Research Article

Permutation-Based Lightweight Authenticated Cipher with Beyond Conventional Security

Ping Zhang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Correspondence should be addressed to Ping Zhang; zhgp@njupt.edu.cn

Received 8 July 2021; Revised 27 September 2021; Accepted 6 October 2021; Published 27 October 2021

Academic Editor: Huaxiong Wang

Copyright © 2021 Ping Zhang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Lightweight authenticated ciphers are specially designed as authenticated encryption (AE) schemes for resource-constrained devices. Permutation-based lightweight authenticated ciphers have gained more attention in recent years. However, almost all of permutation-based lightweight AE schemes only ensure conventional security, i.e., about \( \frac{c}{2} \)-bit security, where \( c \) is the capacity of the permutation. This may be vulnerable for an insufficiently large capacity. This paper focuses on the stronger security guarantee and the better efficiency optimization of permutation-based lightweight AE schemes. On the basis of APE series (APE, APERI, APEOW, and APECA), we propose a new improved permutation-based lightweight online AE mode APE* which supports beyond conventional security and concurrent absorption. Then, we derive a simple security proof and prove that APE* enjoys at most about \( \min(r,c) \)-bit security, where \( r \) is the rate of the permutation. Finally, we discuss the properties of APE* on the hardware implementation.

1. Introduction

With the widespread rise of the big data, Internet of Things (IoT), and fifth generation (5G) and beyond 5G (B5G) networks, leaks of sensitive data from wireless sensor devices and network platforms have become more serious and more common. The collection of sensitive data has become one of the important targets of cyberattacks by hackers. How can we protect the security of our sensitive data? Cryptography is an important method to protect the security of sensitive data.

Lightweight cryptography focuses on the symmetric-key cryptography, whose goal is to settle the data security of resource-constrained devices in the embedded systems, sensor networks, RFID, and low-cost environments. The feature of the lightweight cryptography is that the implementation costs of hardware devices (such as areas, footprints, latency, and throughput) are as low as possible and the implementation efficiency (rate) is as high as possible, without sacrificing security guarantee.

The research of the lightweight cryptography began in 2004 and has been going on for more than a decade. The lightweight cryptography mainly includes the lightweight cipher and its modes of operation. Lightweight ciphers are designed to protect the privacy (confidentiality) of sensitive data on lightweight devices. Up to now, a large number of lightweight ciphers have been proposed, analyzed, and implemented [1–9]. Lightweight authenticated encryption (AE) modes of operation, also called lightweight authenticated ciphers, achieve both the privacy protection of sensitive data and the integrity verification of all data on lightweight devices. Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) held in 2013 greatly contributed to the vigorous development of lightweight AE modes and produced many excellent schemes, such as Ascon [10] and ACORN [10]. From the perspective of the design method, lightweight AE modes include block-cipher-based lightweight AE modes [11–14], stream-cipher-based lightweight AE modes [15, 16], permutation-based lightweight AE modes [17–20], and hash-based lightweight AE modes [19, 20]. Moreover, permutation-based lightweight AE modes have more advantages and attractions than others due to its simple structure, convenient lookup table, and fast running speed.
Authenticated permutation-based encryption (APE) is the first permutation-based lightweight AE mode with nonce-misuse resistance designed by Andreeva et al. [17]. The idea is inspired from Sponge. The encryption algorithm of APE is online (i.e., the $i$-th block of ciphertext only depends on the first $i$ blocks of plaintext), while the decryption algorithm is inverse-online (i.e., the online decryption of the ciphertext blocks is in reverse order). APE is proven up to the conventional security under the random permutation model (RPM), i.e., APE guarantees at most about $c/2$-bit security, where $c$ is the capacity of the permutation.

However, there exist several drawbacks for APE, such as relatively big bandwidth, large hardware footprint, and high computational complexity. To overcome these drawbacks of APE, Sasaki and Yasuda focused on the implementation costs and the proper usage of a nonce on resource-constrained devices [18]. On the basis of APE, they described three new online permutation-based lightweight AE modes, called APE$_{RI}$, APE$_{OW}$, and APE$_{CA}$, to meet the requirements of less bandwidths, smaller hardware footprints, and lower computational complexity. They proved that these three lightweight AE schemes also enjoy the conventional security.

Almost all of the previous permutation-based weight AE schemes, including APE, APE$_{RI}$, APE$_{OW}$, and APE$_{CA}$, only ensure at most about $c/2$-bit security. To ensure enough security, one tends to choose a permutation with a big capacity $c$. Table 1 shows security levels of some permutation-based AE modes using recommended parameters.

However, in some special environments, such as an insufficiently large capacity of the permutation or the partial information leakage of permutation by side channel attacks, this security bound is not enough. Moreover, the associated data and the message were handled separately in APE, APE$_{RI}$, APE$_{OW}$, and APE$_{CA}$, which is not highly efficient. Whether can we construct an efficient lightweight AE mode with beyond $c/2$-bit security?

This paper is devoted to solving the above problem and gives a positive response. On the basis of the current APE, APE$_{RI}$, APE$_{OW}$, and APE$_{CA}$, we propose a novel improved permutation-based lightweight online AE mode APE$^+$. APE$^+$ supports strong security guarantee and high efficiency implementation. The concrete contributions include the following:

1. In order to achieve higher efficiency, we consider to put some good factors into APE$^+$, such as inverse-free, stream-cipher encryption, concurrent absorption, and pure permutation. APE$^+$ is inverse-free, i.e., the decryption algorithm of APE$^+$ does not invoke the inverse of permutation. Besides, it is a stream-cipher encryption mode. For the associated data and the message, APE$^+$ utilizes the method of concurrent absorption to process them, which makes the number of invoking the underlying permutation as few as possible. In particular, in view of the performance of APE$^+$ on the hardware implementation, APE$^+$ is built by the cascade method and has no backward feedback. Therefore, it can be fully pipeline implemented on the hardware. Moreover, APE$^+$ just requires the forward permutation circuit for the encryption and decryption circuits. Therefore, the area of the hardware device and the number of the hardware footprints are minimized. APE$^+$ utilizes the concurrent absorption method, which greatly reduces the computational complexity on the hardware devices.

