PAPER Special Section on Cryptography and Information Security

Security Evaluation of Initialization Phases and Round Functions of Rocca and AEGIS

Nobuyuki TAKEUCHI[†a)], *Nonmember*, Kosei SAKAMOTO[††], *and* Takanori ISOBE[†,††,†††,††††], *Members*

SUMMARY Authenticated-Encryption with Associated-Data (AEAD) plays an important role in guaranteeing confidentiality, integrity, and authenticity in network communications. To meet the requirements of high-performance applications, several AEADs make use of AES New Instructions (AES-NI), which can conduct operations of AES encryption and decryption dramatically fast by hardware accelerations. At SAC 2013, Wu and Preneel proposed an AES-based AEAD scheme called AEGIS-128/128L/256, to achieve high-speed software implementation. At FSE 2016, Jean and Nikolić generalized the construction of AEGIS and proposed more efficient round functions. At ToSC 2021, Sakamoto et al. further improved the constructions of Jean and Nikolić, and proposed an AEAD scheme called Rocca for beyond 5G. In this study, we first evaluate the security of the initialization phases of Rocca and AEGIS family against differential and integral attacks using MILP (Mixed Integer Linear Programming) tools. Specifically, according to the evaluation based on the lower bounds for the number of active S-boxes, the initialization phases of AEGIS-128/128L/256 are secure against differential attacks after 4/3/6 rounds, respectively. Regarding integral attacks, we present the integral distinguisher on 6 rounds and 6/5/7 rounds in the initialization phases of Rocca and AEGIS-128/128L/256, respectively. Besides, we evaluate the round function of Rocca and those of Jean and Nikolić as cryptographic permutations against differential, impossible differential, and integral attacks. Our results indicate that, for differential attacks, the growth rate of increasing the number of active S-boxes in Rocca is faster than those of Jean and Nikolić. For impossible differential and integral attacks, we show that the round function of Rocca achieves the sufficient level of the security against these attacks in smaller number of rounds than those of Jean and Nikolić.
key words: *AEAD, round function, active S-box, impossible differential attack, integral attack, MILP*

1. Introduction

1.1 Background

To construct secure network communications, it is essential to guarantee not only confidentiality but also integrity and authenticity. Authenticated-Encryption with Associated-Data (AEAD) is one approach to providing these capabilities simultaneously using a single cryptographic algorithm.

Manuscript received March 15, 2022.
Manuscript revised June 14, 2022.
Manuscript publicized November 9, 2022.
[†]The authors are with the Graduate School of Information Science, University of Hyogo, Kobe-shi, 650-0047 Japan.
[††]The authors are with the Graduate School of Applied Informatics, University of Hyogo, Kobe-shi, 650-0047 Japan.
[†††]The author is with National Institute of Information and Communications Technology, Koganei-shi, 184-8795 Japan.
[††††]The author is with PRESTO, Japan Science and Technology Agency, Kawaguchi-shi, 332-0012 Japan.
a) E-mail: nobuyuki.takeuchi0722@gmail.com
DOI: 10.1587/transfun.2022CIP0013

At SAC 2013, Wu and Preneel proposed an efficient AES-based AEAD scheme called AEGIS-128/128L/256 to achieve high throughput on software [19]. To maximize performance, the family of AEGIS makes use of the AES New Instructions (AES-NI), which provide a special instruction set of Single Instruction Multiple Data (SIMD). The AEGIS family was submitted to CAESAR competition [1], and AEGIS-128 was chosen the final portfolio of high-performance applications. At FSE 2016, Jean and Nikolić generalized the AEGIS-like round function and proposed more efficient round functions than those of AEGIS family. Later, at ToSC 2021, Sakamoto et al. further optimized the constructions of Jean and Nikolić, proposing Rocca for beyond 5G systems [16].

Minaud showed that there exists a linear bias in the keystream [14], and AEGIS-256 was insecure against this statistical attack. After that, this linear attack was improved by Eichlseder et al. [8]. Note that these are security evaluations on encryption phases on AEGIS family. As a evaluation on the initialization process on AEGIS, Liu et al. showed distinguishing and key recovery attacks by exploiting some algebraic properties in a class of weak keys [13]. As far as we know, there is no detailed evaluation on initialization phases of AEGIS against differential and integral attacks as even designer of AEGIS did not perform the security evaluation of these attacks in the initialization phase. Regarding Rocca, designers evaluated its security against only differential attacks in the initialization phase and concluded that more than 6 rounds were secure against this attack [16]. Additionally, Jean and Nikolić evaluated only the security of round functions against differential forgery attacks in their encryption phases [10].

1.2 Our Contribution

In this study, we perform the detailed security evaluations on the initialization phases of Rocca and AEGIS-128/128L/256, and round functions of Rocca and ones of Jean and Nikolić MILP (Mixed Integer Linear Programming)-aided security evaluation method [15], [17], [20]. A summary of our results is shown in Table 1. Our contributions are summarized as follows:

1. For the first time, the initialization phases of AEGIS-128/128L/256 are found to be secure against differential attacks after 4/3/6 rounds, respectively, according to an evaluation based on the lower bounds for the number of active S-boxes. Regarding integral attacks, we

Table 1 Summary of security evaluations against attack types.

Evaluation methods	Our target	Security level	Required rounds to guarantee security		
			Differential	Integral	Impossible differential
Initialization phase	AEGIS-128 [19]	128-bit	4/10	7/10	-
	AEGIS-128L [19]		3/10	6/10	-
	AEGIS-256 [19]	256-bit	6/16	8/16	-
	Rocca [16]		6/20 [16].	7/20	-
Permutation	Jean and Nicolić-1 [10]	-	-	13	26
	Jean and Nicolić-2 [10]	-	-	15	32
	Jean and Nicolić-3 [10]	-	-	19	48
	Rocca [16]	-	-	10	14

present integral distinguishers on 6 rounds and 6/5/7 rounds in the initialization phases of Rocca and AEGIS-128/128L/256, respectively. These are the first result on integral properties of initialization phases of Rocca and AEGIS-128/128L/256.

