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

Shoichi HIROSE, Member, Hidenori KUWAKADO, Senior Member, and Hirotaka YOSHIDA, 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 Læ0 satisfies both privacy and authenticity if the underlying block cipher is a pseudo-random 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 Læ0 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 Lesamnta-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 Læ0. 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 Læ0 is secure in the standard model: Læ0 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 Læ0 with the block cipher of Lesamnta-LW. Their upper bound on the advantage of any adversary A against Læ0 has the term $\ell q \text{adv}_{E}^{\text{pp}}$, where $\text{adv}_{E}^{\text{pp}}$ is the advantage of an adversary constructed from A against the underlying block cipher $E$. $\ell$ 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 $E$, adv$_{E}^{\text{pp}} = \Omega(t/2^w)$, 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 $\ell q$ and $t$ are $\Omega(2^{w/2})$. For the block cipher of Lesamnta-LW, $w = 128$.

In this paper, we analyze the security of Læ0 in the ideal cipher model. In terms of both privacy and authenticity, our result implies about 120-bit security for instantiation of Læ0 with the block cipher of Lesamnta-LW. We discuss the authenticity of Læ0 under two typical misuses: nonce repetition (NR) and releasing unverified plaintexts (RUP).
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 nonce-based AEAD in Sect. 3. The nonce-based AEAD scheme Lae0 is given in Sect. 6. Syntax and security are formalized for the Merkle-Damgård hashing such as SHA-2 [21].

Nonce-based symmetric encryption was introduced by Rogaway [22]. The generic composition of nonce-based AEAD was discussed by Namprempre et al. [20], which is a mode of operation of a compression function for the Merkle-Damgård hashing.

Robust authenticated encryption was introduced 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 $\Sigma^l$ be identified with the set of all $\Sigma$-sequences of length $l$. $\Sigma^0 = \{\varepsilon\}$, where $\varepsilon$ is the empty sequence. $\Sigma^1 = \Sigma$. Let $(\Sigma^l)^+ = \bigcup_{i \geq 0} (\Sigma^i)^+$ and $(\Sigma^i)^+ = \bigcup_{j \geq 0} (\Sigma^j)^+$. For $x \in \Sigma^*$, the length of $x$ is denoted by $|x|$. For $x_1, x_2 \in \Sigma^*$, $x_1|\underline{x}_2$ represents their concatenation. For $x \in \Sigma^*$ and an integer $0 \leq l \leq |x|$, msb$_l(x)$ represents the most significant $l$ bits of $x$, and 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 $y$. $|y|^{|x|-|y|}$.

Selecting an element $s$ from a set $S$ uniformly at random is denoted by $s \leftarrow S$.

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 $\mathcal{P}(\mathcal{X})$. $\iota$ represents an identity permutation. The set of all block ciphers with a key size $\kappa$ and a block size $n$ is denoted by $\mathcal{B}(\kappa, n)$. A block cipher in $\mathcal{B}(\kappa, n)$ is called a $(\kappa, n)$ block cipher. For a keyed function $f : K \times X \rightarrow Y$, $f(K, \cdot)$ is often denoted by $fx(\cdot)$.

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 $\Sigma^{n/2}$ and range $\Sigma^n$. 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 $\text{Enc} : \mathcal{K} \times N \times A \times M \rightarrow C \times T$ and the decryption function is $\text{Dec} : \mathcal{K} \times N \times A \times C \times T \rightarrow M \cup \{\perp\}$, where $\mathcal{K}$ is a key space, $N$ is a nonce space, $A$ is an associated-data space, $M$ is a message space, $C$ is a ciphertext space, and $T$ is a tag space. $M \subseteq \Sigma^*$, $\perp \notin M$ and $A \subseteq \Sigma^*$. If $M \in M$, then $\Sigma^{|M|} \subset M$. For any $K \in \mathcal{K}$, if $(C, T) \leftarrow \text{Enc}_K(N, A, M)$ for some $(N, A, M) \in N \times A \times M$, then $M \leftarrow \text{Dec}_K(N, A, C, T)$. Otherwise, $\perp \leftarrow \text{Dec}_K(N, A, C, T)$, 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 $S$ be a random function taking $(N, A, M) \in N \times A \times
$M$ as input and returning a binary sequence of length $|\text{Enc}_K(N,A,M)|$, which is chosen uniformly at random. The privacy of an AEAD scheme ($\text{Enc}, \text{Dec}$) is defined by the indistinguishability between $\text{Enc}_K$ and $\mathcal{S}$:

$$\text{Adv}^{\text{priv}}_{(\text{Enc},\text{Dec})}(A) = |\text{Pr}[A^{\text{Enc}_K} = 1] - \text{Pr}[A^{\mathcal{S}} = 1]|,$$

