..., A_a) ← pad(A);
  (C_1, C_2, ..., C_m) ← pad(C);
  Y_0 ← 𝓔(K,N);
  for i = 1 to a − 1 do
      Y_i ← 𝓔(Y_{i−1,0}, A_i || Y_{i−1,1});
  if |A| > 0 ∧ |A| ≡ 0 (mod w) then
      Y_a ← 𝓔(Y_{a−1,0}, A_a || π_0(Y_{a−1,1}));
  else
      Y_a ← 𝓔(Y_{a−1,0}, A_a || π_1(Y_{a−1,1}));
  for i = 1 to m − 1 do
      M_i ← C_i ⊕ Y_{a+i−1,1};
      Y_{a+i} ← 𝓔(Y_{a+i−1,0}, M_i || Y_{a+i−1,1});
  M_m ← C_m ⊕ msb_{|C|−(m−1)w}(Y_{a+m−1,1});
  if |C| > 0 ∧ |C| ≡ 0 (mod w) then
      T' ← 𝓔(Y_{a+m−1,0}, M_m || π_0(Y_{a+m−1,1}));
  else
      T' ← 𝓔(Y_{a+m−1,0}, M_m || π_1(Y_{a+m−1,1}));
  M ← M_1 || ··· || M_{m−1} || msb_{|C|−(m−1)w}(M_m);
  if T' = T then
      return M;
  else
      return ⊥;

Oracle BCenc(S,U):
  return 𝓔(S,U);

Oracle BCdec(S,V):
  return 𝒟(S,V);
```

Fig. 9 Game AG1

obtained by all the previous queries to $\mathscr{E}$ induced by queries to AEenc or AEdec made by $\mathbf{A}$. For a query to $\mathscr{E}$ or $\mathscr{D}$, let $\mathcal{W}_{\mathsf{BC}}$ be the set of (S,U,V)'s obtained by all the previous queries to BCenc or BCdec made by $\mathbf{A}$. A query (S,U) to $\mathscr{E}$ is called fresh if $\mathtt{E}[S,U] = \perp$.

Let $\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}$ be the event that, for a fresh query to $\mathscr{E}$ induced by a query to AEenc or AEdec, $\mathscr{E}$ replies V such that $V_0 = K$ or, for some $(S',U',V') \in \mathcal{W}_{\mathsf{AE}}$, $V_0 = V_0'$ and $\{V_1, \pi_0(V_1), \pi_1(V_1)\} \cap \{V_1', \pi_0(V_1'), \pi_1(V_1')\} \neq \emptyset$, that is,

$$V_1 \in \{V_1', \pi_0(V_1'), \pi_1(V_1'), \pi_0^{-1}(V_1'), \pi_0^{-1}(\pi_1(V_1')), \pi_1^{-1}(V_1'), \pi_1^{-1}(\pi_0(V_1'))\},$$

where $V = V_0 \| V_1$, $V' = V_0' \| V_1'$ and $|V_0| = |V_1| = |V_0'| = |V_1'| = w$. Then,

$$\Pr[\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}] \leq \frac{\sigma}{2^w} + \frac{7\sigma^2}{2^n - q - \sigma}.$$

Let $\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{BC}}$ be the event that, for a fresh query to $\mathscr{E}$ induced by a query to AEenc or AEdec, $\mathscr{E}$ replies V such that, for some $(S',U',V') \in \mathcal{W}_{\mathsf{BC}}$, $S' = V_0$ and $\mathsf{lsb}_w(U') \in \{V_1, \pi_0(V_1), \pi_1(V_1)\}$. Then,

$$\Pr[\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{BC}}] \leq 3q\sigma/(2^n - q - \sigma).$$

Let $\mathsf{Bad}_{\mathsf{BCe}}$ be the event that $\mathbf{A}$ makes at least one query (S,U) to BCenc such that $S = K$ or, for some $(S',U',V') \in \mathcal{W}_{\mathsf{AE}}$, $S = V_0'$ and $U_1 \in \{V_1', \pi_0(V_1'), \pi_1(V_1')\}$. Then, since $q + \sigma \leq 2^w$,

$$\Pr[\mathsf{Bad}_{\mathsf{BCe}} \mid \overline{\mathsf{MCol}}] \leq \frac{q_{\mathrm{e}}}{2^w} + \frac{2^w \cdot 3\gamma(w) q_{\mathrm{e}}}{2^n - (q+\sigma)} \leq \frac{q_{\mathrm{e}}}{2^w} + \frac{3\gamma(w) q_{\mathrm{e}}}{2^w - 1}.$$

Let $\mathsf{Bad}_{\mathsf{BCd}}$ be the event that $\mathbf{A}$ makes at least one query (S,V) to BCdec such that $S = K$ or, for some $(S',U',V') \in \mathcal{W}_{\mathsf{AE}}$, $S = S'$ and $V = V'$, or $S = V_0'$ and $\mathsf{lsb}_w(U) \in \{V_1', \pi_0(V_1'), \pi_1(V_1')\}$, where U is the reply to the query (S,V). Then,

