Hindawi
Security and Communication Networks
Volume 2021, Article ID 1468007, 9 pages
https://doi.org/10.1155/2021/1468007

WILEY | Hindawi

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

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 $c/2$-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, APE^{RI}, APE^{OW}, and APE^{CA}), 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 using 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 lightweight 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.

Table 1: Security levels of permutation-based AE modes using recommended parameters (b, r, c), where b is the permutation size, r is the rate of the permutation, c is the capacity of the permutation, and $b = r + c$.

Scheme	b	r	c	Security
Ascon [10]	320	128	192	96
	320	64	256	128
APE [17]	256	96	160	80
APE^{RI} [18]	256	96	160	80
APE^{OW} [18]	256	96	160	80
APE^{CA} [18]	256	96	160	80
Bettle [20]	144	64	80	64
	256	128	128	121
APE$^+$	256	96	160	96
256	256	128	128	128

Ascon includes two versions with four configurations (three with 128-bit security and one with 96-bit security). In this table, we just list two of them.

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. For two finite

strings x and y, let $x\|y$ or xy denote their concatenation and let $x \oplus y$ denote their bitwise XOR operation from the least bit to the most bit. If X is a set, let $x \xleftarrow{\$} X$ stand for that x is uniformly sampled from the finite set X. If a is a decimal, let $\lceil a \rceil$ be the smallest integer greater than or equal to a. Let $\Pr[\mathbf{A}|\mathbf{B}]$ be the conditional probability that event $\mathbf{A}$ occurs, giving event $\mathbf{B}$.

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 $E: \mathcal{K} \times \{0,1\}^b \longrightarrow \{0,1\}^b$ 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 $\mathrm{Perm}(b)$ be the set of all permutations on b bits. Let P be a primitive utilized in E. Let $\mathscr{A}$ be an adversary with access to encryption, decryption, and the primitive and its inverse oracles, i.e., $(E_K^{\pm}, P^{\pm})$. Let $\mathscr{A}^O \Rightarrow 1$ be the event that an adversary $\mathscr{A}$ outputs 1 after interacting with the oracle O.

Let $K \xleftarrow{\$} \mathcal{K}$, $\pi \xleftarrow{\$} \mathrm{Perm}(b)$, then the SPRP advantage of $\mathscr{A}$ against E is defined as

$$\begin{aligned} \mathrm{Adv}_E^{\mathrm{sprp}}(\mathscr{A}) &= \left|\Pr\left[\mathscr{A}^{E_K^{\pm}, P^{\pm}} \Rightarrow 1\right] - \Pr\left[\mathscr{A}^{\pi^{\pm}, P^{\pm}} \Rightarrow 1\right]\right| \\ &= \Delta\left(E_K^{\pm}, P^{\pm}; \pi^{\pm}, P^{\pm}\right). \end{aligned} \tag{1}$$

If the advantage $\mathrm{Adv}_E^{\mathrm{sprp}}(\mathscr{A})$ 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 σ, and the number of querying the primitive and its inverse oracles p) used by adversaries are limited, we define the maximum advantage as

$$\mathrm{Adv}_E^{\mathrm{sprp}}(t, q, \sigma, p) = \max_{\mathscr{A}} \mathrm{Adv}_E^{\mathrm{sprp}}(\mathscr{A}). \tag{2}$$

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 $E: \mathcal{K} \times \{0,1\}^b \longrightarrow \{0,1\}^b$ that inputs a key $K \in \mathcal{K}$ and a plaintext $x \in \{0,1\}^b$ and produces a ciphertext $y = E_K(x) = E(K,x) = P(x \oplus 0^r \| K) \oplus 0^r \| K$, where $k \le c$.