2. In order to achieve stronger security, the encryption and authentication parts are considered separately. For the encryption part, we utilize the iterated Even–Mansour cipher with a short key [21] to generate the ciphertext while avoiding the defeat that the current plaintext is XOR-ed with the previous ciphertext. For the authentication part, the authentication tag is generated by the XOR of the rate and the capacity of the last permutation to resist forgery attacks. In this paper, we derive a simple security proof by using a modular proof approach and prove that APE$^+$ enjoys at most about $\min[r,c]$-bit AE security under the RPM assumption, where $r$ and $c$ are, respectively, the rate and the capacity of the permutation. Specifically, given a permutation with parameters $b = 256$, $r = 96$, and $c = 160$ (or $b = 256$, $r = 128$, and $c = 128$), APE$^+$ enjoys at most about 96-bit (or 128-bit) AE security, which is shown in Table 1.

The rest of this paper is organized as follows. Notations and some preliminaries are presented in Section 2. Section 3 describes the security model of lightweight AE schemes. Section 4 provides a new permutation-based lightweight AE mode with beyond conventional security and derives a security proof. Section 5 shows some discussions for APE$^+$. Finally, Section 6 ends up with a conclusion.

### 2. Preliminaries

**Notations.** Let $\{0,1\}$ denote the set containing all finite bit strings (including the empty string). Let $b$ be an integer and $\{0,1\}^b$ be the set of all strings whose lengths are $b$ bits. For a finite string $x$, $|x|$ stands for its bit-length.
Strong Pseudorandom Permutation (SPRP). One of the most important security concepts in symmetric ciphers is SPRP. What is SPRP? In a nutshell, if a symmetric cipher is indistinguishable from an ideal random permutation under chosen ciphertext attacks, then this symmetric cipher is an SPRP. The detailed definition is shown as follows.

Let \( E: \mathcal{K} \times \{0,1\}^b \rightarrow \{0,1\}^b \) be a symmetric cipher, where \( \mathcal{K} \) is a nonempty key set. Then, for any \( K \in \mathcal{K} \), \( E_K(\cdot) \) is a permutation on \( b \) bits and \( E_K^{-1}(\cdot) \) is the inverse of \( E_K(\cdot) \). Let \( Perm(b) \) be the set of all permutations on \( b \) bits. Let \( P \) be a primitive utilized in \( E \). Let \( \mathcal{A} \) be an adversary with access to encryption, decryption, and the primitive and its inverse oracles, i.e., \( (E_K^E, P^E) \). Let \( \mathcal{A}^{Perm=1} \) be the event that an adversary \( \mathcal{A} \) outputs 1 after interacting with the oracle \( O \).

Let \( K \in \mathcal{K} \), \( \pi = \text{Perm}(b) \), then the SPRP advantage of \( \mathcal{A} \) against \( E \) is defined as

\[
\text{Adv}^{\text{SPRP}}_{\mathcal{A}}(E) = \left| \Pr[\mathcal{A}^{E_K^E \cdot \pi^E \cdot E_K^{-1} \cdot \pi^{-1} \cdot E_K \cdot E_K^{-1}} = 1] - \Pr[\mathcal{A}^{\pi^E \cdot E_K \cdot E_K^{-1} \cdot \pi^{-1} \cdot E_K \cdot E_K^{-1}} = 1] \right|
\]  

(1)

If the advantage \( \text{Adv}^{\text{SPRP}}_{\mathcal{A}}(E) \) is negligible, the cipher \( E_K \) is a secure strong pseudorandom permutation (SPRP).

If the resources (such as the overall running time \( t \), the number of querying the encryption and decryption oracles \( q \), the total query complexity of the construction \( \sigma \), and the number of querying the primitive and its inverse oracles \( p \) ) used by adversaries are limited, we define the maximum advantage as

\[
\text{Adv}^{\text{SPRP}}(E) = \max_{\mathcal{A}} \text{Adv}^{\text{SPRP}}_{\mathcal{A}}(E).
\]  

(2)

Even–Mansour Cipher with a Short Key [21]. Let \( P \) be a public random \( b \)-bit permutation, \( c \) be the capacity of \( P \), \( r \) be the rate of \( P \), and \( b = r + c \). Let \( \mathcal{K} = \{0,1\}^k \) be a \( k \)-bit key set. To minimize the key material of the Even–Mansour cipher and achieve beyond conventional security bound, the Even–Mansour cipher with a short key is presented. The Even–Mansour cipher with a short key is a function \( E: \mathcal{K} \times \{0,1\}^b \rightarrow \{0,1\}^b \) that inputs a key \( K \in \mathcal{K} \) and a plaintext \( x \in \{0,1\}^b \) and produces a ciphertext \( y = E_K(x) = E(K,x) = P(x \oplus 0^r || K) \oplus 0^c || K \), where \( k \leq c \).

3. Security Model

Syntax of Authenticated Encryption (AE). Let \( \mathcal{K}, \mathcal{N}, \mathcal{H}, \mathcal{M}, \mathcal{C}, \) and \( \mathcal{T} \) be, respectively, the sets of the keys, nonce, associated data, plaintexts, ciphertexts, and authentication tags. A nonce-based AE with associated data scheme \( \Pi = (\mathcal{E}, \mathcal{D}) \) consists of an encryption algorithm \( \mathcal{E}: \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \rightarrow \mathcal{C} \times \mathcal{T} \) and a decryption algorithm \( \mathcal{D}: \mathcal{H} \times \mathcal{N} \times \mathcal{C} \times \mathcal{T} \rightarrow \mathcal{M} \cup \{1\} \), where the symbol \( 1 \) indicates the failure of the decryption oracle. Let \( K \in \mathcal{K} \) be a key, \( N \in \mathcal{N} \) be a nonce, \( A \in \mathcal{H} \) be an associated data, \( M \in \mathcal{M} \) be a plaintext, \( C \in \mathcal{C} \) be a ciphertext, and \( T \in \mathcal{T} \) be an authentication tag, then the syntax is formalized as follows:

\[
(C, T) \leftarrow \mathcal{E}_K(N, A, M),
\]

(3)

where \( \mathcal{E}_K(N, A, M) = (C, T) \) if and only if \( \mathcal{D}(N, A, C, T) = M \). A secure AE scheme returns \( 1 \) if it receives an error \( (N, A, C, T) \) pair.