2. We evaluate the security of the round functions of Rocca and those of Jean and Nikolić against differential, impossible differential, and integral attacks in cases where the round functions are utilized as cryptographic permutations. As a result, for differential attacks, the growth rate of increasing the number of active S-boxes in Rocca is significantly faster than those of Jean and Nikolić. For impossible differential and integral attacks, Rocca achieves the sufficient level of the security against these attacks in a smaller number of rounds than those of Jean and Nikolić.

1.3 Organization

This paper is organized as follows. We first describe each attack type and their security evaluations using an MILP in Sect. 2. In Sect. 3, we describe AEGIS-128/128L/256, round functions of Jean and Nikolić, and Rocca to clarify the scope of our evaluation. In Sect. 4, we explain the specific security evaluation methods for each construction described in Sect. 3. We show the security evaluation results of each construction in Sect. 5 and provide our interpretations in Sect. 6. Finally, Sect. 7 concludes this paper.

2. Preliminaries

This section describes differential, impossible differential, and integral attacks. Subsequently, we describe the security evaluation method using an MILP.

2.1 Differential Attacks

The differential attack [6] is the most popular cryptanalysis tool that targets block ciphers. To evaluate the cipher's resistance against differential attacks, we evaluate its differential probability DP_{f_b}. Then, we calculate its maximum differential probability $DP_{f_b max}$ from DP_{f_b}. Let f_b, Δx, and Δy represent the b-bit block cipher, differences of plaintext, and differences of ciphertext, respectively. DP_{f_b} is defined as follows:

$$DP_{f_b}(\Delta x, \Delta y) = \frac{\#\{x \in \{0,1\}^b \,|\, f_b(x) \oplus f_b(x \oplus \Delta x) = \Delta y\}}{2^b},$$

If b is small, calculating $DP_{f_b max}$ is feasible. However, this is not the case for ciphers having more than a 64-bit block. Therefore, the maximum differential characteristic probability $DCP_{f_b max}$ is used to approximate $DP_{f_b max}$. $DCP_{f_b max}$ is defined as a product of the differential characteristic probability DCP_{f_b} for each round as follows:

$$DCP_{f_b} = \prod_{R=1}^{r} DP_{f_b}(\Delta x_R, \Delta x_{R+1}),$$

$$DCP_{f_b max} = \max_{\substack{\Delta x_1 \neq 0 \\ \Delta x_2, \ldots, \Delta x_{r+1}}} DCP_{f_b},$$

where r is the number of rounds. To obtain $DCP_{f_b max}$ for a block cipher that has an S-box as its only nonlinear layer, we calculate the lower bound for the number of differentially active S-boxes. A differentially active S-box is one whose input has a non-zero difference. $DCP_{f_b max}$ is always bounded below $(DP_{smax})^{AS_{lbD}}$ [12], where DP_{smax} and AS_{lbD} denote the maximum differential probability of the S-box and the lower bound for the number of differentially active S-boxes, respectively. Therefore, we can obtain the upper bound for $DCP_{f_b max}$ by calculating the lower bound for the number of differentially active S-boxes.

2.2 Impossible Differential Attacks

The impossible differential attack [5] is one of the most powerful attacks against block ciphers based on GFN. Differential attacks exploit a pair of input-output differences denoted by Δ_{in} and Δ_{out} such that Δ_{in} can reach Δ_{out} with a high probability. In contrast, impossible differential attacks exploit a pair of Δ_{in} and Δ_{out} such that Δ_{in} cannot reach Δ_{out} after several rounds. Such differences are called the impossible differential distinguisher and are exploited to mount an attack on the key/state recovery. To evaluate the cipher's resistance against impossible differential attacks, we search for its impossible differential distinguisher of the longest round.

2.3 Integral Attacks

The integral attack was first proposed by Daemen et al. [7]

and was formalized to the integral property by Knudsen and Wagner [11]. We define four states for a set of 2^n n-bit cells: ALL ($\mathcal{A}$) if $\forall i, j\ i \neq j \iff x_i \neq x_j$; CONSTANT ($C$) if $\forall i, j\ i \neq j \iff x_i = x_j$; BALANCE ($\mathcal{B}$) $\bigoplus_i^{2^n-1} x_i = 0$; and UNKNOWN ($\mathcal{U}$) Other. When we evaluate the resistance against integral attacks, we search for $\mathcal{B}$ at the longest round, which is exploited to mount an attack on the key/state recovery.

At EUROCRYPT 2015, Todo further generalized the integral property to the division property [18] to exploit the hidden feature between $\mathcal{A}$ and $\mathcal{B}$ states. Before we describe the division property, we define the bit-product function as follows:

Definition 1 (Bit-Product Function)**.** *For any $u \in \mathbb{F}_2^n$, let $\pi_u(x)$ be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For any $x \in \mathbb{F}_2^n$, define $\pi_u(x)$ as follows:*

$$\pi_u(x) = \prod_{i=0}^{n-1} x[i]^{u[i]}.$$

Let $\pi_{\mathbf{u}}$ be a function from $(\mathbb{F}_2^{n_0} \times \mathbb{F}_2^{n_1} \times \cdots \times \mathbb{F}_2^{n_{m-1}})$ to $\mathbb{F}_2$ for all $\mathbf{u} \in \mathbb{F}_2^n$. For any $\mathbf{u} = (u_0, u_1, \ldots, u_{m-1})$, $\mathbf{x} = (x_0, x_1, \ldots, x_{m-1})$, define $\pi_{\mathbf{u}}(\mathbf{x})$ as follows:

$$\pi_{\mathbf{u}}(\mathbf{x}) = \prod_{i=0}^{m-1} \pi_{u_i}(x_i).$$

The division property is defined as follows based on the bit-product function:

Definition 2 (Division Property)**.** *Let $\mathbb{X}$ be the multiset whose elements take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,\ldots,n_m}$, where $\mathbb{K}$ denotes a set of m-dimensional vectors whose i-th element takes zero and n_i, it fulfills the following conditions:*

$$\bigoplus_{\boldsymbol{x} \in \mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \textit{unknown if there exist } \mathbf{k} \in \mathbb{K}\ s.t.\ wt(\mathbf{u}) \geq \mathbf{k}, \\ 0 \qquad\qquad \textit{otherwise}. \end{cases}$$

$wt(\mathbf{u})$ is the Hamming weight of $\mathbf{u}$. If there exist $\mathbf{k} \in \mathbb{K}$ and $\mathbf{k'} \in \mathbb{K}$ satisfying $\mathbf{k} \geq \mathbf{k'}$ in the division property, $\mathcal{D}_{\mathbb{K}}^{n_1,\ldots,n_m}$, $\mathbf{k}$ can be removed from $\mathbb{K}$ as it is redundant.

For efficient evaluation of the division property, Xiang et al. proposed an MILP method of evaluating the division property using the division trail, which allows us to illustrate the propagation of the division property and makes the evaluation easier [20]. The division trail is defined as follows:

Definition 3 (Division Trail)**.** *Let f_r denote the round function of an iterated block cipher. Assume that the input multiset to the block cipher has the initial division property $\mathcal{D}_{\mathbf{k}}^{n,m}$, and denote the division property after the i-round propagation through f_r by $\mathcal{D}_{\mathbb{K}_i}^{n,m}$. Thus, we have the following chain of division property propagations:*

$$\{\mathbf{k}\} \stackrel{def}{=} \mathbb{K}_0 \xrightarrow{f_r} \mathbb{K}_1 \xrightarrow{f_r} \mathbb{K}_2 \xrightarrow{f_r} \cdots$$

Moreover, for any vector $\mathbf{k}_i^*$ in $\mathbb{K}_i$ $(i \geq 1)$, there must exist a vector $\mathbf{k}_{i-1}^*$ in $\mathbb{K}_{i-1}$ such that $\mathbf{k}_{i-1}^*$ can propagate to $\mathbf{k}_i^*$ by division property propagation rules. Furthermore, for $(\mathbf{k}_0, \mathbf{k}_1, \ldots, \mathbf{k}_r) \in \mathbb{K}_0 \times \mathbb{K}_1 \times \cdots \times \mathbb{K}_r$, if $\mathbf{k}_{i-1}$ can propagate to $\mathbf{k}_i$ for all $i \in \{1, 2, \ldots, r\}$, $(\mathbf{k}_0, \mathbf{k}_1, \ldots, \mathbf{k}_r)$ is an r-round division trail.

Proposition 1. *Denote the division property of input multiset to an iterated block cipher by $\mathcal{D}_{\mathbf{k}}^{n,m}$; let f_r be the round function. Denote*

$$\{\mathbf{k}\} \stackrel{def}{=} \mathbb{K}_0 \xrightarrow{f_r} \mathbb{K}_1 \xrightarrow{f_r} \mathbb{K}_2 \xrightarrow{f_r} \cdots \xrightarrow{f_r} \mathbb{K}_r$$

as the r-round division property propagation. Thus, the set of the last vectors of all r-round division trails that start with $\mathbf{k}$ is equal to $\mathbb{K}_r$.

When any vector of $\mathbb{K}_r$ derived from the division property $\mathcal{D}_{\mathbb{K}_0}$ of the input multiset is always less than or equal to "1", it means that there is no integral distinguisher at the r-round.

2.4 Security Evaluation by MILP

MILP (Mixed Integer Linear Programming) is efficient at finding variables to maximize or minimize a particular objective function based on constraints expressed by a linear inequality. An MILP is applied to various attacks and security evaluations in symmetric key cryptography. In this study, we use the Gurobi Optimizer [9] as the MILP solver.

(1) Evaluation of the lower bounds for the number of active S-boxes

To evaluate the lower bounds for the number of active S-boxes using an MILP, we use the method proposed by Mouha et al. at Inscrypt 2011 [15]. For evaluation, the method expresses all operations in a cryptographic scheme as linear inequalities and assigns them to an MILP model as constraints. Then, the total number of active S-boxes is assigned to the MILP model as the objective function. The lower bounds for the number of active S-boxes can then be obtained so that it can be minimized.

(2) Searching for the impossible differential distinguisher

We use the MILP model proposed by Sasaki et al. at EUROCRYPT 2017 [17] for the impossible differential distinguisher. In this evaluation, as with the differentially active S-box evaluation method, the differential propagation on all operations in a cryptographic scheme is expressed as linear inequalities and assigned to the MILP model as constraints. We add additional constraints to fix the input and output differences to a certain condition. Then, we apply the MILP method without an objective function to obtain the result that shows whether this model is feasible. If the result is infeasible, the pair of input and output differences fixed by constraints is an impossible difference.

(3) Searching for the integral distinguisher

We use the search method for the integral distinguisher using the MILP method proposed by Xiang et al. at ASIACRYPT 2016 [20]. We first express the propagation of the division property as linear inequalities and assign them to the MILP model as constraints. We add additional constraints to assign ALL($\mathcal{A}$) or CONSTANT(C) to the input. For the output, one output bit (byte) is assigned $\mathcal{D}_1^8$ ($\mathcal{D}_1^1$), and the remaining bits (bytes) are set to zero. Then, we solve this MILP model without an objective function. The infeasible result indicates that its input division property does not propagate to its output division property (i.e., the output bit (byte) assigned $\mathcal{D}_1^8$ ($\mathcal{D}_1^1$) is BALANCE($\mathcal{B}$)).

