mathematics

MDPI

Article

Polynomial Intermediate Checksum for Integrity under Releasing Unverified Plaintext and Its Application to COPA

Ping Zhang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; zhgp@njupt.edu.cn

Abstract: COPA, introduced by Andreeva et al., is the first online authenticated encryption (AE) mode with nonce-misuse resistance, and it is covered in COLM, which is one of the final CAESAR portfolios. However, COPA has been proven to be insecure in the releasing unverified plaintext (RUP) setting. This paper mainly focuses on the integrity under RUP (INT-RUP) defect of COPA. Firstly, this paper revisits the INT-RUP security model for adaptive adversaries, investigates the possible factors of INT-RUP insecurity for "Encryption-Mix-Encryption"-type checksum-based AE schemes, and finds that these AE schemes with INT-RUP security vulnerabilities utilize a common poor checksum technique. Then, this paper introduces an improved checksum technique named polynomial intermediate checksum (PIC) for INT-RUP security and emphasizes that PIC is a sufficient condition for guaranteeing INT-RUP security for "Encryption-Mix-Encryption"-type checksum-based AE schemes. PIC is generated by a polynomial sum with full terms of intermediate internal states, which guarantees no information leakage. Moreover, PIC ensures the same level between the plaintext and the ciphertext, which guarantees that the adversary cannot obtain any useful information from the unverified decryption queries. Again, based on PIC, this paper proposes a modified scheme COPA-PIC to fix the INT-RUP defect of COPA. COPA-PIC is proven to be INT-RUP up to the birthday-bound security if the underlying primitive is secure. Finally, this paper discusses the properties of COPA-PIC and makes a comparison for AE modes with distinct checksum techniques. The proposed work is of good practical significance. In an interactive system where two parties communicate, the receiver can effectively determine whether the information received from the sender is valid or not, and thus perform the subsequent operation more effectively.

Keywords: authenticated encryption; checksum technique; integrity under releasing unverified plaintext; provable security

MSC: 94A60; 68P25

Citation: Zhang, P. Polynomial Intermediate Checksum for Integrity under Releasing Unverified Plaintext and Its Application to COPA. *Mathematics* **2024**, *12*, 1011. https://doi.org/10.3390/math12071011

Academic Editor: Antanas Cenys

Received: 4 March 2024
Revised: 20 March 2024
Accepted: 26 March 2024
Published: 28 March 2024

1. Introduction

1.1. Background

With the increasing demand for lightweight sensors in the development of space–aerial–ground–sea cooperative information networks, and the scalability, timeliness, and security of the network, lightweight cryptography has been deeply explored in academia and industry. To solve the practical application problems, authenticated encryption (AE) has been extended to lightweight AE, which provides both privacy and authenticity on resource-constrained devices. In conventional security models of AE, the decrypted plaintext must be released after integrity is successfully verified. However, in lightweight devices, there are not enough resources to store the whole decrypted plaintext. Moreover, there exist side channel attacks to obtain the properties of the plaintext indirectly. Thus, releasing the decrypted plaintext before verification (releasing unverified plaintext, RUP) is often desirable and can contribute effectively to the improvement of efficiency in lightweight devices [1–4].

Andreeva et al. introduced stronger security models in the RUP setting [1]. For privacy, they proposed a new notion called PA (Plaintext Awareness). PA, in fact, is a plaintext extractor which tries to deceive adversaries by simulating the decryption oracle. An AE scheme is PA if it is infeasible to distinguish the decryption oracle from the plaintext extractor. For authenticity, they proposed a new notion called INT-RUP (Integrity under Releasing Unverified Plaintext). INT-RUP is a stronger security metric than INT-CTXT (Integrity of Ciphertext). An AE scheme is INT-RUP if an adversary can not generate a fresh valid ciphertext–tag pair given the additional power of access to an unverified decryption oracle, after the encryption oracle. This paper is only interested in INT-RUP security of various AE schemes.