The nonce-based AE with associated data scheme \( \Pi = (\mathcal{E}, \mathcal{D}) \) is called as an online AE scheme (or authenticated online cipher) if and only if the \( j \)-th ciphertext block \( C_j \) only depends on the first \( j \) plaintext blocks \( M_1, \ldots, M_j \), where \( j = 1, \ldots, m = \lfloor |M|/r \rfloor \). That is to say, for any fixed key \( K \), nonce \( N \), and associated data \( A \), if two plaintexts \( M \) and \( M' \) share an \( l \)-block common prefix, where \( 0 \leq l \leq m - 1 \), then their encrypted ciphertexts \( C \) and \( C' \) also share an \( l \)-block common prefix. Therefore, a secure authenticated online cipher requires that ciphertexts do not reveal any further information about plaintexts than its length and the longest common prefix with previous plaintexts.

Ideal Online Function and Ideal Authenticated Online Cipher. Let \( f \) be a function randomly chosen from \( N \times \mathcal{K} \times \{0,1\}^{(j-r)r} \times \{0,1\}^r \rightarrow \{0,1\}^s \), where \( 1 \leq j \leq m = \lfloor |M|/r \rfloor \) and \( 1 \leq s \leq r \). We define an ideal online function \( g: N \times \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C} \) as follows:

\[
C = g(N, A, M) = f^N_j(N, A, M_1, \ldots, M_j),
\]

(4)

\[
C_j = f^N_j(N, A, M_1, \ldots, M_{j-1}, M_j).
\]

(5)

Let \( t \) be a tag-generation function randomly chosen from \( N \times \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T} \), and we define an ideal authenticated online cipher \( \mathcal{S}: N \times \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C} \) as follows:

\[
(C, T) = \mathcal{S}(N, A, M),
\]

(6)

where \( C = g(N, A, M) \) and \( T = t(N, A, M) \).

AE Security Model. The security model of AE schemes includes the conventional security model (privacy and authenticity) [11, 17] and all-in-one AE security model [18, 22–24]. In fact, all-in-one AE security model covers the conventional privacy and authenticity security models. Therefore, we consider all-in-one AE security model. Let \( \Pi = (\mathcal{E}, \mathcal{D}) \) be an AE scheme. The all-in-one AE security model is defined as follows.

Definition 1 (AE security [24]). Let \( P \) be a public random permutation, \( K \) be a key, and \( \Pi[P] \) be a \( P \)-based AE scheme. Let \( q, \sigma, \rho \geq 0 \). Then, the AE security advantage of the adversary is
Adv_{\Pi[P]}^{ae}(q, \sigma, p) = \left| \Pr[\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P} = 1] - \Pr[\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P} = 1] \right| = \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P), \quad (6)

where q is the number of querying the encryption oracle \mathcal{E} or the decryption oracle \mathcal{D}, generating at most \sigma blocks, p is the number of querying the permutation P or its inverse P^{-1}, $ is an ideal authenticated online cipher, and $ \perp $ stands for the failure of the decryption oracles.

4. APE*: Authenticated Permutation-Based Encryption Scheme with Beyond Conventional Security for Lightweight Applications

In this section, we provide a new pure permutation-based lightweight online AE mode APE* which enjoys beyond conventional security. Section 4.1 describes the specifica-

4.1. APE*: Pure Permutation-Based Lightweight Authenti-

We utilize the concurrent absorption method [25] to process of invoking the underlying permutation as few as possible, the rate of the last permutation is XOR-ed to the capacity of the authentication part. Moreover, to prevent forgery attacks, we utilize the iterated Even–Mansour cipher with a short key [21], to generate the ciphertext for the encryption part and invoke the Even–Mansour cipher with a short key [21], to replace the Even–Mansour modular structure of our scheme by the random permutation Q and rename the new scheme as \Pi[Q]. There exists a nontrivial gap for this replacement. According to the definition of the AE security, we have

\begin{align}
\text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p) &= \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \\
&= \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \\
&\leq \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; \mathcal{E}[Q], \mathcal{D}[Q], P) \\
&+ \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \\
&\leq \text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) + \text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p). \quad (8)
\end{align}

It follows that we need to calculate the upper bounds of \text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) and \text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p). First, according to the advantage of the Even–Mansour cipher with a short key [21], we have

\begin{align}
\text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) &= \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; \mathcal{E}[Q], \mathcal{D}[Q], P) \leq \frac{\mu P}{2^c}. \quad (9)
\end{align}

where $\mu$ is the maximal multiplicity. Now, we consider the rationality of $\mu$. The probability that the multiplicity exceeds $\mu$ is upper bounded by $\left( \frac{q}{\mu} \right) (1/2^c)^{\mu-1}$, which is very close to zero. By Stirling’s approximation, this probability is also bounded by $2^c (\text{ea}/2^c)^{2^c}$, where $e = 2.71828182845 \ldots$. Assume that $\text{ea}/2^c = (\text{ea}/2^c)^{1/2}$ and $16\text{ea}/2^c \ll 1$, and we have $\mu = (\text{ea} \cdot 2^c / p \cdot 2^c)^{1/2}$. It follows that

\begin{align}
\text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) &\leq \left( \frac{\text{ea} P}{2^b} \right)^{1/2}. \quad (10)
\end{align}

Then, we need to compute the following advantage:

\begin{align}
\Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \leq \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \leq \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P). \quad (11)
\end{align}

conventional security. Besides, APE* also has an authenticated online cipher. In this section, we prove that APE* enjoys at most about $\min[r, c]$-bit AE security. Let \Pi[P] = (\mathcal{E}, \mathcal{D}) stand for our APE* scheme with a permutation P.

\begin{align}
\text{Theorem 1. Let } P^\perp && \text{Perm} && (b) && \text{be a public } b \text{-bit random permutation and } b = r + c. \quad \text{Then,}
\end{align}

\begin{align}
\text{Adv}^{ae}_{\Pi[P]}(q, \sigma, p) &\leq \sqrt{\frac{e^2 \sigma q}{2^b} + \frac{15 (\sigma + q)^2}{2^b} + \frac{2 \sigma q}{2^c} + \frac{q}{2^c}}. \quad (7)
\end{align}

where $e = 2.71828182845 \ldots$ is the base of the natural logarithm.