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

(2) Authenticity

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

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

where $K \leftarrow \mathcal{K}$. $A$ succeeds in forgery if it succeeds in making a decryption query such that its corresponding reply from $\text{Dec}_K$ is not $\perp$. $A$ is not allowed to make a trivial decryption query. Namely, if $A$ 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 $X \in \Sigma^*$,

$$\text{pad}(X) = \begin{cases} X & \text{if } |X| > 0 \text{ and } |X| \equiv 0 \pmod{w} \\
X||10^{(t+1)w-|X|} & \text{if } |X| = 0 \text{ or } |X| \not\equiv 0 \pmod{w}, \end{cases}$$

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

Let $\text{pad}(X) = (X_1, X_2, \ldots, X_t)$, where $|X_i| = w$ for every $i$ such that $1 \leq i \leq x$. $x = 1$ if $|X| = 0$, and $x = [|X|/w]$ if $|X| > 0$. $X_t$ is called the $i$-th block of $\text{pad}(X)$.

For $E \in \mathcal{B}(w,n)$ and $\pi_0, \pi_1 \in \mathcal{P}(\Sigma^w)$, the nonce-based AEAD scheme Lae0 = ($E_0, D_0$) is presented by Algorithm 1. The encryption function $E_0$ is also depicted in Fig. 2. For Lae0, the key space is $\Sigma^n$, the nonce space is $\Sigma^n$, and the tag space is $\Sigma^\tau$, where $0 < \tau \leq n$. The associated-data space, the message space and the ciphertext space are $\Sigma^n$. If $(C,T) \leftarrow \text{E}_{0}(N,A,M)$, then $|C| = |M|$.

**Algorithm 1** Encryption $E_0$ and decryption $D_0$ of Lae0

```plaintext
function $E_0(N,A,M)$
$(A_1,A_2,\ldots,A_k) \leftarrow \text{pad}(A)$;
$(M_1,M_2,\ldots,M_n) \leftarrow \text{pad}(M)$;
$Y_0 \leftarrow E_K(N)$;
for $i = 1$ to $a - 1$ do
    $Y_i \leftarrow E_{Y_{i-1}}(A_iY_{i-1})$;
if $|A| > 0 \land |A| \equiv 0 \pmod{w}$ then
    $Y_a \leftarrow E_{Y_{a-1}}(A_a[\pi_0(Y_{a-1})])$;
else
    $Y_a \leftarrow E_{Y_{a-1}}(A_a[\pi_1(Y_{a-1})])$;
end
for $i = 1$ to $m - 1$ do
    $C_i \leftarrow M_i \oplus Y_{a+i-1}$;
    $Y_{a+i} \leftarrow E_{Y_{a+i-1}}(M_i||Y_{a+i-1})$;
end
$C_m \leftarrow M_m \oplus Y_{a+m-1}$;
if $|M| > 0 \land |M| \equiv 0 \pmod{w}$ then
    $T \leftarrow E_{Y_{a+m-1}}(M_m[\pi_0(Y_{a+m-1})])$;
else
    $T \leftarrow E_{Y_{a+m-1}}(M_m[\pi_1(Y_{a+m-1})])$;
end
$C \leftarrow C_1||\cdots||C_{m-1}||\text{msb}_{|M|}(m-1)(C_m)$;
return $(C,T)$;

function $D_0(N,A,C,T)$
$(A_1,A_2,\ldots,A_k) \leftarrow \text{pad}(A)$;
$(C_1,C_2,\ldots,C_m) \leftarrow \text{pad}(C)$;
$Y_0 \leftarrow E_K(N)$;
for $i = 1$ to $a - 1$ do
    $Y_i \leftarrow E_{Y_{i-1}}(A_iY_{i-1})$;
if $|A| > 0 \land |A| \equiv 0 \pmod{w}$ then
    $Y_a \leftarrow E_{Y_{a-1}}(A_a[\pi_0(Y_{a-1})])$;
else
    $Y_a \leftarrow E_{Y_{a-1}}(A_a[\pi_1(Y_{a-1})])$;
end
for $i = 1$ to $m - 1$ do
    $M_i \leftarrow C_i \oplus Y_{a+i-1}$;
    $Y_{a+i} \leftarrow E_{Y_{a+i-1}}(M_i||Y_{a+i-1})$;
end
$M_m \leftarrow C_m \oplus \text{msb}_{|C|}(m-1)(Y_{a+m-1})$;
if $|C| > 0 \land |C| \equiv 0 \pmod{w}$ then
    $T' \leftarrow E_{Y_{a+m-1}}(M_m[\pi_0(Y_{a+m-1})])$;
else
    $T' \leftarrow E_{Y_{a+m-1}}(M_m[\pi_1(Y_{a+m-1})])$;
end
$M \leftarrow M_1||\cdots||M_{m-1}||\text{msb}_{|M|}(m-1)(M_m)$;
if $T' = T$ then
    return $M$;
else
return $\perp$;
```