OCB [5–7] and COPA [8] are not INT-RUP. Andreeva et al. presented a forgery attack under the INT-RUP security model and left fixing OCB and COPA to be INT-RUP in an efficient way as an open problem [1]. Zhang et al. focused on the weakness of the checksum processing, described a new generalized checksum technique—PCC (Plaintext and Ciphertext Checksum)—and proved that all AE schemes with PCC are insecure under the INT-RUP security model [9]. To fix the weakness of PCC, they provided an intermediate checksum (IC) technique to generate the authentication tag. Based on the IC technique, they proposed a modified OCB scheme with IC, called OCB-IC, to settle the INT-RUP security of OCB [9,10]. Chakraborti et al. focused on the rate (which means the number of message blocks processed per block of cipher invocation) of block-cipher-based AE schemes to find the cause of INT-RUP insecurity [11]. They considered the weakness during the tag processing, showed a generic INT-RUP attack on a "rate-1" block-cipher-based affine AE mode, described an INT-RUP attack on CPFB (rate-3/4), and presented a variant mCPFB (rate-3/4) which supports INT-RUP security. Zhang and Wu focused on the security of online AE schemes in a RUP setting and looked for the reason of the INT-RUP insecurity of the schemes [12]. They found that if the encryption part of AE schemes has a CCJP (Control Ciphertext to Jump between two Plaintexts) property and the input of the authentication part is built by linear combinations of all plaintext blocks (i.e., the authentication tag is generated by the plaintext checksum), it is easy to make an INT-RUP forgery attack. Datta et al. investigated the integrity of the COLM structure in an RUP setting, rewrote a nonce-respecting INT-RUP forgery attack against COPA's XOR mixing, and presented nonce-respecting and nonce-misusing INT-RUP forgery attacks for any mixing functions [13]. They demonstrated that its security highly depends on the choice of mixing function. Hirose et al. focused on the security of rate-1 AE schemes under RUP [14]. They showed that any rate-1 AE scheme cannot satisfy strong security requirements under RUP and then introduced new strictly weaker security notions of tag-PA and tag-INT by relaxing the security requirements; finally, they presented a new rate-1 AE scheme OCBt which is both tag-PA and tag-INT. They considered the efficiency by rate-1 and full parallelizability and security by robustness against decryption misuse. Chakraborti et al. considered the INT-RUP security of AE schemes under the lightweight application and proposed two lightweight AE modes: LOCUS and LOTUS with higher security and lighter primitives [15]. They utilized the intermediate checksum technique to generate the final authentication tag. In addition to the one-pass AE schemes with INT-RUP security, there exist two-pass AE modes with INT-RUP security. Andreeva et al. considered the INT-RUP security of SIV, HBS, and BTM and proved their INT-RUP security [1]. Chang et al. proposed a lightweight deterministic AE mode ANYDAE and proved that ANYDAE achieves INT-RUP security [16]. Recently, Andreeva et al. focused on the rate-1 online fork AE mode SAEF and showed that SAEF is INT-RUP secure up to the birthday bound by the H-coefficient technique [17]. Datta et al. considered SAEB and TinyJAMBU and presented their integrity security in the setting of a releasing unverified plaintext model [18].

This paper revisits the possible causes which result in INT-RUP insecurity, investigates almost all of the one-pass checksum-based AE schemes [5–8,11,13,19–27], and finds that these AE schemes with INT-RUP security defects utilize a common checksum technique.

This paper focuses on the weakness of the checksum technique and tries to introduce an improved checksum technique to settle the INT-RUP security of COPA.

1.2. Problem Statement

For almost all of the one-pass AE schemes, their checksum is generated by the XOR-sum of all plaintext blocks, which results in INT-RUP insecurity. Andreeva et al. presented a forgery attack with a high probability by making one encryption query and two decryption queries under the INT-RUP security model, and they left fixing COPA to be INT-RUP in an efficient way as an open problem [1].

The IC technique [9,10] is a good technique for settling the INT-RUP security defect of OCB. However, the IC technique cannot be directly applied to COPA. COPA is an authenticated online cipher, which means that the i-block ciphertext just relies on the first i plaintext blocks. In other words, the intermediate checksum in this case only relates to the last ciphertext block. Even if you utilize the encrypted internal states to generate the intermediate checksum, the adversary just needs to keep the last ciphertext block the same to make a successful forgery. In addition, the intermediate parity checksum (IPC) technique [10] was utilized to try to settle the INT-RUP security defect of COPA, but it ultimately failed. The i-block plaintext can be recovered by the $(i-1)$-block ciphertext and the i-block ciphertext, which can be used by adversaries to launch forgery attacks. Therefore, it is necessary to propose a new improved intermediate checksum technique for settling the INT-RUP security defect of COPA.