Proof. We utilize the modular proof approach. First, our scheme can be described as a scheme based on an Even–Mansour cipher with a short key $E_K$, i.e., \Pi[P] can be represented as $\Pi[E_K]$, where $K$ is the secret key. Then, we replace the Even–Mansour modular structure of our scheme by the random permutation Q and rename the new scheme as \Pi[Q]. There exists a nontrivial gap for this replacement. According to the definition of the AE security, we have

\begin{align}
\text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p) &= \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \\
&= \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \\
&\leq \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; \mathcal{E}[Q], \mathcal{D}[Q], P) \\
&+ \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; \mathcal{E}[Q], \mathcal{D}[Q], P) \\
&\leq \text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) + \text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p). \quad (8)
\end{align}

It follows that we need to calculate the upper bounds of \text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) and \text{Adv}^{ae}_{\Pi[Q]}(q, \sigma, p). First, according to the advantage of the Even–Mansour cipher with a short key [21], we have

\begin{align}
\Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; \mathcal{E}[Q], \mathcal{D}[Q], P) &\leq \frac{\mu P}{2^c}. \quad (9)
\end{align}

where $\mu$ is the maximal multiplicity. Now, we consider the rationality of $\mu$. The probability that the multiplicity exceeds $\mu$ is upper bounded by $\left( \frac{q}{\mu} \right) (1/2^c)^{\mu-1}$, which is very close to zero. By Stirling’s approximation, this probability is also bounded by $2^c (\text{ea}/2^c)^{2^c}$, where $e = 2.71828182845 \ldots$. Assume that $\text{ea}/2^c = (\text{ea}/2^c)^{1/2}$ and $16\text{ea}/2^c \ll 1$, and we have $\mu = (\text{ea} \cdot 2^c / p \cdot 2^c)^{1/2}$. It follows that

\begin{align}
\text{Adv}^{ppr}_{\Pi[Q]}(q, \sigma, p) &\leq \left( \frac{\text{ea} P}{2^b} \right)^{1/2}. \quad (10)
\end{align}

Then, we need to compute the following advantage:

\begin{align}
\Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P) \leq \Delta(\mathcal{E}_K^{\mathcal{D}_K, \mathcal{D}_P}, P; S, \perp, P). \quad (11)
\end{align}
Input: a key $K$, a nonce $N$, an associated data $A$, and a plaintext $M$

Output: a ciphertext $C$ and a tag $T$

1. Partition $M$ into $M_1[1] \cdots [M_m]$, $|M| = r$, $1 \leq i \leq m$  
2. Partition $A$ into $A_1[1] \cdots [A_a]$, $|A_a| = c$, $1 \leq j \leq a$  
3. $C_0 = N$, $V_0 = K$  
4. if $a \leq m$ then  
5. for $0 \leq i < a - 1$ do  
6. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
7. $C_{i+1} = K_{i+1} \oplus M_{i+1}$  
8. $V_{i+1} = W_{i+1} \oplus A_{i+1}$  
9. end for  
10. for $a \leq i < m - 1$ do  
11. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
12. $C_{i+1} = K_{i+1} \oplus M_{i+1}$  
13. $V_{i+1} = W_{i+1} \oplus A_{i+1}$  
14. end for  
15. $(K_{m+1}, W_{m+1}) = P(C_m, V_m \oplus 1)$  
16. $T = W_{m+1} \oplus K \oplus K_{m+1}$  
17. else  
18. for $0 \leq i < m - 1$ do  
19. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
20. $C_{i+1} = K_{i+1} \oplus M_{i+1}$  
21. $V_{i+1} = W_{i+1} \oplus A_{i+1}$  
22. end for  
23. for $m \leq i < a - 1$ do  
24. $(K_{a-1+i}, W_{a-1+i}) = P(C_i, V_i)$  
25. $C_{a-1+i} = K_{a-1+i}$  
26. $V_{a-1+i} = W_{a-1+i} \oplus A_{a-1+i}$  
27. end for  
28. $(K_{a+i}, W_{a+i}) = P(C_i, V_a \oplus 1)$  
29. $T = W_{a+i} \oplus K \oplus K_{a+i}$  
30. end if  
31. return $(C = C_1[1] \cdots [C_m], T)$

Algorithm 1: Encryption algorithm: $\mathcal{E}_K(N, A, M)$.

Now, we replace the random permutation $Q$ by the random function $f$ and rename the new scheme as $\Pi[f]$. According the hybrid argument and the RP/RF switch lemma, we have

Input: a key $K$, a nonce $N$, an associated data $A$, a ciphertext $C$, and a tag $T$