3. Our Targets

In this section, we provide the specifications of AEGIS-128/128L/256 and Rocca and describe the efficient round functions proposed by Jean and Nicolić. We only describe the initialization phase and round functions for AEGIS-128/128L/256 and Rocca, as the encryption phase is not involved in our evaluation. The internal state size, key size, and initialization vector/nonce size of each target are given in Table 2.

3.1 AEGIS-128/128L/256

AEGIS-128/128L/256 were proposed by Wu and Preneel at SAC 2013 [19]. AEGIS realizes high-speed software implementation on with AES-NI. AEGIS consists of four phases: initialization, processing the authenticated data, encryption, and finalization.

(1) AEGIS-128

Figure 1 shows the round function of AEGIS-128. Let K_{128}, IV_{128}, C_a, and C_b be the 128-bit key, the 128-bit initialization vector, and the two 128-bit constants in the initialization phase, respectively. K_{128}, IV_{128}, C_a, and C_b are loaded into the state S as follows:

$$\begin{aligned} &S[0] = K_{128} \oplus IV_{128}, && S[1] = C_b, \\ &S[2] = C_a, && S[3] = K_{128} \oplus C_a, \\ &S[4] = K_{128} \oplus C_b. \end{aligned}$$

The data m_r inserted in r round are expressed as follows:

$$m_{2i-1} = K_{128}, \quad m_{2i} = K_{128} \oplus IV_{128}, \quad (1 \leq i \leq 5).$$

In the initialization phase, 10 iterations of the round function shown in Fig. 1 is applied to the state S. In Fig. 1, let A be one AES round function, A(S) and A(S, K) are defined as follows:

$$\mathrm{A}(S) = \mathrm{MixColumns} \circ \mathrm{ShiftRows} \circ \mathrm{SubBytes}(S).$$
$$\mathrm{A}(S, K) = (\mathrm{MixColumns} \circ \mathrm{ShiftRows} \circ \mathrm{SubBytes}(S)) \oplus K.$$

(2) AEGIS-128L

Figure 2 shows the round function of AEGIS-128L. Let K_{128L}, IV_{128L}, C_a, and C_b be the 128-bit key, the 128-bit initialization vector, and the two 128-bit constants in the initialization phase, respectively. K_{128L}, IV_{128L}, C_a, and C_b are loaded into the internal state S as follows:

$$\begin{aligned} &S[0] = K_{128L} \oplus IV_{128L}, && S[1] = C_b, \\ &S[2] = C_a, && S[3] = C_b, \\ &S[4] = K_{128L} \oplus IV_{128L}, && S[5] = K_{128L} \oplus C_a, \\ &S[6] = K_{128L} \oplus C_b, && S[7] = K_{128L} \oplus C_a. \end{aligned}$$

The data $m_r = m_{r,a} || m_{r,b}$ inserted in r round are expressed as follows:

$$m_{r,a} = IV_{128L}, \qquad m_{r,b} = K_{128L}.$$

In the initialization phase, 10 iterations of the round function shown in Fig. 2 is applied to the internal state S.

(3) AEGIS-256

Figure 3 shows the round function of AEGIS-256. Let $K_{256} = K_{256,a} || K_{256,b}$, $IV_{256} = IV_{256,a} || IV_{256,b}$, C_a, and C_b be the 256-bit key, the 256-bit initialization vector, and the two 128-bit constants in the initialization phase, respectively. $K_{256} = K_{256,a} || K_{256,b}$, $IV_{256} = IV_{256,a} || IV_{256,b}$, C_a, and C_b are loaded into the internal state S as follows:

$$\begin{aligned} &S[0] = K_{256,a} \oplus IV_{256,a}, && S[1] = K_{256,b} \oplus IV_{256,b}, \\ &S[2] = C_b, && S[3] = C_a, \\ &S[4] = K_{256,a} \oplus C_a, && S[5] = K_{256,b} \oplus C_b. \end{aligned}$$

Table 2 Size of our targets.

Our target	Internal state	Key	IV/Nonce
AEGIS-128	640-bit	128-bit	128-bit
AEGIS-128L	1024-bit	128-bit	128-bit
AEGIS-256	768-bit	256-bit	256-bit
Jean and Nicolić-1 (Fig. 4)	896-bit	-	-
Jean and Nicolić-2 (Fig. 5)	1024-bit	-	-
Jean and Nicolić-3 (Fig. 6)	1536-bit	-	-
Rocca	1024-bit	256-bit	128-bit

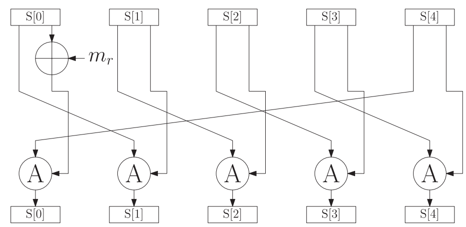


Fig. 1 Round function of AEGIS-128.

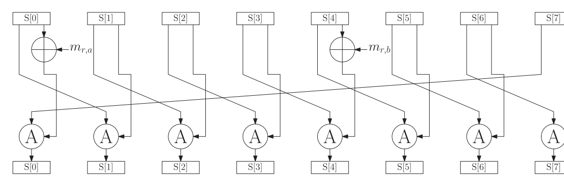


Fig. 2 Round function of AEGIS-128L.