1.3. Our Contributions

This paper mainly considers the INT-RUP insecurity of COPA and focuses on the weakness of the checksum processing. This paper first revisits the INT-RUP security model which allows for an adaptive adversary to make queries in any order and then introduces a new improved checksum technique: polynomial intermediate checksum (PIC), which is a generalization of IC. In the PIC technique, the intermediate internal states generated by either an encryption or a decryption algorithm are hidden from the adversaries, and PIC is generated by a polynomial sum with full terms of intermediate internal states, which guarantees no information leakage. Moreover, PIC maintains the same level between the plaintext and the ciphertext, which guarantees that the adversary cannot obtain any useful information from the unverified decryption queries. This technique is very effective in solving the INT-RUP security of checksum-based AE schemes. Finally, based on the PIC technique, a modified scheme called COPA-PIC is proposed to fix the INT-RUP security defect of COPA. COPA-PIC retains the main structure and the advantages of COPA.

From the perspective of the design idea, at the beginning, COPA-PIC is designed in terms of tweakable blockciphers (TBCs), as TBC-based AE modes have more advantages than AE modes based on other primitives; particularly, their structure is clear and their proof is simple [19,22,28–31]. In addition, TBCs can also be constructed by distinct primitives. Therefore, a TBC-based COPA-PIC is first illustrated, and then a blockcipher-based TBC and a permutation-based TBC are utilized to further instantiate COPA-PIC.

From the perspective of the security guarantee, COPA-PIC is proven INT-RUP up to the birthday bound of $n/2$-bit security if the underlying primitive (including TBC, block cipher, and permutation) is secure, where n is the block size of the underlying primitive.

From the perspective of the efficiency, the number of underlying primitive invocations of COPA-PIC is less than that of COPA. To be specific, let a be the number of blocks of the associated data and l be the number of blocks of the plaintext. Then, the encryption, decryption, and verification algorithms of COPA-PIC invoke $a+2l+2$, $a+2l+2$, and $a+l+2$ underlying primitives, respectively, while the encryption, decryption, and verification algorithms of COPA invoke $a+2l+2$ underlying primitives. In other words, the encryption and decryption costs of COPA-PIC are the same as those of COPA, but the verification cost of COPA-PIC is close to half of COPA. In practical scenarios, such as an interactive system where two parties communicate, the receiver can first effectively deter-

mine whether the information received from the sender is valid or not, and then perform the decryption operation more effectively to obtain the correct plaintext. Therefore, the efficiency of COPA-PIC is significantly improved in practical applications. The comparison between COPA and COPA-PIC is shown in Table 1.

Table 1. Comparison between COPA and COPA-PIC for a-block associated data and l-block plaintext, where # Encryption, # Decryption, and # Verification, respectively, stand for the number of invoking underlying primitives in the encryption, decryption, and verification algorithms, and n is the block size.

Schemes	Checksum Technique	# Encryption	# Decryption	# Verification
COPA	PCC	$a+2l+2$	$a+2l+2$	$a+2l+2$
COPA-PIC	PIC	$a+2l+2$	$a+2l+2$	$a+l+2$
Schemes	**Security**	**Security Bound**	**Rate**	**Reference**
COPA	INT-CTXT	$O(2^{n/2})$	1/2	[8]
COPA-PIC	INT-RUP	$O(2^{n/2})$	1/2	This paper

The proposed work is of high significance to both theoretical investigations and practical applications. This work supports Zhang and Wu's view that it is easy to make an INT-RUP forgery attack if the encryption part of the AE schemes has a CCJP property and the input of the authentication part is mainly subject to linear combinations of all plaintext blocks [12]. The PIC technique is essentially an improvement of Chakraborti et al.'s technique and covers the IC technique. The PIC technique aims to settle the problem of INT-RUP security for "Encryption-Mix-Encryption"-type checksum-based AE schemes. Moreover, the proposed work also meets the requirements of strong security and high efficiency in lightweight devices in the next-generation network. In particular, it is of good practical significance to establish the rapid feedback mechanism of third-party error authentication.

1.4. Organization of This Paper

Some preliminaries are presented in Section 2. A new polynomial intermediate checksum (PIC) technique is described in Section 3. Section 4 provides a modified scheme COPA-PIC to fix the INT-RUP security defect of COPA and derives its security proof. Finally, this paper concludes with some discussions and a mention of future works in Section 5.