Output: a plaintext $M$ or $\perp$

1. Partition $C$ into $C_1[1] \cdots [C_m]$, $|C_i| = r$, $1 \leq i \leq m$  
2. Partition $A$ into $A_1[1] \cdots [A_a]$, $|A_a| = c$, $1 \leq j \leq a$  
3. $C_0 = N$, $V_0 = K$  
4. if $a \leq m$ then  
5. for $0 \leq i < a - 1$ do  
6. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
7. $M_{i+1} = K_{i+1} \oplus C_{i+1}$  
8. $V_{i+1} = W_{i+1} \oplus A_{i+1}$  
9. end for  
10. for $a \leq i < m - 1$ do  
11. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
12. $M_{i+1} = K_{i+1} \oplus C_{i+1}$  
13. $V_{i+1} = W_{i+1}$  
14. end for  
15. $(K_{m+1}, W_{m+1}) = P(C_m, V_m \oplus 1)$  
16. $T = W_{m+1} \oplus K \oplus K_{m+1}$  
17. else  
18. for $0 \leq i < m - 1$ do  
19. $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$  
20. $M_{i+1} = K_{i+1} \oplus C_{i+1}$  
21. $V_{i+1} = W_{i+1} \oplus A_{i+1}$  
22. end for  
23. for $m \leq i < a - 1$ do  
24. $(K_{a-1+i}, W_{a-1+i}) = P(C_i, V_a \oplus 1)$  
25. $C_{a-1+i} = K_{a-1+i}$  
26. $V_{a-1+i} = W_{a-1+i} \oplus A_{a-1+i}$  
27. end for  
28. $(K_{a+i}, W_{a+i}) = P(C_i, V_a \oplus 1)$  
29. $T = W_{a+i} \oplus K \oplus K_{a+i}$  
30. end if  
31. if $T = T$ then  
32. return $M = M_1[1] \cdots [M_m] \perp M_m$  
33. else  
34. return $\perp$ (INVALID)  
35. end if

Algorithm 2: Decryption algorithm: $\mathcal{D}_K(N, A, C, T)$.  

Figure 1: APE*: permutation-based lightweight AE mode with beyond conventional security and concurrent absorption for $a$-block associated data and $m$-block plaintext (upper: $a \leq m$; lower: $a > m$).
\[ \text{Adv}_{\Pi(q)}(\epsilon, \sigma, \rho) = \Delta(\mathcal{E}[Q], \mathcal{D}[Q], P; \epsilon, \sigma, \rho) \]
\[ \leq \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) + \Delta(\mathcal{D}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) \]
\[ \leq \frac{(\sigma + \rho)^2}{2^{3\sigma+1}} + \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho). \]  
(12)

Next, we need to evaluate \( \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) \). According to the definitions of privacy and authenticity [17], we have

\[ \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) \leq \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) + \Delta(\mathcal{D}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) \]
\[ = \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho) + \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \sigma, \epsilon, \rho). \]
\[ = \text{Adv}_{\Pi(f)}^\text{auth}(\epsilon, \sigma, \rho) + \text{Adv}_{\Pi(f)}^\text{priv}(\epsilon, \sigma, \rho), \]  
(13)

where

\[ \text{Adv}_{\Pi(f)}^\text{auth}(\epsilon, \sigma, \rho) = \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho), \]
\[ \text{Adv}_{\Pi(f)}^\text{priv}(\epsilon, \sigma, \rho) = \Delta(\mathcal{E}[f], \mathcal{D}[f], P; \epsilon, \sigma, \rho). \]  
(14)

In the first step, we calculate the PRIV advantage \( \text{Adv}_{\Pi(f)}^\text{priv}(\epsilon, \sigma, \rho) \). Assume that the adversary queries \((N^w_1, A_{1}^w, M^w_1), \ldots, (N^w_q, A^w_q, M^w_q)\) to the encryption oracle \( \mathcal{E}[f] \) and gains the corresponding responses \((C^1, T^1), \ldots, (C^q, T^q)\). Here, the adversary is deterministic and authentic, i.e., each query of the adversary \((N^w_1, A_{1}^w, M^w_1), \ldots, (N^w_q, A^w_q, M^w_q)\) is completely determined by the previous query-response pairs \([\{N^1, A^1, M^1, C^1, T^1\}, \ldots, (N^w_q, A^w_q, M^w_q, C^w_q, T^w_q)\}\), where \(1 \leq w \leq q - 1\) and \((N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)\) are distinct.

Let us define some symbols for the \( i \)-th encryption query-response pair \((N^i, A^i, M^i, C^i, T^i)\), where \(1 \leq i \leq q\). Let

\[ a^i = |[A^i]|/|c| \quad \text{and} \quad m^i = |[M^i]|/|r| \]

be, respectively, the block lengths of the associated data \( A^i \) and the plaintext \( M^i \). Then, \( A^i = A^i_{1} \| A^i_{2} \| \cdots \| A^i_{m^i} \) and \( M^i = M^i_{1} \| M^i_{2} \| \cdots \| M^i_{m^i} \). Here, we assume that the block length of the associated data is always less than or equal to the block length of the plaintext. Let \( I^i_0 = (N^i_0, 0), I^i_1 = (C^i_0, V^i_1), \ldots, I^i_0 = (C^i_{m^i - 1}, V^i_{m^i}), O^i_0 = (K^i_0, W^i_1), \ldots, O^i_0 = (K^i_{m^i - 1}, W^i_{m^i}) \) be the inputs and outputs of the random function \( f \), where \( C^i_s = K^i_s \| M^i_s \) for \( 1 \leq s \leq m^i \) and \( V^i_s = W^i_s \| A^i_s \) for \( 1 \leq s \leq q \).

We define an event \( \text{Coll} \) that stands for a collision between the inputs of the random function \( f \). For an authenticated online cipher, we consider that any two distinct queries \((N^i, A^i, M^i) \neq (N^j, A^j, M^j)\) share a common prefix, where \(1 \leq i, j \leq q\). The adversary is non-co-operative; therefore, \( N^1 = N^q = N \) is a common prefix. We consider the following cases:

Case 1: if \( A^i = A^j = A \) is fully common, then \( M^i \neq M^j \). Assume that \( M^i \) and \( M^j \) have a \( \alpha \)-longest common prefix, i.e., \( M^i_1 \| \cdots \| M^i_{\alpha} = M^j_1 \| \cdots \| M^j_{\alpha}, \) where \( \alpha \geq 0 \) (\( \alpha = 0 \) means \( M^i_1 \neq M^j_1 \)). Therefore, \( I^i_1 \| I^j_1 \| \cdots \| I^i_{\alpha} = I^j_1 \| \cdots \| I^j_{\alpha} \) \( \neq I^i_{\alpha+1} \). The event \( \text{Coll} \) occurs if one of the following collisions happens:

1. \( I^i_{\alpha+1} = I^j_{\alpha+1} \) for \( t \neq \alpha + 1 \), where \( 1 \leq i, j \leq q \).
2. \( I^i_{\alpha+1} = I^j_{\alpha+1} \) for \( t = \alpha \) and \( 1 \leq i, j \leq q \).
3. \( I^i_{\alpha+1} = I^j_{\alpha+1} \) for \( 1 \leq s \leq m^i \) and \( 1 \leq t \leq m^j \), where \( 1 \leq i, j \leq q \).