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 $\mathcal{E}: \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \longrightarrow \mathcal{C} \times \mathcal{T}$ and a decryption algorithm $\mathcal{D}: \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \longrightarrow \mathcal{M} \cup \{\perp\}$, where the symbol $\perp$ 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:

$$\begin{aligned} (C, T) &\leftarrow \mathcal{E}_K(N, A, M), \\ \frac{M}{\perp} &\leftarrow \mathcal{D}_K(N, A, C, T), \end{aligned} \tag{3}$$

where $\mathcal{E}_K(N, A, M) = (C, T)$ if and only if $\mathcal{D}_K(N, A, C, T) = M$. A secure AE scheme returns $\perp$ 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 $j = 1, \ldots, m = \lceil |M|/r \rceil$. 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 $0 \le l \le m - 1$, then their encrypted ciphertexts C and $C\prime$ 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^j be a function randomly chosen from $\mathcal{N} \times \mathcal{H} \times \{0,1\}^{(j-1)r} \times \{0,1\}^s \longrightarrow \{0,1\}^s$, where $1 \le j \le m = \lceil |M|/r \rceil$ and $1 \le s \le r$. We define an ideal online function $g: \mathcal{N} \times \mathcal{H} \times \mathcal{M} \longrightarrow \mathcal{C}$ as follows:

$$\begin{aligned} C &= g(N, A, M) = \|_{j=1}^{m} f^j\left(N, A, M_1 \| \cdots \| M_{j-1}, M_j\right), \\ C_j &= f^j\left(N, A, M_1 \| \cdots \| M_{j-1}, M_j\right), \\ C &= C_1 \| \cdots \| C_m. \end{aligned} \tag{4}$$

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

$$(C, T) = \$(N, A, M), \tag{5}$$

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 $q, \sigma, p > 0$. Then, the AE security advantage of the adversary is

$$\begin{aligned}\mathrm{Adv}^{\mathrm{ae}}_{\Pi[P]}(q,\sigma,p) &= \left|\Pr\left[\mathscr{A}^{\mathscr{E}_K,\mathscr{D}_K,P^{\pm}}=1\right]-\Pr\left[\mathscr{A}^{\$,\perp,\mathrm{P}^{\pm}}=1\right]\right| \\ &= \Delta\left(\mathscr{E}_K,\mathscr{D}_K,P^{\pm};\$,\perp,P^{\pm}\right),\end{aligned} \tag{6}$$

where q is the number of querying the encryption oracle $\mathscr{E}$ or the decryption oracle $\mathscr{D}$, generating at most σ 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 specification of APE$^+$. Section 4.2 derives the security proofs of APE$^+$.

4.1. APE$^+$: Pure Permutation-Based Lightweight Authenticated Online Cipher. Let P be a public b-bit random permutation and $b = r + c$. Let $K \in \mathscr{K}$ be a key with k-bit, $N \in \mathscr{N}$ be a nonce, and $A \in \mathscr{H}$ be an associated data. Let $M = M_1 \| M_2 \| \cdots \| M_m \in \mathscr{M}$ be a plaintext, $C = C_1 \| C_2 \| \cdots \| C_m \in \mathscr{C}$ be the corresponding ciphertext, and $T \in \mathscr{T}$ be the corresponding authentication tag, where $m = \lceil |M|/r \rceil$ is the block length of the plaintext. Let τ be the bit-length of the tag and $\tau = k = c$.

To design a lightweight online AE mode with beyond conventional security, 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 generate the authentication tag for the authentication part. Moreover, to prevent forgery attacks, the rate of the last permutation is XOR-ed to the capacity of the last permutation with the short key to realize the authentication tag with a random mask. To make the number of invoking the underlying permutation as few as possible, we utilize the concurrent absorption method [25] to process the associated data and the message. The overview of APE$^+$ is shown in Figure 1.

APE$^+$ consists of an encryption algorithm $\mathscr{E}$ and a decryption algorithm $\mathscr{D}$. The encryption algorithm $\mathscr{E}$ takes as input a key K, a nonce N, an associated data A, and a plaintext M and returns a ciphertext C and a tag T. The decryption algorithm $\mathscr{D}$ takes K, N, A, C, and T as inputs and returns either M or $\perp$. The encryption and decryption algorithms are depicted in Algorithms 1 and 2.

4.2. Beyond Conventional Security of APE$^+$. APE, APE^{RI}, APE^{OW}, and APE^{CA} only ensure at most about $2^{c/2}$ adversarial queries (i.e., $c/2$-bit security). APE$^+$ is a pure permutation-based lightweight AE scheme with beyond conventional security. Besides, APE$^+$ is also an authenticated online cipher. In this section, we prove that APE$^+$ enjoys at most about $\min\{r, c\}$-bit AE security. Let $\Pi[P] = (\mathscr{E}, \mathscr{D})$ stand for our APE$^+$ scheme with a permutation P.