2. Preliminaries

The basic notations and concepts closely follow [9,10]. Some of the important symbols are described in Abbreviations.

Block ciphers. Block cipher is an important part of symmetric-key ciphers, and its standardized algorithms, such as AES or SM4, have been widely used in practice.

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, where $\mathcal{K}$ is a key space and n is the block size. For any $K \in \mathcal{K}$, $E_K(\cdot) = E(K,\cdot)$ is an n-bit permutation. Let $\mathcal{A}$ be an adversary with access to the encryption oracle or encryption and decryption oracles; then, the pseudorandom permutation (PRP) and strong pseudorandom permutation (SPRP) advantages of $\mathcal{A}$ against E are, respectively, defined as

$$Adv_E^{prp}(\mathcal{A}) = |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K} \Rightarrow 1] - Pr[\pi \xleftarrow{\$} Perm(n) : \mathcal{A}^{\pi} \Rightarrow 1]|,$$
$$Adv_E^{sprp}(\mathcal{A}) = |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K^{\pm 1}} \Rightarrow 1] - Pr[\pi \xleftarrow{\$} Perm(n) : \mathcal{A}^{\pi^{\pm 1}} \Rightarrow 1]|.$$

Tweakable blockciphers (TBCs). As the generalization of block ciphers, TBCs have been widely used in the fields of disk encryption, length-preserving encryption, storage encryption, etc. Related works about TBCs include [30,32–39].

Let $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\mathcal{K}$ is a key space and Γ is a tweak space. For any $K \in \mathcal{K}$, $t \in \Gamma$, $\widetilde{E}_K^t(\cdot) = \widetilde{E}(K,t,\cdot)$ is an n-bit permutation. Let $\mathcal{A}$ be an

adversary with access to the tweakable encryption oracle or tweakable encryption and tweakable decryption oracles, then the tweakable PRP (TPRP) and strong TPRP (STPRP) advantages of $\mathcal{A}$ against $\widetilde{E}$ are, respectively, defined as

$$Adv_{\widetilde{E}}^{\widetilde{prp}}(\mathcal{A}) = |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\widetilde{E}_K} \Rightarrow 1] - Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\widetilde{\pi}} \Rightarrow 1]|,$$
$$Adv_{\widetilde{E}}^{\widetilde{sprp}}(\mathcal{A}) = |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\widetilde{E}_K^{\pm 1}} \Rightarrow 1] - Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\widetilde{\pi}^{\pm 1}} \Rightarrow 1]|.$$

The above adversary is just allowed to query the encryption oracle in the tweak space Γ for TPRP, while it is allowed to query both encryption and decryption oracles in the tweak space Γ for STPRP. However, in real life, the encryption part of some cryptographic schemes is allowed to query both encryption and decryption oracles in a subset of tweaks and the authentication part of an associated data is just allowed to query the encryption oracle in another subset of tweaks, such as COPA. Granger et al. introduced a mixed security notion to settle this problem [22]. Consider a partition $\Gamma_0 \cup \Gamma_1 = \Gamma$ of the tweak space into encryption-only tweaks Γ_0 and encryption-and-decryption tweaks Γ_1; then, the mixed TPRP (MTPRP) advantage of $\mathcal{A}$ against $\widetilde{E}$ is defined as

$$Adv_{\widetilde{E}}^{\widetilde{mprp}}(\mathcal{A}) = |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\widetilde{E}_K, \widetilde{E}_K^{\pm 1}} \Rightarrow 1] - Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\widetilde{\pi}, \widetilde{\pi}^{\pm 1}} \Rightarrow 1]|.$$

Note that, here, $\mathcal{A}$ is not allowed to query $\widetilde{E}_K^{-1}$ or $\widetilde{\pi}^{-1}$ for tweaks from Γ_0. In fact, MTPRP covers TPRP if $(\Gamma_0, \Gamma_1) = (\Gamma, \varnothing)$ and STPRP if $(\Gamma_0, \Gamma_1) = (\varnothing, \Gamma)$.