The data m_r inserted in r round are expressed as follows:

$$m_{4i-3} = K_{256,a}, \qquad m_{4i-2} = K_{256,b},$$
$$m_{4i-1} = K_{256,a} \oplus IV_{256,a}, \qquad m_{4i} = K_{256,b} \oplus IV_{256,b},$$
$$(1 \leq i \leq 4).$$

In the initialization phase, 16 iterations of the round function shown in Fig. 3 is applied to the internal state S.

3.2 Round Functions Proposed by Jean and Nicolić

At FSE 2016, Jean and Nicolić demonstrated the construction of an efficient round function based on only the AES round function and XOR for AEAD [10]. They defined *rate* as a metric to estimate the efficiency of the round function.

Definition 4 (*Rate*)**.** *Rate is defined as the number of the AES round functions required to encrypt a 128-bit message. Thus, rate is expressed by the following equation:*

$$Rate = \frac{\#AESs}{\#messages},$$

where #AESs and #messages are the number of the AES round functions and inserted 128-bit message blocks in one round, respectively.

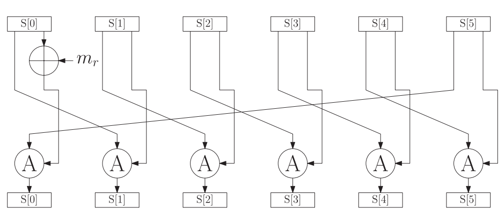


Fig. 3 Round function of AEGIS-256.

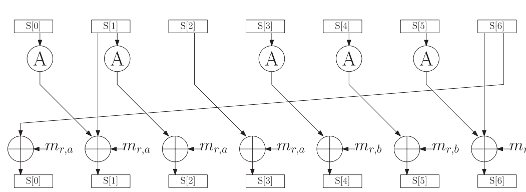


Fig. 4 Construction of Jean and Nicolić-1 ($rate$ = 2.5, $\#state$ = 7).

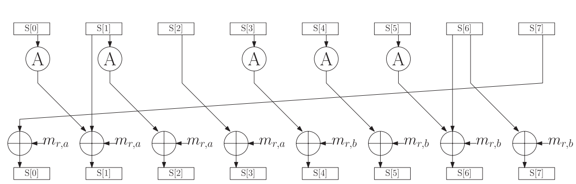


Fig. 5 Construction of Jean and Nicolić-2 ($rate$ = 2.5, $\#state$ = 8).

To achieve high-speed encryption, a round function with a smaller rate is required. In this study, we evaluate the round functions with $rate \leq 2.5$ among those presented by Jean and Nicolić. Figures 4, 5, and 6 show the round functions with $rate \leq 2.5$, as provided by Jean and Nicolić.

3.3 Rocca

At ToSC 2021, Sakamoto et al. proposed Rocca, an AEAD scheme for Beyond 5G systems [16]. To minimize the critical path of the round function, they improved the study of Jean and Nicolić by removing the case of applying both AES-NI and XOR to one internal state and presented a more efficient round function. Based on that, they proposed an AEAD named Rocca which achieves outstanding performance.

Rocca consists of four phases: initialization, processing the associated data, encryption, and finalization. Figure 7 shows the round function of Rocca. Let $K_R = K_{R,a}||K_{R,b}$, N_R, C_0, and C_1 be the 256-bit key, the 128-bit nonce, and the two 128-bit constants in the initialization phase, respectively. $K_R = K_{R,a}||K_{R,b}$, N_R, C_0, and C_1 are loaded into the internal state S as follows:

$$S[0] = K_{R,b}, \qquad S[1] = N_R,$$
$$S[2] = C_0, \qquad S[3] = C_1,$$
$$S[4] = N_R \oplus K_{R,b}, \qquad S[5] = 0,$$
$$S[6] = K_{R,a}, \qquad S[7] = 0.$$

In the initialization phase, the round constants C_0 and C_1 are loaded into $m_{r,a}$ and $m_{r,b}$ in each round, respectively. In the initialization phase, 20 iterations of the round function shown in Fig. 7 is applied to the internal state S.

4. Methods of MILP-Aided Security Evaluations

This section describes the evaluation of the security of target constructions. To evaluate the security against differential, impossible differential, and integral attacks, we search for the lower bounds for the number of active S-boxes, and find the longest impossible difference and integral distinguisher in a byte-wise, using MILP-based tools [9].

4.1 Security Evaluations in the Initialization Phase

To evaluate the security of the initialization phase, we evaluate

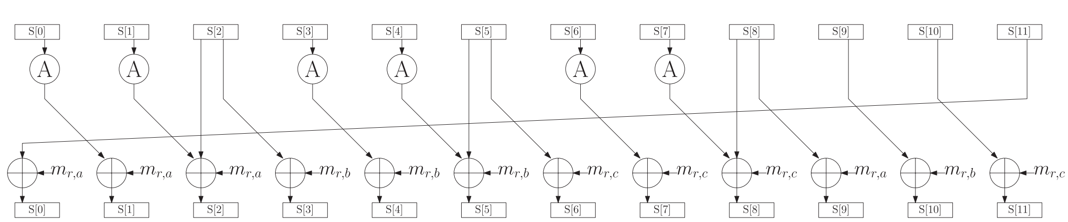


Fig. 6 Construction of Jean and Nicolić-3 ($rate$ = 2, $\#state$ = 12).

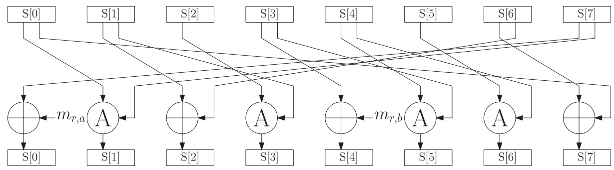


Fig. 7 Round function of Rocca.

our target against differential and integral attacks. In our evaluation, we assume that attackers can control the IV/nonce space as related-key attacks are out of scope. Regarding impossible differential attacks, because the input space that the adversary can control and the output size of the initialization phase are different, it does not make sense as the evaluation of initialization phase. Jean and Nicolić have not specify the initialization phase. Therefore, we evaluate the initialization phases of AEGIS-128/128L/256 and Rocca.