Let \( t \) be the maximum block length of the plaintext, i.e., \( m^i \leq m^j \) and \( m^j \leq t \), and let \( \sigma = q \). Therefore, after removing the duplicate conditions, the probability that the event \( \text{Coll} \) occurs is

\[ \Pr[\text{Coll}] = \sum_{1 \leq i, j \leq q} \frac{1}{2^q} \left[ \frac{1}{2^q} + \sum_{i=1}^{q} \frac{1}{2^q} \right] \]
\[ \leq \frac{(q + \rho)^2}{2^{3q+1}} + \frac{\sigma}{2^{3q+1}}. \]  
(15)

Case 2: if \( A^i \neq A^j \) but \( A^i \) and \( A^j \) have an \( \alpha \)-longest common prefix, then \( A^i_{\alpha+1} \| \cdots \| A^i_{\alpha+m^i} \) and \( A^j_{\alpha+1} \| \cdots \| A^j_{\alpha+m^j} \), where \( \alpha \geq 0 \). We assume that \( M^i \) and \( M^j \) have a \( \beta \)-longest common prefix, where \( \beta \geq 0 \). Then, \( M^i_{\beta+1} \| \cdots \| M^i_{\beta+m^i} = M^j_{\beta+1} \| \cdots \| M^j_{\beta+m^j} \). Therefore, \( I^i_{\beta+1} \| I^j_{\beta+1} \| \cdots \| I^i_{\beta+m^i} \) \( \neq I^i_{\beta+1} \). The event \( \text{Coll} \) occurs if one of the following collisions happens:

1. \( I^i_{\beta+1} = I^j_{\beta+1} \) for \( t \neq \beta + 1 \), where \( 1 \leq i, j \leq q \).
2. \( I^i_{\beta+1} = I^j_{\beta+1} \) for \( \beta + 2 \leq s \leq m^i \) and \( 1 \leq t \leq m^j \), where \( 1 \leq i, j \leq q \).
3. \( I^i_{\beta+1} = I^j_{\beta+1} \) for \( 1 \leq s \neq t \leq m^i \), where \( 1 \leq i, j \leq q \).
\( I_1 = I_0 = I_0 = (N, 0) \) for \( 1 \leq s \leq m' \), where \( 1 \leq i \neq j \leq q \).

It follows that, in Case 2.2, the probability that the event \( \text{Coll} \) occurs is

\[
\text{Pr}[\text{Coll}] = \sum_{1 \leq i \neq j \leq q} \left( \frac{1}{2^b} + \sum_{1 \leq \ell \neq q_\ell \leq 2^b} \frac{1}{2^b} + \sum_{1 \leq \ell \neq q_\ell \leq 2^b} \frac{1}{2^b} + \sum_{1 \leq \ell \neq q_\ell \leq 2^b} \frac{1}{2^b} \right)
\]

Summarizing the above mutually exclusive cases, the probability that the event \( \text{Coll} \) occurs is

\[
\text{Pr}[\text{Coll}] \leq \frac{(q + \sigma)^2}{2^{b+1}} + \frac{\sigma}{2^b}.
\]

In the second step, we evaluate the AUTH advantage \( \text{Adv}_{\text{Auth}}[f] (q, \sigma, p) \). Assume that the adversary makes \( q_d \) nontrivial forgery attempts \( (N_1, A_1, C_1, T_1), \ldots, (N_{qd}, A_{qd}, C_{qd}, T_{qd}) \) to the decryption oracle \( \mathcal{D}[f] \) after querying \( q_e \) encryption oracles, where \( (N_1, A_1, C_1, T_1), \ldots, (N_{qd}, A_{qd}, C_{qd}, T_{qd}) \notin (N_1, A_1, C_1, T_1), \ldots, (N_{qd}, A_{qd}, C_{qd}, T_{qd}) \) and \( q = q_e + q_d \). Here, we define an event \( \text{Forge} \) that some decryption queries among \( q_d \) forgery attempts do not return \( \perp \). If the event \( \text{Forge} \) does not occur, the responses of querying \( (\mathcal{E}[f], \mathcal{D}[f]) \) and \( (S, I) \) are identical. Therefore, by the total probability formula, we have

\[
\text{Adv}_{\text{Auth}}[f] (q, \sigma, p) \leq \text{Pr}[\text{Forge}] \leq \text{Pr}[\text{Coll}] + \text{Pr}[\text{Forge} \rightarrow \text{Coll}]
\]

The probability that the event \( \text{Coll} \) happens is similar to the PRIV advantage except that we need to consider an extra query complexity—the decryption query complexity under the forgery attempts, i.e., \( \text{Pr}[\text{Coll}] \leq (q + \sigma)^2/2^{b+1} + \sigma/2^b \), where \( \sigma \) is the total query complexity of the encryption and decryption queries.

To compute the probability \( \text{Pr}[\text{Forge} \rightarrow \text{Coll}] \), we consider the following cases:

Case 1: \( T'^f \) is new, i.e., \( T'^f \notin \{T_1', \ldots, T_{qd}'\} \), where \( 1 \leq i \leq q_d \). For each forgery attempt, the probability of correctly guessing the image of a new point for the adversary is at most \( 1/(2^e - q_d) \).

Case 2: \( T'^f \) is old, but \( (N_{qi}, A_{qi}, C_{qi}) \) is new. We further analyze this case as follows.

Case 2.1: \( N_{qi} \) is new, i.e., \( N_{qi} \notin \{N_1, \ldots, N_{qd}\} \). The image of this new point under a new random function is uniform, random, and independent. Therefore, the probability for correctly guessing the tag \( T'^f \) is at most \( 1/2^e \).