Theorem 1. *Let $P \xleftarrow{\$} Perm(b)$ be a public b-bit random permutation and $b = r + c$. Then,*

$$\mathrm{Adv}^{\mathrm{ae}}_{\Pi[P]}(q,\sigma,p) \le \sqrt{\frac{ep\sigma}{2^b}} + \frac{1.5(\sigma+q)^2}{2^b} + \frac{2\sigma}{2^r} + \frac{q}{2^c}, \tag{7}$$

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

$$\begin{aligned}\mathrm{Adv}^{\mathrm{ae}}_{\Pi[P]}(q,\sigma,p) &= \Delta\left(\mathscr{E}_K,\mathscr{D}_K,P;\$,\perp,\mathrm{P}\right) \\ &= \Delta\left(\mathscr{E}[E_K],\mathscr{D}[E_K],P;\$,\perp,\mathrm{P}\right) \\ &\le \Delta\left(\mathscr{E}[E_K],\mathscr{D}[E_K],P;\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P\right) \\ &\quad + \Delta\left(\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P;\$,\perp,\mathrm{P}\right) \\ &\le \mathrm{Adv}^{sprp}_{E}(q,\sigma,p) + \mathrm{Adv}^{ae}_{\Pi[\mathrm{Q}]}(q,\sigma,p).\end{aligned} \tag{8}$$

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

$$\mathrm{Adv}^{\mathrm{sprp}}_{E}(q,\sigma,p) = \Delta\left(\mathscr{E}[E_K],\mathscr{D}[E_K],P;\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P\right) \le \frac{\mu p}{2^c}, \tag{9}$$

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

$$\mathrm{Adv}^{\mathrm{sprp}}_{E}(q,\sigma,p) \le \left(\frac{ep\sigma}{2^b}\right)^{1/2}. \tag{10}$$

Then, we need to compute the following advantage:

$$A\,dv^{\mathrm{ae}}_{\Pi[\mathrm{Q}]}(q,\sigma,p) = \Delta\left(\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P;\$,\perp,\mathrm{P}\right). \tag{11}$$

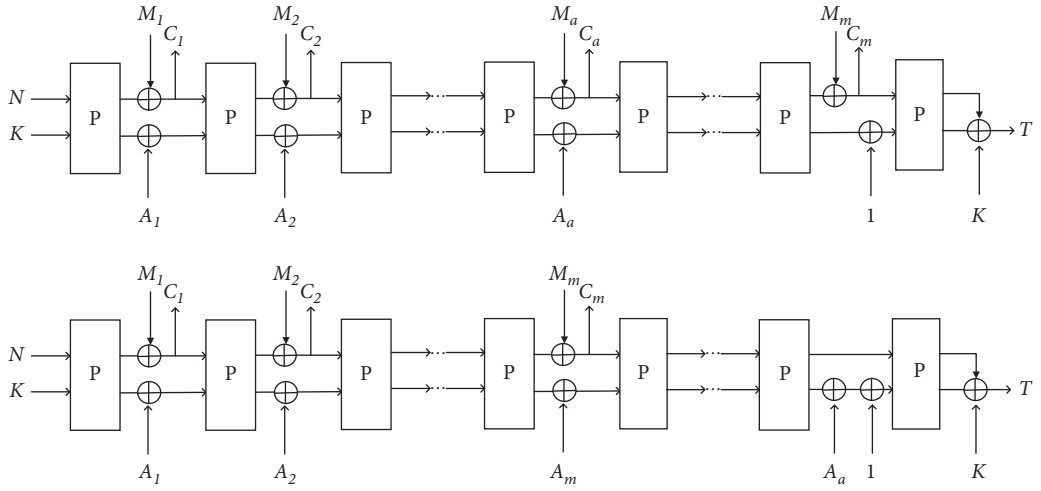

FIGURE 1: APE$^+$: permutation-based lightweight AE mode with beyond conventional security and concurrent absorption for a-block associated data and m-block plaintext (upper: $a \le m$; lower: $a > m$).