$$\Pr[\mathsf{Bad}_{\mathsf{BCd}} \mid \overline{\mathsf{MCol}} \cap \overline{\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}}] \leq \frac{q_{\mathrm{d}}}{2^w} + \frac{q_{\mathrm{d}}}{2^w - 1} + \frac{3\gamma(w) q_{\mathrm{d}}}{2^w - 1}.$$

Let Forge be the event that $\mathbf{A}$ succeeds in forgery. Let $\mathsf{Bad} = \mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}} \cup \mathsf{Bad}_{\mathsf{AE}}^{\mathsf{BC}} \cup \mathsf{Bad}_{\mathsf{BCe}} \cup \mathsf{Bad}_{\mathsf{BCd}}$. If Bad does not occur, then, since $\{\pi_0, \pi_1, \iota\}$ is pairwise everywhere distinct, for each query to AEdec made by $\mathbf{A}$, the final query to $\mathscr{E}$ induced by the query is fresh. Thus,

$$\mathrm{Adv}_{\mathsf{Lae0}}^{\mathrm{auth}}(\mathbf{A}) = \Pr[\mathsf{Forge}] \leq \Pr[\mathsf{Bad}] + \Pr[\mathsf{Forge} \mid \overline{\mathsf{Bad}}],$$

where

$$\Pr[\mathsf{Forge} \mid \overline{\mathsf{Bad}}] \leq q_{\mathrm{D}}/(2^n - q - \sigma).$$

In addition,

$$\Pr[\mathsf{Bad}] = \Pr[\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}} \cup \mathsf{Bad}_{\mathsf{AE}}^{\mathsf{BC}} \cup \mathsf{Bad}_{\mathsf{BCe}} \cup \mathsf{Bad}_{\mathsf{BCd}}] \leq \Pr[\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}] + \Pr[\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{BC}}] + \Pr[\mathsf{Bad}_{\mathsf{BCe}} \cup (\mathsf{Bad}_{\mathsf{BCd}} \cap \overline{\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}})],$$

and

$$\Pr[\mathsf{Bad}_{\mathsf{BCe}} \cup (\mathsf{Bad}_{\mathsf{BCd}} \cap \overline{\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}})] \leq \Pr[\mathsf{MCol}] + \Pr[\mathsf{Bad}_{\mathsf{BCe}} \cup (\mathsf{Bad}_{\mathsf{BCd}} \cap \overline{\mathsf{Bad}_{\mathsf{AE}}^{\mathsf{AE}}}) \mid \overline{\mathsf{MCol}}].$$

Thus,

$$\Pr[\mathsf{Bad}] \leq \frac{3\gamma(w) q + q_{\mathrm{d}}}{2^w - 1} + \frac{q + \sigma + 1}{2^w} + \frac{7\sigma^2 + 3q\sigma}{2^n - q - \sigma}.$$

This completes the proof. □

6. Conclusion

The privacy and authenticity of $\mathsf{Lae0}$ have been analyzed in the ideal cipher model. The analysis implies that, for both privacy and authenticity, the instantiation of $\mathsf{Lae0}$ with the Lesamnta-LW block cipher has about 120-bit security against generic attacks regarding the block cipher as a black box.

Acknowledgments

The first author was supported in part by JSPS KAKENHI Grant Number JP18H05289.

References

[1] FIPS PUB 197, "Advanced encryption standard (AES)," 2001.
[2] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Duplexing the sponge: Single-pass authenticated encryption and other applications," SAC 2011, ed. A. Miri and S. Vaudenay, Lect. Notes Comput. Sci., vol.7118, pp.320–337, Springer, 2011.
[3] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge functions," ECRYPT Hash Workshop, 2007.
[4] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "The Keccak sponge function family," 2008. http://keccak.noekeon.org.
[5] FIPS PUB 202, "SHA-3 standard: Permutation-based hash and extendable-output functions," 2015.
[6] ISO/IEC 29192-5, "Information technology – security techniques – lightweight cryptography – part 5: Hash-functions," 2016.
[7] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," CRYPTO 2011, ed. P. Rogaway, Lect. Notes Comput. Sci., vol.6841, pp.222–239, Springer, 2011.