Case 2.2: \( N_{qi} \) is old, but \( (A_{qi}, C_{qi}) \) is new. Under the condition of the event \( \neg \text{Coll} \), the input of the last random function \( f \) is new. The outputs of \( f \) with distinct inputs are random and independent. Therefore, the probability for correctly guessing the same tag is at most \( 1/2^e \).

Summarizing the above two cases, the successful probability of \( q_d \) forgery attempts is upper bounded by \( q_d/(2^e - q_d) \).

Therefore, according to the sugar water inequality \( a/b \leq a + m + b/m, \) where \( b > a > 0 \) and \( m \geq 0 \), and \( q = q_e + q_d \), we have

\[
\text{Adv}_{\text{Auth}}[f] (q, \sigma, p) \leq \text{Pr}[\text{Forge}] \leq \text{Pr}[\text{Coll}] + \text{Pr}[\text{Forge} \rightarrow \text{Coll}]
\]

The probability of the event \( \text{Coll} \) happens is similar to the PRIV advantage except that we need to consider an extra query complexity—the decryption query complexity under the forgery attempts, i.e., \( \text{Pr}[\text{Coll}] \leq (q + \sigma)^2/2^{b+1} + \sigma/2^b \), where \( \sigma \) is the total query complexity of the encryption and decryption queries.

To compute the probability \( \text{Pr}[\text{Forge} \rightarrow \text{Coll}] \), we consider the following cases:

Case 1: \( T'^f \) is new, i.e., \( T'^f \notin \{T_1', \ldots, T_{qd}'\} \), where \( 1 \leq i \leq q_d \). For each forgery attempt, the probability of correctly guessing the image of a new point for the adversary is at most \( 1/(2^e - q_d) \).

Case 2: \( T'^f \) is old, but \( (N_{qi}, A_{qi}, C_{qi}) \) is new. We further analyze this case as follows.

Case 2.1: \( N_{qi} \) is new, i.e., \( N_{qi} \notin \{N_1, \ldots, N_{qd}\} \). The image of this new point under a new random function is uniform, random, and independent. Therefore, the probability for correctly guessing the tag \( T'^f \) is at most \( 1/2^e \).

Case 2.2: \( N_{qi} \) is old, but \( (A_{qi}, C_{qi}) \) is new. Under the condition of the event \( \neg \text{Coll} \), the input of the last random function \( f \) is new. The outputs of \( f \) with distinct inputs are random and independent. Therefore, the probability for correctly guessing the same tag is at most \( 1/2^e \).

Therefore, combining (1)–(6), we can obtain the result of Theorem 1.

According to Theorem 1, the AE security of \( \text{APE}^+ \) is up to \( 2 \min[\epsilon, r, c] \) adversarial queries against non-misusing adversaries. In other words, \( \text{APE}^+ \) ensures at most about \( \min[\epsilon, r, c] \)-bit AE security, which is a beyond conventional \((\epsilon/2\text{-}\text{bit})\) security.

5. Discussions

The original intention of designing our \( \text{APE}^+ \) scheme is to achieve higher efficiency, better performance, and stronger security on the lightweight devices. \( \text{APE}^+ \) is an improved version of APE series (including \( \text{APE}, \text{APE}^R \), \( \text{APE}^O \), and \( \text{APE}^C \)). Therefore, \( \text{APE}^+ \) inherits most of the advantages of APE series. Besides, it has the following advantages in the hardware implementation:

1. \( \text{APE}^+ \) is a pure permutation-based lightweight online AE mode with concurrent absorption. The rate of
processing the associated data and the message is faster on hardware devices.

(2) APE⁺ is inverse-free, i.e., its decryption circuit does not invoke the inverse of permutation. Moreover, it is a stream-cipher encryption mode.

(3) APE⁺ is built by the cascade method and has no backward feedback. Therefore, it can be fully pipeline implemented.

(4) To the best of our knowledge, APE⁺ is the first AE mode which supports beyond conventional security against blockwise adaptive adversaries in the lightweight devices.

(5) APE series and APE⁺ are designed and have proven security against nonce-misusing adversaries up to common prefix. Jovanovic et al. showed an attack on APE with a complexity of about $2^{n/2}$ in the noncespecting setting (here, "noncespecting" means that the nonce is never repeated in the encryption queries) according to the defect $M_t \oplus C_{t-1}$ [26]. If there exists $k$ such that $M_t \oplus C_{t-1} = M_1 = 0$, the adversary breaks the privacy with a complexity of about $2^{n/2}$ in the noncespecting setting. In fact, this attack also works for APE series. This defect exists in APE⁺RI, APE⁺OW, and APE⁺CA, while it does not exist in APE⁺. Therefore, APE⁺ is robust against this kind of attack.

Table 2 shows the comparison of permutation-based lightweight AE modes. From the perspective of hardware implementation costs, APE⁺ just needs the permutation circuit on hardware devices as its encryption and decryption algorithms only call the permutation $P$. Therefore, the area of the hardware device and the number of hardware footprints are minimized. From the perspective of the efficiency, the bandwidth of implementing is $|N| + |A| + |M| + c$. Moreover, the computational costs of the encryption and decryption algorithms are $1 + \max\{|A|/r, |[M]/r|\}$. We utilize the method of concurrent absorption to process the associated data and the message. Therefore, the computational complexity is obviously reduced. From the perspective of the security, APE⁺ enjoys at most about $\min\{r, c\}$-bit AE security, which is a great contribution of this paper. Fixing a permutation with recommended parameters $b = 256$, $r = 96$, and $c = 160$, APE series enjoy at most about 80-bit security while APE⁺ enjoys at most about 96-bit security. Security levels of permutation-based AE modes using recommended parameters are shown in Table 1.

This paper just focuses on the single-key security of APE⁺. Recently, the multikey or multiuser security and related-key security are also very hot research topics of lightweight ciphers. The implementation of APE⁺ on the hardware circuit and the security under the multikey or multiuser and related-key settings are our next important works.