Construction of TBCs. TBCs can be constructed from primitives that are widely used today, such as block ciphers and permutations. In these constructions, since the tweak is an important component of TBCs, it must be instantiated in advance when implementing with block ciphers and permutations. Moreover, considering the application of TBC in the actual modes of operations, the update of the tweak is as simple as possible. In practice, due to the wide application of nonce-based encryption, authentication, and authenticated encryption modes of operations, using a nonce to instantiate a tweak has become a common technical means. Here, we consider a nonce-based instantiation of a tweak space $\Gamma = \mathcal{N} \times \mathcal{I} \times \mathcal{J}$, where $\mathcal{N}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set, and we give two general methods for constructing TBCs as follows.

Method 1: Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. By the XEX* construction [6], a blockcipher-based TBC $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ is built as follows:

$$\widetilde{E}_K^{N,i,j}(x) = E_K(x \oplus \Delta) \text{ and } \widetilde{E}_K^{N,i',j'}(x) = E_K(x \oplus \Delta') \oplus \Delta',$$

where $K \in \mathcal{K}, (N,i,j) \in \Gamma_0, (N,i',j') \in \Gamma_1, \Gamma_0 \cap \Gamma_1 = \varnothing, \Gamma_0 \cup \Gamma_1 \subseteq \Gamma, \Delta = 2^i 3^j L, \Delta' = 2^{i'} 3^{j'} L$, and $L = E_K(N)$.

Method 2: Let $\pi : \{0,1\}^n \to \{0,1\}^n$ be a public n-bit permutation. By the MEM construction [22], a permutation-based TBC $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ is built as follows:

$$\widetilde{E}_K^{N,i,j}(x) = \pi(x \oplus \Delta) \text{ and } \widetilde{E}_K^{N,i',j'}(x) = \pi(x \oplus \Delta') \oplus \Delta',$$

where $K \in \mathcal{K}, (N,i,j) \in \Gamma_0, (N,i',j') \in \Gamma_1, \Gamma_0 \cap \Gamma_1 = \varnothing, \Gamma_0 \cup \Gamma_1 \subseteq \Gamma, \Delta = 2^i 3^j L, \Delta' = 2^{i'} 3^{j'} L$, and $L = \pi(N||K)$.

The security of these two general methods for constructing TBCs is shown in the following lemmas.

Lemma 1 (XEX* [6])**.** *Assume that the adversary makes q construction queries to $\widetilde{E}$ and $\widetilde{E}^{-1}$ and $2^i 3^j \neq 1$ for all $(i,j) \in \mathcal{I} \times \mathcal{J}$. Let $\widetilde{E} = XEX^*[E, 2^{\mathcal{I}} 3^{\mathcal{J}}]$; then,*

$$Adv_{\widetilde{E}}^{\widetilde{mprp}}(q) \leq Adv_E^{sprp}(2q) + 9.5q^2/2^n.$$

Lemma 2 (MEM [22]). *Assume that the adversary makes q construction queries to $\widetilde{E}$ and $\widetilde{E}^{-1}$ and p primitive queries to π and π^{-1} and $2^i3^j \neq 1$ for all $(i,j) \in \mathcal{I} \times \mathcal{J}$. Let $\widetilde{E} = MEM[\pi, 2^{\mathcal{I}}3^{\mathcal{J}}]$; then,*

$$Adv^{\widetilde{mprp}}_{\widetilde{E},\pi}(q,p) \leq 4.5q^2/2^n + 3qp/2^n + p/2^k.$$

Syntax of AE. In the RUP setting, Andreeva et al. introduced a new syntax for AE modes [1]. They divided the conventional decryption algorithm into a decryption algorithm and a verification algorithm so that the decryption algorithm always releases plaintext and the verification algorithm only performs integrity verification. The new syntax of nonce-based AE schemes $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{V})$ consists of an encryption algorithm $\mathcal{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$, a decryption algorithm $\mathcal{D}$: $\mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \to \mathcal{M}$, and a verification algorithm $\mathcal{V} : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \to \top/\bot$, which is described as follows:

$$\begin{aligned}
&\mathcal{E}_K(N, A, M) = (C, T),\\
&\mathcal{D}_K(N, A, C, T) = M,\\
&\mathcal{V}_K(N, A, C, T) = \top/\bot,
\end{aligned}$$

where $K \in \mathcal{K}, N \in \mathcal{N}, A \in \mathcal{H}, M \in \mathcal{M}, C \in \mathcal{C}, T \in \mathcal{T}$, and the symbols $\top$ and $\bot$ indicate the success and failure of integrity verification, respectively.