[8] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "spongent: A lightweight hash function," CHES 2011, ed. B. Preneel and T. Takagi, Lect. Notes Comput. Sci., vol.6917, pp.312–325, Springer, 2011.
[9] 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.
[10] I. Damgård, "A design principle for hash functions," in Brassard [30], pp.416–427, Springer, 1990.
[11] R.C. Merkle, "One way hash functions and DES," in Brassard [30], pp.428–446, Springer, 1990.
[12] S. Hirose, H. Kuwakado, and H. Yoshida, "Authenticated encryption based on Lesamnta-LW hashing mode," ICISC 2019, ed. J.H. Seo,

Lect. Notes Comput. Sci., vol.11975, pp.52–69, Springer, 2019.
[13] J. Katz and M. Yung, "Complete characterization of security notions for probabilistic private-key encryption," Proc. Thirty-Second Annual ACM Symposium on Theory of Computing, pp.245–254, May 2000.
[14] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," ASIACRYPT 2000, ed. T. Okamoto, Lect. Notes Comput. Sci., vol.1976, pp.531–545, Springer, 2000.
[15] C.S. Jutla, "Encryption modes with almost free message integrity," EUROCRYPT 2001, ed. B. Pfitzmann, Lect. Notes Comput. Sci., vol.2045, pp.529–544, Springer, 2001.
[16] P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: a block-cipher mode of operation for efficient authenticated encryption," ACM Conference on Computer and Communications Security, pp.196–205, Nov. 2001.
[17] NIST Special Publication 800-38C, "Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality," 2004.
[18] NIST Special Publication 800-38D, "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," 2007.
[19] ISO/IEC 19772, "Information technology – security techniques – authenticated encryption," 2009.
[20] S. Cogliani, D. Maimut, D. Naccache, R.P. do Canto, R. Reyhanitabar, S. Vaudenay, and D. Vizár, "OMD: A compression function mode of operation for authenticated encryption," SAC 2014, ed. A. Joux and A.M. Youssef, Lect. Notes Comput. Sci., vol.8781, pp.112–128, Springer, 2014.
[21] FIPS PUB 180-4, "Secure hash standard (SHS)," Aug. 2015.
[22] P. Rogaway, "Nonce-based symmetric encryption," FSE 2004, ed. B.K. Roy and W. Meier, Lect. Notes Comput. Sci., vol.3017, pp.348–359, Springer, 2004.
[23] C. Namprempre, P. Rogaway, and T. Shrimpton, "Reconsidering generic composition," EUROCRYPT 2014, ed. P.Q. Nguyen and E. Oswald, Lect. Notes Comput. Sci., vol.8441, pp.257–274, Springer, 2014.
[24] P. Rogaway and T. Shrimpton, "A provable-security treatment of the key-wrap problem," EUROCRYPT 2006, ed. S. Vaudenay, Lect. Notes Comput. Sci., vol.4004, pp.373–390, Springer, 2006.
[25] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda, "How to securely release unverified plaintext in authenticated encryption," ASIACRYPT 2014, ed. P. Sarkar and T. Iwata, Lect. Notes Comput. Sci., vol.8873, pp.105–125, Springer, 2014.
[26] V.T. Hoang, T. Krovetz, and P. Rogaway, "Robust authenticated-encryption AEZ and the problem that it solves," EUROCRYPT 2015, ed. E. Oswald and M. Fischlin, Lect. Notes Comput. Sci., vol.9056, pp.15–44, Springer, 2015.
[27] S. Hirose, Y. Sasaki, and H. Yoshida, "Lesamnta-LW revisited: Improved security analysis of primitive and new PRF mode," ACNS 2020, ed. M. Conti, J. Zhou, E. Casalicchio, and A. Spognardi, Lect. Notes Comput. Sci., vol.12146, pp.89–109, Springer, 2020.
[28] R. Shiba, K. Sakamoto, F. Liu, K. Minematsu, and T. Isobe, "Integral and impossible differential attacks on the reduced-round Lesamnta-LW-BC," The 38th Symposium on Cryptography and Information Security, 1B1-2, 2021.
[29] R. Motwani and P. Raghavan, Randomized Algorithms, Cambridge University Press, 1995.
[30] G. Brassard, ed., Advances in Cryptology - CRYPTO '89, Lect. Notes Comput. Sci., vol.435, Springer, 1990.

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 team leader at the National Institute of Advanced Industrial Science and Technology (AIST). He is a member of IACR, IPSJ, and JSAE. In 2013, he won the award of industrial standardization that has been granted by the Japanese Ministry of Economy, Trade and Industry (METI).