(1) Differential attacks

Since AEGIS-128/128L/256 and Rocca consist of only AES round functions and XORs, only the S-box of an AES round is a non-linear operation. As the maximum differential probability of an S-box is 2^{-6}, the lower bound for the number of active S-boxes should be larger than 22 and 43 to guarantee 128-bit and 256-bit security, respectively against differential attacks.

(2) Integral attacks

To evaluate integral attacks, we consider a specific class of input values (IV/nonce) such that any 1 byte is CONSTANT($\mathcal{C}$), and the others are ALL($\mathcal{A}$). Under this condition, we search for the longest integral distinguisher in the initialization phases of AEGIS-128/128L/256 and Rocca.

4.2 Security Evaluation in the Permutation Based on the Round Function

Next, we consider the security of the round functions of our targets in the case where these are utilized as underlying round functions of cryptographic permutations. Specifically, we evaluate the security against differential attacks, impossible differential attacks, and integral attacks. In this evaluation, we assume that the attackers can control the input states space unlike the case of initialization phase evaluations. Note that the round function of AEGIS-128/128L/256 is not bijective as IV is inserted into the middle round in the initialization phase in the feedforward manner. Therefore, we evaluate the security of permutations based on the round function of Jean and Nicolić (Figs. 4, 5, and 6) and Rocca.

(1) Differential attacks

As with the security evaluation of the initialization phase, we search for the lower bounds for the number of active S-boxes for each construction.

(2) Impossible differential attacks

As with the search space, we consider the case where 1 byte of each input/output space is active, and the other bytes are inactive. This is a common method to find the longest impossible differences as it generally takes the most number of rounds to achieve full diffusion when the output or input has only one active bit/word. Some block cipher designers have used this method to evaluate their designs [2]–[4]. Under this condition, we search for the longest impossible differential distinguisher for each construction.

(3) Integral attacks

We consider the input patterns such that any 1 byte is CONSTANT($\mathcal{C}$), and the other bytes are ALL($\mathcal{A}$) to avoid finding the trivial BALANCE($\mathcal{B}$) as our targets are permutations. Under this condition, we search for the longest integral distinguisher for each construction.

5. Results

This section describes the results of our security evaluation explained in Sect. 4 for each construction.

5.1 Initialization Phase

Tables 3 and 4 shows the lower bounds for the number of active S-boxes for each round and the maximum rounds of the integral distinguisher, respectively.

(1) AEGIS-128/128L/256

As AEGIS-128/128L/256 claims 128/128/256-bit security, respectively [19], the lower bounds for the number of active S-boxes should be 22/22/43 or more in the initialization phase to be secure against differential attacks under the active S-box evaluations. According to Table 3, the required number of rounds is estimated as 4/3/6 rounds against differential attacks, respectively. According to Table 4, the required number of rounds is estimated as 7/6/8 rounds against integral attacks, respectively. Tables 5, 6, and 7 show examples of the division property of these distinguisher in the maximum round. In these tables, we show the number of active bits in each input byte and give the position of the balanced byte by B and the unknown byte by U, and each byte is labeled as $0, 1, \ldots, (N/8 - 1)$ from left to right, where N denotes the internal state size of each target.

(2) Rocca

As Rocca claims 256-bit security [16]. the lower bound for the number of active S-boxes should be 43 or more in the initialization phase to be secure against differential attacks. According to Tables 3 and 4, the required number of rounds is estimated as 6/7 rounds against differential/integral attacks, respectively. Table 8 shows an example of the division property of the distinguisher in the maximum round.

5.2 Cryptographic Permutation

Tables 9 and 10 shows the lower bounds for the number of active S-boxes in each round and the longest impossible

Table 3 The lower bound for the number of active S-boxes in the initialization phase.

our target	security level	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R
AEGIS-128	128-bit	1	6	13	**31**	41	51	62	70	78	83
AEGIS-128L		2	11	**30**	62	74	85	86	94	111	120
AEGIS-256	256-bit	1	6	17	31	36	**44**	65	77	87	101
Rocca		1	6	9	30	38	**54**	62	82	85	93

Table 4 Maximum rounds of the integral distinguisher in the initialization phase.

Our target	Rounds	Data
AEGIS-128	6/10	2^{127}
AEGIS-128L	5/10	2^{127}
AEGIS-256	7/16	2^{255}
Rocca	6/20	2^{127}

Table 5 Division property of 6-round distinguisher in AEGIS-128.

IV	78888888 88888888
S[0]	UUUUUUUU UUUUUUUU
S[1]	UUUUUUUU UUUUUUUU
S[2]	BBBBBBBB BBBBBBBB
S[3]	UUUUUUUU UUUUUUUU
S[4]	UUUUUUUU UUUUUUUU

Table 6 Division property of 5-round distinguisher in AEGIS-128L.

IV	78888888 88888888
S[0]	UUUUUUUU UUUUUUUU
S[1]	UUUUUUUU UUUUUUUU
S[2]	BBBBBBBB BBBBBBBB
S[3]	UUUUUUUU UUUUUUUU
S[4]	UUUUUUUU UUUUUUUU
S[5]	UUUUUUUU UUUUUUUU
S[6]	BBBBBBBB BBBBBBBB
S[7]	UUUUUUUU UUUUUUUU

Table 7 Division property of 7-round distinguisher in AEGIS-256.