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 $M_1 \| \cdots \| M_m$, $|M| = r, 1 \le i \le m$
(2) Partition A into $A_1 \| \cdots \| A_a$, $|A_j| = c, 1 \le j \le a$
(3) $C_0 = N, V_0 = K$
(4) **if** $a \le m$ **then**
(5) **for** $0 \le i \le a - 1$ **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** $a \le i \le m - 1$ **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) $V_{i+1} = W_{i+1}$
(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** $0 \le i \le m - 1$ **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** $m \le i \le a - 1$ **do**
(24) $(K_{i+1}, W_{i+1}) P(C_i, V_i)$
(25) $C_{i+1} = K_{i+1}$
(26) $V_{i+1} = W_{i+1} \oplus A_{i+1}$
(27) **end for**
(28) $(K_{a+1}, W_{a+1}) = P(C_a, V_a \oplus 1)$
(29) $T = W_{a+1} \oplus K \oplus K_{a+1}$
(30) **end if**
(31) return $(C = C_1 \| C_2 \| \cdots \| C_{m-1} \| C_m, T)$

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

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 $C_1 \| \cdots \| C_m$, $|C_i| = r$, $1 \le i \le m$
(2) Partition A into $A_1 \| \cdots \| A_a$, $|A_j| = c$, $1 \le j \le a$
(3) $C_0 = N$, $V_0 = K$
(4) **if** $a \le m$ **then**
(5) **for** $0 \le i \le a - 1$ **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** $a \le i \le m - 1$ **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) $T\prime = W_{m+1} \oplus K \oplus K_{m+1}$
(17) **else**
(18) **for** $0 \le i \le m - 1$ **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** $m \le i \le a - 1$ **do**
(24) $(K_{i+1}, W_{i+1}) = P(C_i, V_i)$
(25) $C_{i+1} = K_{i+1}$
(26) $V_{i+1} = W_{i+1} \oplus A_{i+1}$
(27) **end for**
(28) $(K_{a+1}, W_{a+1}) = P(C_a, V_a \oplus 1)$
(29) $T' = W_{a+1} \oplus K \oplus K_{a+1}$
(30) **end if**
(31) **if** $T' = T$ **then**
(32) return $M = M_1 \| M_2 \| \cdots \| M_{m-1} \| M_m$
(33) **else**
(34) return $\perp$ (INVALID)
(35) **end if**

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

$$\begin{aligned}\mathrm{Adv}^{\mathrm{ae}}_{\Pi[\mathrm{Q}]}(q,\sigma,p) &= \Delta(\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P;\$,\perp,\mathrm{P})\\ &\le \Delta(\mathscr{E}[\mathrm{Q}],\mathscr{D}[\mathrm{Q}],P;\mathscr{E}[f],\mathscr{D}[f],P)\\ &\quad+\Delta(\mathscr{E}[f],\mathscr{D}[f],P;\$,\perp,\mathrm{P})\\ &\le \frac{(\sigma+q)^2}{2^{b+1}}+\Delta(\mathscr{E}[f],\mathscr{D}[f],P;\$,\perp,\mathrm{P}).\end{aligned} \tag{12}$$

Next, we need to evaluate $\Delta(\mathscr{E}[f],\mathscr{D}[f],P;\$,\perp,\mathrm{P})$. According to the definitions of privacy and authenticity [17], we have

$$\begin{aligned}&\Delta(\mathrm{E}[f],\mathscr{D}[f],P;\$,\perp,P)\\ &\le \Delta(\mathrm{E}[f],\mathscr{D}[f],P;\mathrm{E}[f],\perp,P)+\Delta(\mathrm{E}[f],\perp,P;\$,\perp,P)\\ &= \Delta(\mathrm{E}[f],\mathscr{D}[f],P;\mathrm{E}[f],\perp,P)+\Delta(\mathrm{E}[f],P;\$,P)\\ &= \mathrm{Adv}^{\mathrm{auth}}_{\Pi[f]}(q,\sigma,p)+\mathrm{Adv}^{\mathrm{priv}}_{\Pi[f]}(q,\sigma,p),\end{aligned} \tag{13}$$

where

$$\begin{aligned}\mathrm{Adv}^{\mathrm{auth}}_{\Pi[f]}(q,\sigma,p) &= \Delta(\mathscr{E}[f],\mathscr{D}[f],P;\mathscr{E}[f],\perp,P),\\ \mathrm{Adv}^{\mathrm{priv}}_{\Pi[f]}(q,\sigma,p) &= \Delta(\mathscr{E}[f],P;\$,\mathrm{P}).\end{aligned} \tag{14}$$