![Fig. 2](image_url) The encryption function $E_0$ of the nonce-based AEAD scheme Lae0. $(C,T) \leftarrow \text{E}_{0}(N,A,M)$, where $\text{pad}(A) = (A_1,A_2)$, $\text{pad}(M) = (M_1,M_2,M_3)$, 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 \text{Lae0} in the Ideal Cipher Model

The security of \text{Lae0} = (E0, 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 \text{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 \(1 - \frac{1}{e}\), no bin has more than \(e\) \ln \(t\) balls in it.

For Lemma 1, let \(t = 2^w\). Then,

\[
e \ln t / \ln t = \gamma(w) = \frac{w}{(\log_2 w - \log_2 \log_2 e)},
\]

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, \text{Lae0} is secure against nonce-respecting adversaries causing at most \(O(2^w / \gamma(w))\) evaluations of its underlying block cipher. For \(w = 128\), \(2^w / \gamma(w) \approx 2^{12.25}\).

The main idea of the proof of the following theorem is simple: The outputs of \text{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 \text{E0} and the set of them obtained by the queries to \(E\) and \(E^{-1}\) made by the adversary are disjoint.

**Theorem 1** Let \(A\) be any adversary against \text{Lae0} for privacy. Suppose that \(A\) makes at most \(q_e\) and \(q_d\) queries to \(E\) and \(E^{-1}\), respectively. Suppose that \(\sigma\) is the total number of the queries to \(E\) induced by the queries to \(E0\) and \(D0\) made by \(A\). Let \(q = q_e + q_d\) and suppose that \(q + \sigma \leq 2^w\). Then,

\[
\text{Adv}_{\text{Lae0}}^{\text{priv}}(A) \leq \frac{\gamma(w)q_e + q_d + q + \sigma + 1}{2^w} + \frac{(q + \sigma)^2}{2^{w-1}}
\]
in the ideal cipher model.

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

\[
\text{Pr}[A^{\text{E0}x} = 1] = \text{Pr}[A^{\text{PGr1}} = 1].
\]

PGr2 differs from PGr1 only in \(\varepsilon\) and \(\mathcal{D}\), which are given in Fig. 4. PGr2 is equivalent to PGr1 until \text{bad} gets true in \(\varepsilon\) or \(\mathcal{D}\). Thus,

\[
|\text{Pr}[A^{\text{PGr1}} = 1] - \text{Pr}[A^{\text{PGr2}} = 1]| \leq (q + \sigma)^2 / 2^{w+1}.
\]

PGr3 differs from PGr2 only in \text{Initialization}, \(\varepsilon\) and \(\mathcal{D}\), which are given in Fig. 5. The differences are minor, and

\[
\text{Pr}[A^{\text{PGr3}} = 1] = \text{Pr}[A^{\text{PGr2}} = 1].
\]

PGr4 differs from PGr3 only in \(\varepsilon\) and \(\mathcal{D}\), which are
given in Fig. 6. The differences are also minor, and

\[
\Pr[A^{\text{PGi4}} = 1] = \Pr[A^{\text{PGi3}} = 1].
\]

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

\[
\Pr[A^S = 1] = \Pr[A^{\text{PGi1}} = 1].
\]

PGi2 differs from PGi1 only in $\mathcal{E}$ and $\mathcal{D}$, which are given in Fig. 8. Similar to the transformation from PGi1 to PGi3,

\[
\Pr[A^{\text{PGi1}} = 1] - \Pr[A^{\text{PGi2}} = 1] \leq q^2/2^{n+1}.
\]

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

PGi4 is equivalent to PGi2 until bad gets true in PGi4. Let Bad be the event that $A^{\text{PGi4}}$ sets bad true. Then,

\[
\Pr[A^{\text{PGi4}} = 1] - \Pr[A^{\text{PGi2}} = 1] \leq \Pr[\text{Bad}].
\]

For PGi4, let Hit be the event that $\mathcal{E}$ 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 A, or $\mathcal{D}$ receives a query $(K, V)$ for some $V$. Then,

\[
\Pr[\text{Bad}] \leq \Pr[\text{Hit}] + \Pr[\text{Bad} | \text{Hit}]
\]

and

\[
\Pr[\text{Hit}] \leq (q + \sigma)/2^n.
\]