IV	78888888 88888888
S[0]	UUUUUUUU UUUUUUUU
S[1]	UUUUUUUU UUUUUUUU
S[2]	BBBBBBBB BBBBBBBB
S[3]	BBBBBBBB BBBBBBBB
S[4]	UUUUUUUU UUUUUUUU
S[5]	UUUUUUUU UUUUUUUU

differences and integral distinguishers for each construction, respectively.

(1) Round functions proposed by Jean and Nicolić

According to Table 9, the round function shown in Fig. 4 has the best property regarding the lower bound for the number of active S-boxes among the three round functions shown in Figures 4, 5, and 6. According to Table 10, the round function shown in Figure 6 has the best property regarding resistance against both impossible differential and integral attacks.

Table 8 Division property of 6-round distinguisher in Rocca.

IV	78888888 88888888
S[0]	BBBBBBBB BBBBBBBB
S[1]	BBBBBBBB BBBBBBBB
S[2]	UUUUUUUU UUUUUUUU
S[3]	UUUUUUUU UUUUUUUU
S[4]	BBBBBBBB BBBBBBBB
S[5]	UUUUUUUU UUUUUUUU
S[6]	UUUUUUUU UUUUUUUU
S[7]	UUUUUUUU UUUUUUUU

(2) Rocca

According to Table 9, Rocca does not have as good a property regarding the lower bound for the number of active S-boxes under 6 rounds. However, the growth of the number of active S-boxes is faster after 7 rounds than that of the three round functions proposed by Jean and Nicolić, and Rocca has the most number of active S-boxes after 8 rounds among our targets, apart from 12 rounds. According to Table 10, Rocca has the best property among our targets regarding resistance against both impossible differential and integral attacks.

6. Discussion

In this section, we compare our targets in terms of the security and efficiency. For a fair comparison, we consider *the number of AES round calls to achieve the required level of the security*, based on the results of the security evaluation shown in Sect. 5, as the performance highly depends on the number of AES round calls, as already discussed in [10], [16].

Table 11 shows the required number of AES round calls needed to guarantee the security for each attack. Note that for the cryptographic permutation, we only consider integral and impossible differential attacks, because the round functions that we evaluate do not claim any security as a cryptographic permutation (i.e., it is not clear how many active S-boxes are necessary to achieve the security goals). In contrast, for integral and impossible differential attacks, it is possible to find these characteristics independently from the claimed security. Thus, for the permutation evaluations, we focus on the required number of rounds in which there is no byte-wise integral/impossible differential characteristics.

6.1 Initialization Phase

(1) Comparison based on the required number of rounds

According to Table 1 for differential attacks, AEGIS-128L

Table 9 The lower bound for the number of active S-boxes in the permutation based on the round function.

Our target	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R	11R	12R
Jean and Nicolić-1	0	1	5	7	9	25	30	31	36	53	60	75
Jean and Nicolić-2	0	0	1	5	7	9	25	27	31	35	40	53
Jean and Nicolić-3	0	0	0	0	1	5	9	15	30	35	40	45
Rocca	0	0	2	6	11	18	26	39	44	53	61	70

Table 10 Longest rounds of the impossible differential distinguisher and the integral distinguisher in the permutation based on the round function.

Our target	Impossible differential distinguisher	Integral distinguisher	
	Rounds	Rounds	Data
Jean and Nicolić-1	25	12	2^{895}
Jean and Nicolić-2	31	14	2^{1023}
Jean and Nicolić-3	47	18	2^{1535}
Rocca	13	9	2^{1023}

Table 11 The Number of AES calls required to be secure against each attack.

Evaluation methods	Our target	Security level	#AES/1 round	Required number of AES calls		
				Differential attacks	Integral attacks	Impossible Differential attacks
Initialization phase	AEGIS-128	128-bit	5	**20**	**35**	-
	AEGIS-128L		8	24	48	-
	AEGIS-256	256-bit	6	36	48	-
	Rocca		4	**24**	**28**	-
Permutation	Jean and Nicolić-1	-	5	-	65	130
	Jean and Nicolić-2	-	5	-	75	160
	Jean and Nicolić-3	-	6	-	114	288
	Rocca	-	4	-	**40**	**56**

achieves 128-bit security at the smaller number of rounds than AEGIS-128, and Rocca and AEGIS-256 achieve 256-bit security at the same number of rounds. For integral attacks, AEGIS-128L and Rocca achieve the required security in the smaller number of rounds than AEGIS-128 and AEGIS-256, respectively.

(2) Comparison based on the number of the AES round calls

In terms of the number of AES round calls, Rocca achieves the required security against both impossible differential and integral attacks with the smallest number of AES round function calls. Notably, for differential attacks, Rocca achieves its claimed security with the same number of the AES round calls as that of AEGIS-128L, although Rocca claims stronger security than AEGIS-128L.

6.2 Cryptographic Permutation

(1) Comparison based on the number of rounds

Rocca guarantees the security against integral and impossible differential attacks at smallest numbers of rounds among target schemes. Particularly for impossible differences, Rocca achieves the security at almost half that of the round function shown in Fig. 4.

(2) Comparison based on the number of the AES round calls

Rocca achieves the required security against both impossible differential and integral attacks by much smallest number of AES round function calls. Notably, for impossible differential attacks, Rocca requires only 56 AES round calls, whereas the round functions shown in Figs. 4, 5, and 6 need many more AES calls to guarantee the same security: 130, 160, and 288, respectively.