6. Conclusions

Most of the devices widely used in smart home and Internet of Things are resource constrained. The privacy security and authenticity security of data from these devices are crucial in the process of data transmission. The lightweight AE modes designed by permutations have more advantages and attractions for the protection of data security due to its simple structure, convenient lookup table, and fast running speed. However, almost all of permutation-based lightweight AE modes enjoy conventional security. In this paper, we discuss the problem of whether can we design an efficient lightweight AE mode to achieve beyond conventional security bound for permutation-based lightweight ciphers. We propose a new permutation-based lightweight AE mode APE⁺ with beyond conventional security, derive its security proof, and discuss the properties of APE⁺. APE⁺ has proven AE security up to about $2^{\min\{r, c\}}$ adversarial queries and it is robust, where $r$ and $c$ are, respectively, the rate and the capacity of the permutation. APE⁺ is an improved version of APE series and inherits most of the advantages of APE series. It is well suited for the protection of the data security in some special environments, such as an insufficiently large capacity of the permutation or the partial information leakage of permutation by side channel attacks.

Data Availability

The data used to support the findings of the study are available within the article.

Conflicts of Interest

The author declares that there are no conflicts of interest.

| Scheme               | APE   | APE⁺RI | APE⁺OW | APE⁺CA | Betle | APE⁺  |
|----------------------|-------|--------|--------|--------|-------|-------|
| Bandwidth            | $|N| + X + c$ | $|N| + X + c$ | $X + b$ | $|N| + X + c/2$ | $|N| + X + b$ | $|N| + X + c$ |
| Encryption           | $P$   | $P$    | $P$    | $P$    | $P$   | $P$   |
| Decryption           | $P, P^{-1}$ | $P^{-1}$ | $P^{-1}$ | $P^{-1}$ | $P^1$ | $P$   |
| Encryption cost      | $n + a + m$ | $n + a + m$ | $n + a + m$ | $n + a + m$ | $1 + a + m$ | $1 + max(a, m)$ |
| Decryption cost      | $n + a + m$ | $n + a + m$ | $n + a + m$ | $n + a + m$ | $1 + a + m$ | $1 + max(a, m)$ |
| Security             | $c/2$  | $c/2$  | $\min\{r, c/2\}$ | $c/2$  | $\min\{r/2, c - \log r, r\}$ | $\min\{r, c\}$ |
| Nonce-misuse         | Yes    | Yes    | Yes    | Yes    | No    | Yes   |
| Reference            | [17]   | [18]   | [18]   | [18]   | [20]  | This paper |

Table 2: Comparison of permutation-based AE modes. Let $X = |A| + |M|$, $n = |[N]/r|$, $a = |[A]/c|$, $m = |[M]/r|$, and $m' = |[M] - (c/2)/r|$. 

Let $X = |A| + |M|$, $n = |[N]/r|$, $a = |[A]/c|$, $m = |[M]/r|$, and $m' = |[M] - (c/2)/r|$. 

Security and Communication Networks
Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 61902195), Natural Science Fund for Colleges and Universities in Jiangsu Province (General Program, Grant no. 19KJB520045), and NUPTSF (Grant no. NY219131).

References

[1] C. Beierle, G. Leander, A. Moradi, and R. Sasoozadeh, “CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks,” IACR Transactions on Symmetric Cryptology, vol. 2019, no. 1, pp. 5–45, 2019.

[2] A. Bogdanov, L. R. Knudsen, and G. Leander, “Present: an ultra-lightweight block cipher,” in Lecture Notes in Computer Science 4727, P. Paillier and I. Verbauwhede, Eds., pp. 450–466, Springer-Verlag, Berlin, Germany, 2007.

[3] W. Wu and L. Zhang, “Lblock: a lightweight block cipher,” in Lecture Notes in Computer Science, J. López and G. Tsudik, Eds., Springer-Verlag, Berlin, Germany, pp. 327–344, 2011.

[4] A. R. Raza, K. Mahmood, M. F. Amjad, H. Abbas, and M. Afzal, “On the efficiency of software implementations of lightweight block ciphers from the perspective of programming languages,” Future Generation Computer Systems, vol. 104, pp. 43–59, 2020.

[5] B. Rashidi, “High-throughput and flexible ASIC implementations of SIMON and SPECK lightweight block ciphers,” International Journal of Circuit Theory and Applications, vol. 47, no. 8, pp. 1254–1268, 2019.

[6] P. Li, S. Zhou, B. Ren et al., “Efficient implementation of lightweight block ciphers on volta and pascal architecture,” Journal of Information Security and Applications, vol. 47, pp. 235–245, 2019.

[7] Y. Wei, P. Xu, and Y. Rong, “Related-key impossible differential cryptanalysis on lightweight cipher TWINE,” Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp. 509–517, 2019.

[8] D. Dinu, Y. L. Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, “Triathlon of lightweight block ciphers for the internet of things,” Journal of Cryptographic Engineering, vol. 9, no. 3, pp. 283–302, 2019.

[9] T. Hiscock, O. Savry, and L. Goubin, “Lightweight instruction-level encryption for embedded processors using stream ciphers,” Microprocessors and Microsystems, vol. 64, pp. 43–52, 2019.

[10] F. Farnoud, A. Ahubakr, K. J. Peter, and G. Kris, “Faceoff between the CAESAR lightweight finalists: ACORN vs. Ascon,” in Proceedings of the International Conference on Field-Programmable Technology, pp. 330–333, Naha, Japan, December 2018.

[11] Z. Bao, J. Guo, T. Iwata, and K. Minematsu, “ZOCB and ZOTR: tweakable blockcipher modes for authenticated encryption with full absorption,” IACR Transactions on Symmetric Cryptology, vol. 2019, no. 2, pp. 1–54, 2019.

[12] Y. Naito and T. Sugawara, “Lightweight authenticated encryption mode of operation for tweakable block ciphers,” IACR Trans. Cryptogr. Hardw. Embed. Syst.vol.2020, no. 1, pp. 66–94, 2020.

[13] J. Mohsen, B. Nasour, and N. Zeinolabedin, “Lightweight implementation of SILC, CLOC, AES-JAMBU and COLM authenticated ciphers,” Microprocessors and Microsystems, vol. 72, Article ID 102925, 2020.