In the first step, we calculate the PRIV advantage $\mathrm{Adv}^{\mathrm{priv}}_{\Pi[f]}(q,\sigma,p)$. Assume that the adversary queries $(N^1,A^1,M^1),\ldots,((N^q,A^q,M^q)$ to the encryption oracle $\mathscr{E}[f]$ and gains the corresponding responses $(C^1,T^1),\ldots,(C^q,T^q)$. Here, the adversary is deterministic and adaptive, i.e., each query of the adversary $(N^{w+1},A^{w+1},M^{w+1})$ is completely determined by the previous query-response pairs $\{(N^1,A^1,M^1,C^1,T^1),\ldots,(N^w,A^w,M^w,C^w,T^w)\}$, where $1\le w\le q-1$ 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 $1\le i\le q$. Let $a^i=\lceil|A^i|/c\rceil$ and $m^i=\lceil|M^i|/r\rceil$ be, respectively, the block lengths of the associated data A^i and the plaintext M^i. Then, $A^i=A^i_1\|A^i_2\|\cdots\|A^i_{a^i}$ 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 $I^i_0=(N^i,0),I^i_1=(C^i_1,V^i_1),\ldots,I^i_{a^i}=(C^i_{a^i},V^i_{a^i}),\ldots,I^i_{m^i}=(C^i_{m^i},V^i_{m^i}\oplus 1)$ and $O^i_1=(K^i_1,W^i_1),\ldots,O^i_{a^i}=(K^i_{a^i},W^i_{a^i}),\ O^i_{a^i+1}=(K^i_{a^i+1},V^i_{a^i+1}),\ldots,O^i_{m^i}=(K^i_{m^i},V^i_{m^i}),O^i_{m^i+1}=(K^i_{m^i+1},T^i\oplus K^i_{m^i+1})$ be the inputs and outputs of the random function f, where $C^i_s=K^i_s\oplus M^i_s$ for $1\le s\le m^i$ and $V^i_t=W^i_t\oplus A^i_t$ for $1\le t\le a^i$.

We define an event **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 $(N^i,A^i,M^i)\ne(N^j,A^j,M^j)$ share a common prefix, where $1\le i\ne j\le q$. The adversary is nonce-misuse; therefore, $N^i=N^j=N$ is a common prefix. We consider the following cases:

Case 1: if $A^i=A^j=A$ is fully common, then $M^i\ne M^j$. Assume that M^i and M^j have an α-longest common prefix, i.e., $M^i_1\|\cdots\|M^i_\alpha=M^j_1\|\cdots\|M^j_\alpha$ and $M^i_{\alpha+1}\ne M^j_{\alpha+1}$, where $\alpha\ge 0$ ($\alpha=0$ means $M^i_1\ne M^j_1$). Therefore, $I^i_0\|\cdots\|I^i_\alpha=I^j_0\|\cdots\|I^j_\alpha$ and $I^i_{\alpha+1}\ne I^j_{\alpha+1}$. The event **Coll** occurs if one of the following collisions happens:

(1) $I^i_{\alpha+1}=I^j_t$ for $t\ne\alpha+1$, where $1\le i\ne j\le q$.
(2) $I^i_s=I^j_t$ for $\alpha+2\le s\le m^i,1\le t\le m^j$, where $1\le i\ne j\le q$.
(3) $I^i_s=I^i_t$ for $1\le s\ne t\le m^i$, where $1\le i\le q$.
(4) $I^i_s=I^i_0=I^j_0=(N^i,0)$ for $1\le s\le m^i$, where $1\le i\ne j\le q$.