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

\[
\Pr[\text{Bad} | \text{Hit}] \leq \Pr[\text{Bad}_{\text{AE}} | \text{Hit}] + \Pr[\text{Bad}_{\text{BC}} | \text{Hit}].
\]

\[
\Pr[\text{Bad}_{\text{AE}} | \text{Hit}] \leq \sigma(q + \sigma)/2^n.
\]

Further, for $\text{Bad}_{\text{BC}}$, let $\text{Bad}_{\text{BCae}}$ and $\text{Bad}_{\text{BCbd}}$ be the events that a query from BCenc and BCdec sets bad true for the first time, respectively. Then,

\[
\Pr[\text{Bad}_{\text{BC}} | \text{Hit}] \leq \Pr[\text{Bad}_{\text{BCae}} | \text{Hit}] + \Pr[\text{Bad}_{\text{BCbd}} | \text{Hit}].
\]

For $\text{Bad}_{\text{BCae}}$, from Lemma 1,

\[
\Pr[\text{Bad}_{\text{BCae}} | \text{Hit}] \leq \gamma(w)q_d/2^n + 1/2^n.
\]

For $\text{Bad}_{\text{BCbd}}$, considering the probability of collision among the replies from $\mathcal{E}$, we obtain

\[
\Pr[\text{Bad}_{\text{BCbd}} | \text{Hit}] \leq q_d/2^n + (q + \sigma)^2/2^{n+1}.
\]

Thus,

\[
\Pr[A^{\text{PGi4}} = 1] - \Pr[A^{\text{PGi2}} = 1] \leq \frac{\gamma(w)q_d + q + \sigma + 1}{2^n} + \frac{\sigma(q + \sigma)}{2^n} + \frac{(q + \sigma)^2}{2^{n+1}}.
\]

Consequently,

\[
\text{Adv}_{\text{La0}}^{\text{priv}}(A) \leq \Pr[A^{\text{PGi4}} = 1] - \Pr[A^{\text{PGi2}} = 1] + \Pr[A^{\text{PGi1}} = 1] - \Pr[A^{\text{PGi2}} = 1] + \Pr[A^{\text{PGi1}} = 1] - \Pr[A^{\text{PGi2}} = 1].
\]
Hirose et al.: Provable Security Analysis of Authenticated Encryption Based on LESAMNTA-LW in the Ideal Cipher Model

\[
\gamma(w)q_e + q_d + q + \sigma + 1
\]
\[
\frac{\sigma(q + \sigma)}{2^n} + \frac{(q + \sigma)^2}{2^n} + \frac{q^2}{2^{n+1}},
\]
where
\[
\frac{\sigma(q + \sigma)}{2^n} + \frac{(q + \sigma)^2}{2^n} + \frac{q^2}{2^{n+1}} \leq \frac{(q + \sigma)^2}{2^n}.
\]

5.2 Authenticity

We discuss the authenticity of \(L_{a0}\) under misuses. Namely, we assume NR and RUP in the following analysis.

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

From the following theorem, for authenticity, \(L_{a0}\) 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 \(\pi_0\) and \(\pi_1\) on \(\Sigma^w\) used in \(L_{a0}\), suppose that \(f_0, f_1\) is pairwise everywhere distinct. Let \(A\) be any adversary against \(L_{a0}\) for authenticity. Suppose that \(A\) makes at most \(q_e\) and \(q_d\) queries to \(E\) and \(E_1\), respectively, and \(q_D\) queries to \(D_0\). Suppose that \(\sigma\) is the total number of the queries to \(E\) induced by the queries to \(E_0\) and \(D_0\) made by \(A\). Let \(q = q_e + q_d\) and suppose that \(q + \sigma \leq 2^w\). Then,

\[
\text{Adv}_{L_{a0}}(A) \leq 3\gamma(w)q + q_e + q_d + q + \sigma + 1
\]
\[
\frac{q_d + 7q^2 + 3q\sigma}{2^w - 1} + \frac{q + \sigma + 1}{2^w} + \frac{q_d + 7q^2 + 3q\sigma}{2^w - 1} + q_d + 7q^2 + 3q\sigma
\]
in the ideal cipher model.

**Proof** In this proof, we refer to the game AG1 given in Fig. 9. In this game, \(BC_{enc}\) and \(BC_{dec}\) implement \(E\) and \(E_1\) using lazy evaluation, respectively. \(AE_{enc}\) and \(AE_{dec}\) implement \(E_0\) and \(D_0\), respectively.