7. Conclusion

In this study, we first evaluated the security of the initialization phases of Rocca and AEGIS family against differential attacks and integral attacks using MILP (Mixed Integer Linear Programming) tools. Specifically, we revealed that the initialization phases of AEGIS-128/128L/256 were secure against differential attacks after 4/3/6 rounds, respectively, by the evaluation based on the lower bounds for the number of active S-boxes. Regarding integral attacks, we presented integral distinguisher on 6 rounds and 6/5/7 rounds in the initialization phases of Rocca and AEGIS-128/128L/256, respectively. Besides, we evaluated the round function of Rocca and those of Jean and Nikolić as cryptographic permutations against differential, impossible differential, and integral attacks. Our results indicated that, for differential attacks, the growth rate of increasing the number of active

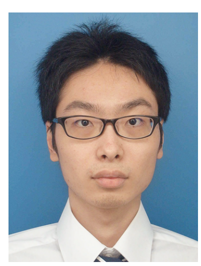
S-boxes in Rocca is faster than those of Jean and Nikolić. For impossible differential and integral attacks, we showed that the round function of Rocca achieves the sufficient level of the security against these attacks in smaller number of rounds than those of Jean and Nikolić. Moreover, among our targets, we showed that Rocca achieves a sufficient level of security with the smallest number of the AES round calls.

Acknowledgments

Takanori Isobe is supported by JST, PRESTO Grant Number JPMJPR2031, Grant-in-Aid for Scientific Research (B) (KAKENHI 19H02141). Kosei Sakamoto is supported by Grant-in-Aid for JSPS Fellows (KAKENHI 20J23526) for Japan Society for the Promotion of Science. This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[1] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, https://competitions.cr.yp.to/caesar.html, 2018.
[2] S. Banik, Z. Bao, T. Isobe, H. Kubo, F. Liu, K. Minematsu, K. Sakamoto, N. Shibata, and M. Shigeri, "WARP: Revisiting GFN for lightweight 128-bit block cipher," SAC, volume 12804 of Lecture Notes in Computer Science, pp.535–564, Springer, 2020.
[3] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy," ASIACRYPT (2), volume 9453 of Lecture Notes in Computer Science, pp.411–436, Springer, 2015.
[4] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S.M. Sim, "The SKINNY family of block ciphers and its low-latency variant MANTIS," CRYPTO (2), volume 9815 of Lecture Notes in Computer Science, pp.123–153, Springer, 2016.
[5] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," EUROCRYPT, volume 1592 of Lecture Notes in Computer Science, pp.12–23, Springer, 1999.
[6] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," J. Cryptol., vol.4, no.1:3, pp.3–72, 1991.
[7] J. Daemen, L.R. Knudsen, and V. Rijmen, "The block cipher square," FSE, volume 1267 of Lecture Notes in Computer Science, pp.149–165, Springer, 1997.
[8] M. Eichlseder, M. Nageler, and R. Primas, "Analyzing the linear keystream biases in AEGIS," IACR Trans. Symmetric Cryptol., vol.2019, no.4, pp.348–368, 2019.
[9] Gurobi Optimization Inc., Gurobi optimizer 6.5. Official webpage, http://www.gurobi.com/, 2015.
[10] J. Jean and I. Nikolic, "Efficient design strategies based on the AES round function," FSE, volume 9783 of Lecture Notes in Computer Science, pp.334–353, Springer, 2016.
[11] L.R. Knudsen and D.A. Wagner, "Integral cryptanalysis," FSE, volume 2365 of Lecture Notes in Computer Science, pp.112–127, Springer, 2002.
[12] X. Lai, J.L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," EUROCRYPT, volume 547 of Lecture Notes in Computer Science, pp.17–38. Springer, 1991.
[13] F. Liu, T. Isobe, W. Meier, and K. Sakamoto, "Weak keys in reduced AEGIS and tiaoxin," IACR Cryptol. ePrint Arch., page 187, 2021.
[14] B. Minaud, "Linear biases in AEGIS keystream," Selected Areas in Cryptography - SAC 2014 - 21st International Conference, A. Joux and A.M. Youssef, eds., Montreal, QC, Canada, Aug. 2014, Revised Selected Papers, volume 8781 of Lecture Notes in Computer Science, pp.290–305, Springer, 2014.
[15] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," Inscrypt, volume 7537 of Lecture Notes in Computer Science, pp.57–76, Springer, 2011.
[16] K. Sakamoto, F. Liu, Y. Nakano, S. Kiyomoto, and T. Isobe, "Rocca: An efficient aes-based encryption scheme for beyond 5G," IACR Trans. Symmetric Cryptol., vol.2021, no.2, pp.1–30, 2021.
[17] Y. Sasaki and Y. Todo, "New impossible differential search tool from design and cryptanalysis aspects: Revealing structural properties of several ciphers," EUROCRYPT (3), volume 10212 of Lecture Notes in Computer Science, pp.185–215, 2017.
[18] Y. Todo, "Structural evaluation by generalized integral property," EUROCRYPT (1), volume 9056 of Lecture Notes in Computer Science, pp.287–314, Springer, 2015.
[19] H. Wu and B. Preneel, "AEGIS: A fast authenticated encryption algorithm," Selected Areas in Cryptography, volume 8282 of Lecture Notes in Computer Science, pp.185–201, Springer, 2013.
[20] Z. Xiang, W. Zhang, Z. Bao, and D. Lin, "Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers," ASIACRYPT (1), volume 10031 of Lecture Notes in Computer Science, pp.648–678, 2016.



Nobuyuki Takeuchi received the B.E. degree from University of Hyogo, Japan, in 2021. He is currently a M.E. student at University of Hyogo, Japan. His research interest is cryptography.

Kosei Sakamoto received the B.E. degree from Kansai University, Japan, in 2017. In 2020, he received the M.E. degree from University of Hyogo. He is currently a Ph.D. student at University of Hyogo, Japan. His research interest is cryptography.

Takanori Isobe received the B.E., M.E., and Ph.D. degrees from Kobe University, Japan, in 2006, 2008, and 2013, respectively. From 2008 to 2017, he worked at the Sony Corporation. Since 2017, he has been an Associate Professor at University of Hyogo. His current research interests include information security and cryptography.