Let l be the maximum block length of the plaintext, i.e., $m^i\le l$ and $m^j\le l$, and let $\sigma=ql$. Therefore, after removing the duplicate conditions, the probability that the event **Coll** occurs is

$$\begin{aligned}\Pr[\mathbf{Coll}] &= \sum_{1\le i\ne j\le q}\sum_{t\ne\alpha+1}\frac{1}{2^b}+\sum_{1\le i\ne j\le q}\sum_{\alpha+2\le s\le m^i}\sum_{1\le t\le m^j}\frac{1}{2^b}+\sum_{i=1}^{q}\sum_{1\le s\ne t\le m^i}\frac{1}{2^b}+\sum_{i=1}^{q}\sum_{s=1}^{m^i}\frac{1}{2^r}\\ &\le \sum_{1\le i\ne j\le q}\frac{(l-1)+l(l-2)}{2^b}+\sum_{i=1}^{q}\frac{l(l-1)/2}{2^b}+\sum_{i=1}^{q}\sum_{s=1}^{l}\frac{1}{2^r}\left(\mathrm{As}\,I^i_{s-1}=\left(*,T^i\right)\right)\le\frac{(q+\sigma)^2}{2^{b+1}}+\frac{\sigma}{2^r}.\end{aligned} \tag{15}$$

Case 2: if $A^i\ne A^j$ but A^i and A^j have an α-longest common prefix, then $A^i_1\|\cdots\|A^i_\alpha=A^j_1\|\cdots\|A^j_\alpha$ and $A^i_{\alpha+1}\ne A^j_{\alpha+1}$, where $\alpha\ge 0$. We assume that M^i and M^j have a β-longest common prefix, where $\beta\ge 0$. Then, $M^i_1\|\cdots\|M^i_\beta=M^j_1\|\cdots\|M^j_\beta$ and $M^i_{\beta+1}\ne M^j_{\beta+1}$.

Case 2.1: if $\beta\ge\alpha$, then $(A^i_{\alpha+1},M^i_{\alpha+1})\ne(A^j_{\alpha+1},M^j_{\alpha+1})$. Therefore, $I^i_0\|\cdots\|I^i_\alpha=I^j_0\|\cdots\|I^j_\alpha$ and $I^i_{\alpha+1}\ne I^j_{\alpha+1}$. The probability that the event **Coll** occurs is the same with Case 1.

Case 2.2: if $\beta<\alpha$, then $(A^i_{\beta+1},M^i_{\beta+1})\ne(A^j_{\beta+1},M^j_{\beta+1})$. Therefore, $I^i_0\|\cdots\|I^i_\beta=I^j_0\|\cdots\|I^j_\beta$ and $I^i_{\beta+1}\ne I^j_{\beta+1}$. The event **Coll** occurs if one of the following collisions happens:

(1) $I^i_{\beta+1}=I^j_t$ for $t\ne\beta+1$, where $1\le i\ne j\le q$.
(2) $I^i_s=I^j_t$ for $\beta+2\le s\le m^i$ and $1\le t\le m^j$, where $1\le i\ne j\le q$.
(3) $I^i_s=I^i_t$ for $1\le s\ne t\le m^i$, where $1\le i\le q$.

(4) $I_s^i = I_0^i = I_0^j = (N^i, 0)$ for $1 \le s \le m^i$, where $1 \le i \ne j \le q$.

It follows that, in Case 2.2, the probability that the event **Coll** occurs is

$$\begin{aligned}\Pr[\mathbf{Coll}] &= \sum_{1\le i\ne j\le q}\sum_{t\ne\beta+1}\frac{1}{2^b} + \sum_{1\le i\ne j\le q}\sum_{\beta+2\le s\le m^i}\sum_{1\le t\le m^j}\frac{1}{2^b} + \sum_{i=1}^{q}\sum_{1\le s\ne t\le m^i}\frac{1}{2^b} + \sum_{i=1}^{q}\sum_{s=1}^{m^i}\frac{1}{2^r} \\ &\le \sum_{1\le i\ne j\le q}\frac{(l-1)+l(l-2)}{2^b} + \sum_{i=1}^{q}\frac{l(l-1)/2}{2^b} + \sum_{i=1}^{q}\sum_{s=1}^{l}\frac{1}{2^r}\left(\mathrm{As}\, I_{s-1}^i = \left(*, T^i\right)\right) \le \frac{(q+\sigma)^2}{2^{b+1}} + \frac{\sigma}{2^r}.\end{aligned} \tag{16}$$