It is assumed that, for each query made by \(A\), \(AE_{enc}\) and \(AE_{dec}\) give all \(Y_j\)'s to \(A\) together with the corresponding reply. Then, they are more informative than in the RUP setting.

Let \(E\) be the set of input-output pairs of the underlying block cipher obtained by the queries to \(\mathcal{E}\) induced by the queries to \(AE_{enc}\) and \(AE_{dec}\).

Let \(M_{Col}\) be the event that

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

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

\[
\Pr[M_{Col}] \leq 1/2^w.
\]

For a query to \(\mathcal{E}\) or \(\mathcal{D}\), let \(W_{AE}\) be the set of \((S, U, V)\)’s...
obtained by all the previous queries to $\varepsilon$ induced by queries to $\text{AEEnc}$ or $\text{AEdc}$ made by $A$. For a query to $\varepsilon$ or $\emptyset$, let $\mathcal{W}_{\text{BC}}$ be the set of $(S, U, V)$'s obtained by all the previous queries to $\text{BCenc}$ or $\text{BCdec}$ made by $A$. A query $(S, U)$ to $\varepsilon$ is called fresh if $E(S, U) = \bot$.

Let $\text{Bad}_{\text{AE}}^\mathcal{E}$ be the event that, for a fresh query to $\varepsilon$ induced by a query to $\text{AEEnc}$ or $\text{AEdc}$, $\varepsilon$ replies $V$ such that $V_0 = K$ or, for some $(S', U', V') \in \mathcal{W}_{\text{AE}}, V_0 = V_0'$ 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,

$$V_1 \in \{V'_1, \pi_0(V'_1), \pi_1(V'_1), \pi_0^{-1}(V'_1), \pi_1^{-1}(V'_1)\},$$

where $V = V_0 || V_1, V' = V_0' || V'_1$ and $|V_0| = |V_1| = |V_0'| = |V'_1| = w$. Then,

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

Let $\text{Bad}_{\text{BC}}^\mathcal{E}$ be the event that, for a fresh query to $\varepsilon$ induced by a query to $\text{AEEnc}$ or $\text{AEdc}$, $\varepsilon$ replies $V$ such that, for some $(S', U', V') \in \mathcal{W}_{\text{BC}}, S' = V_0$ and $\text{lsb}(U') \in \{V'_1, \pi_0(V'_1), \pi_1(V'_1)\}$. Then, since $q + \sigma \leq 2^w$,

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

Let $\text{Bad}_{\text{BCd}}$ be the event that $A$ makes at least one query $(S, U) = V$ to $\text{BCdec}$ such that $S = K$ or, for some $(S', U', V') \in \mathcal{W}_{\text{AE}}, S = S'$ and $V = V'$, or $S = V_0'$ and $\text{lsb}(U) \in \{V'_1, \pi_0(V'_1), \pi_1(V'_1)\}$, where $U$ is the reply to the query $(S, V)$. Then,

$$\Pr[\text{Bad}_{\text{BCd}} | \text{MCol} \cap \text{Bad}_{\text{AE}}] \leq \frac{q e}{2^w} + \frac{q d}{2^w - 1} + \frac{3\gamma(q)d}{2^w - 1}.$$

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

$$\text{Adv}_{\text{La0}}^\mathcal{E}(A) = \Pr[\text{Forge}] \leq \Pr[\text{Bad}] + \Pr[\text{Forge} | \text{Bad}],$$

where

$$\Pr[\text{Forge} | \text{Bad}] \leq q_d/(2^n - q - \sigma).$$

In addition,

$$\Pr[\text{Bad}] = \Pr[\text{Bad}_{\text{AE}}] + \Pr[\text{Bad}_{\text{BC}}] + \Pr[\text{Bad}_{\text{BCe}}] + \Pr[\text{Bad}_{\text{BCd}}],$$

and

$$\Pr[\text{Bad}_{\text{BCe}} \cup (\text{Bad}_{\text{BCd}} \cap \text{Bad}_{\text{AE}})] \leq \Pr[\text{MCol}] + \Pr[\text{Bad}_{\text{BCe}} \cup (\text{Bad}_{\text{BCd}} \cap \text{Bad}_{\text{AE}}) | \text{MCol}].$$

Thus,

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

This completes the proof. $\Box$

6. Conclusion

The privacy and authenticity of Lae0 have been analyzed in the ideal cipher model. The analysis implies that, for both privacy and authenticity, the instantiation of 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. Kniežević, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, “spongeDR: 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, keccak.noekeon.org.
His research interests are in 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).