Summarizing the above mutually exclusive cases, the probability that the event **Coll** occurs is

$$\Pr[\mathbf{Coll}] \le \frac{(q+\sigma)^2}{2^{b+1}} + \frac{\sigma}{2^r}. \tag{17}$$

If the event **Coll** does not occur, all inputs of f are fresh, except that the inputs from the common prefix are equal. Therefore, $\mathscr{E}[f]$ is indistinguishable from \$. In the nonce-misuse setting, we have

$$\mathrm{Adv}^{\mathrm{priv}}_{\Pi[f]}(q,\sigma,p) \le \Pr[\mathbf{Coll}] \le \frac{(q+\sigma)^2}{2^{b+1}} + \frac{\sigma}{2^r}. \tag{18}$$

In the second step, we evaluate the AUTH advantage $\mathrm{Adv}^{\mathrm{auth}}_{\Pi[f]}(q,\sigma,p)$. Assume that the adversary makes q_d nontrivial forgery attempts $(N'^1, A'^1, C'^1, T'^1), \ldots, (N'^{q_d}, A'^{q_d}, C'^{q_d}, T'^{q_d})$ to the decryption oracle $\mathscr{D}[f]$ after querying q_e encryption oracles, where $(N'^1, A'^1, C'^1, T'^1), \ldots, (N'^{q_d}, A'^{q_d}, C'^{q_d}, T'^{q_d}) \notin \{(N^1, A^1, C^1, T^1), \ldots, (N^{q_e}, A^{q_e}, C^{q_e}, T^{q_e})\}$ and $q = q_e + q_d$. Here, we define an event **Forge** that some decryption queries among q_d forgery attempts do not return $\perp$. If the event **Forge** does not occur, the responses of querying $(\mathscr{E}[f], \mathscr{D}[f])$ and $(\$, \perp)$ are identical. Therefore, by the total probability formula, we have

$$\begin{aligned}\mathrm{Adv}^{\mathrm{auth}}_{\Pi[f]}(q,\sigma,p) &\le \Pr[\mathbf{Forge}] \\ &= \Pr[\mathbf{Forge}|\mathbf{Coll}]\Pr[\mathbf{Coll}] \\ &\quad + \Pr[\mathbf{Forge}|\neg\mathbf{Coll}]\Pr[\neg\mathbf{Coll}] \\ &\le \Pr[\mathbf{Coll}] + \Pr[\mathbf{Forge}|\neg\mathbf{Coll}].\end{aligned} \tag{19}$$

The probability that the event **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., $\Pr[\mathbf{Coll}] \le (q+\sigma)^2/2^{b+1} + \sigma/2^r$, where σ is the total query complexity of the encryption and decryption queries.

To compute the probability $\Pr[\mathbf{Forge}|\neg\mathbf{Coll}]$, we consider the following cases:

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

Case 2: T'^i is old, but (N'^i, A'^i, C'^i) is new. We further analyze this case as follows.

Case 2.1: N'^i is new, i.e., $N'^i \notin \{N^1, \ldots, N^{q_e}\}$. 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'^i is at most $1/2^c$.

Case 2.2: N'^i is old, but (A'^i, C'^i) is new. Under the condition of the event $\neg$**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 $1/2^c$.

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

Therefore, according the sugar water inequality $a/b \le a + m/b + m$, where $b > a > 0$ and $m \ge 0$, and $q = q_e + q_d$, we have

$$\begin{aligned}\mathrm{Adv}^{\mathrm{auth}}_{\Pi[f]}(q,\sigma,p) &\le \Pr[\mathbf{Forge}] \\ &\le \Pr[\mathbf{Coll}] + \Pr[\mathbf{Forge}|\neg\mathbf{Coll}] \\ &\le \frac{(q+\sigma)^2}{2^{b+1}} + \frac{\sigma}{2^r} + \frac{q}{2^c}.\end{aligned} \tag{20}$$

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

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

5. Discussions

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

(1) APE$^+$ is a pure permutation-based lightweight online AE mode with concurrent absorption. The rate of

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

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

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 $2^{c/2}$ in the nonce-respecting setting (here, "nonce-respecting" means that the nonce is never repeated in the encryption queries) according to the defect $M_i \oplus C_{i-1}$ [26]. If there exists k such that $M_k \oplus C_{k-1} = M_1 = 0$, the adversary breaks the privacy with a complexity of about $2^{c/2}$ in the nonce-respecting 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 $1 + \max\{\lceil |A|/r \rceil, \lceil |M|/r \rceil\}$ as 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 ensure 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.

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 S. Rasoolzadeh, "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. Abubakr, 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.

[14] N. Yusuke, S. Yu, and S. Takeshi, "Lightweight authenticated encryption mode suitable for threshold implementation," in *Lecture Notes in Computer Science 12106*, C. Anne and I. Yuval, Eds., pp. 705–735, Springer-Verlag, Berlin, Germany, 2020.

[15] B. Andrey, M. Florian, R. Francesco, R. Vincent, and T. Elmar, "ALE: AES-based lightweight authenticated encryption," in *Lecture Notes in Computer Science 8424*, M. Shiho, Ed., pp. 447–466, Springer-Verlag, Berlin, Germany, 2013.

[16] W. E. Daniel, O. S. J. Markku, S. Peter, and M. S. Eric, "The hummingbird-2 lightweight authenticated encryption algorithm," in *Lecture Notes in Computer Science 7055*, M. Shiho, Ed., pp. 19–31, Springer-Verlag, Berlin, Germany, 2011.

[17] E. Andreeva, B. Bilgin, A. Bogdanov et al., "APE: authenticated permutation-based encryption for lightweight cryptography," in *Lecture Notes in Computer Science 8540*, C. Cid and C. Rechberger, Eds., pp. 168–186, Springer-Verlag, Berlin, Germany, 2014.

[18] Y. Sasaki and K. Yasuda, "Optimizing online permutation-based ae schemes for lightweight applications," *IEICE - Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 102, no. 1, pp. 35–47, 2019.

[19] H. Kim and K. Kim, "Preliminary design of a novel lightweight authenticated encryption scheme based on the sponge function," in *Proceedings of the 10th Asia Joint Conference on Information Security*, pp. 110-111, Kaohsiung City, Taiwan, May 2015.

[20] A. Chakraborti, N. Datta, M. Nandi, and K. Yasuda, "Beetle family of lightweight and secure authenticated encryption ciphers," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 2, pp. 218–241, 2018.

[21] P. Zhang and Q. Yuan, "Minimizing key materials: the even-mansour cipher revisited and its application to lightweight authenticated encryption," *Security and Communication Networks*, vol. 2020, Article ID 41801391, 2020.

[22] P. Rogaway and T. Shrimpton, "A provable-security treatment of the key-wrap problem," in *Lecture Notes in Computer Science 4004*, S. Vaudenay, Ed., Springer-Verlag, Berlin, Germany, pp. 373–390, 2006.

[23] C. Namprempre, P. Rogaway, and T. Shrimpton, "Reconsidering generic composition," in *Lecture Notes in Computer Science 8441*, P. Q. Nguyen and E. Oswald, Eds., Springer-Verlag, Berlin, Germany, pp. 257–274, 2014.

[24] R. Granger, P. Jovanovic, B. Mennink, and S. Neves, "Improved masking for tweakable blockciphers with applications to authenticated encryption," in *Lecture Notes in Computer Science 9665*, M. Fischlin and J. S. Coron, Eds., Springer-Verlag, Berlin, Germany, pp. 263–293, 2016.

[25] Y. Sasaki and K. Yasuda, "How to incorporate associated data in sponge-based authenticated encryption," in *Lecture Notes in Computer Science 9048*, K. Nyberg, Ed., Springer-Verlag, Berlin, Germany, pp. 353–370, 2015.

[26] P. Jovanovic, A. Luykx, B. Mennink, Y. Sasaki, and K. Yasuda, "Beyond conventional security in sponge-based authenticated encryption modes," *Journal of Cryptology*, vol. 32, no. 3, pp. 895–940, 2019.