INT-RUP security model of AE. Let $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{V})$ be a nonce-based AE scheme. Let $K \in \mathcal{K}$ and $\mathcal{A}$ be an adversary which makes at most q queries to $\mathcal{E}_K(\cdot,\cdot,\cdot)$ and $\mathcal{D}_K(\cdot,\cdot,\cdot,\cdot)$, and at most q_v queries to $\mathcal{V}_K(\cdot,\cdot,\cdot,\cdot)$. Assume that $\mathcal{A}$ is an adaptive adversary which can perform encryption and decryption oracle queries in any order. In other words, $\mathcal{A}$ can perform the interleaved queries to $\mathcal{E}_K(\cdot,\cdot,\cdot)$ and $\mathcal{D}_K(\cdot,\cdot,\cdot,\cdot)$. $\mathcal{A}$ forges if at least one forgery attempt in all q_v forgery attempts succeeds. Then, the INT-RUP-advantage of $\mathcal{A}$ against $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{V})$ is defined as

$$Adv^{int-rup}_{\Pi}(\mathcal{A}) = Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \mathcal{V}_K} \, forges].$$

Let $Adv^{int-rup}_{\Pi}(t, q, l, \sigma)$ be the INT-RUP-advantage of the adversary $\mathcal{A}$ against the nonce-based AE scheme Π under the limited running time t, queries q, block length l, query complexity σ, and other resources.

3. Polynomial Intermediate Checksum (PIC) Technique

This paper investigates almost all of the "Encryption-Mix-Encryption"-type checksum-based AE schemes with INT-RUP insecurity, focuses on the weakness of their checksum technique, and tries to introduce an improved checksum technique to settle the INT-RUP insecurity of COPA. This section first introduces a polynomial intermediate checksum (PIC) technique for supporting INT-RUP security and then presents the INT-RUP security of "Encryption-Mix-Encryption"-type AE modes with PIC.

3.1. PIC Technique

The checksum technique used in the previous "Encryption-Mix-Encryption"-type AE modes includes the plaintext checksum (PC), the plaintext and ciphertext checksum (PCC), intermediate checksum (IC), and intermediate parity checksum (IPC). However, these checksum techniques do not always guarantee INT-RUP security for "Encryption-Mix-Encryption"-type AE modes. To always guarantee INT-RUP security for "Encryption-Mix-Encryption"-type AE modes, here, we introduce a new polynomial intermediate checksum (PIC) technique, which is a generalization of IC. As the name suggests, PIC is a full-term polynomial XOR-sum of intermediate internal states. The intermediate internal states are generated by encrypting all of the plaintext blocks or decrypting all of the ciphertext

blocks, which make them hidden from the adversaries. In other words, PIC guarantees no information leakage.

To always guarantee the INT-RUP security, PIC must satisfy the following two conditions simultaneously:

Condition 1. It is generated by all of the plaintext blocks.

Condition 2. It is generated by all of the ciphertext blocks.

The above two conditions are indispensable. **Conditions 1 and 2** show that PIC is constructed by polynomials with full terms and provides the same level for the plaintext and the ciphertext to resist the releasing unverified plaintext attack. What calls for special attention is that PIC must be a polynomial function with full terms of the plaintext blocks, and it must also be a polynomial function with full terms of the ciphertext blocks. Otherwise, leaving the missing term unchanged makes it easy to make a successful forgery. Having the same level between the plaintext and the ciphertext ensures that the adversary cannot obtain any useful information from the unverified decryption queries. In other words, PIC can resist the unverified decryption queries. For "Encryption-Mix-Encryption"-type checksum-based AE schemes, PIC is a sufficient condition for guaranteeing the INT-RUP security.

3.2. INT-RUP Security of "Encryption-Mix-Encryption"-Type AE Modes with PIC

The following mathematical model is utilized to formally describe "Encryption-Mix-Encryption"-type AE modes with PIC.

Let $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\mathcal{K}$ is a key space, $\Gamma = \mathcal{N} \times \mathcal{I} \times \mathcal{J}$ is a tweak space, $\mathcal{N}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set. Let N be a nonce, M be a plaintext, C be a ciphertext, and T be an authentication tag. The overview of "Encryption-Mix-Encryption"-type nonce-based AE modes with PIC is described in Figure 1.

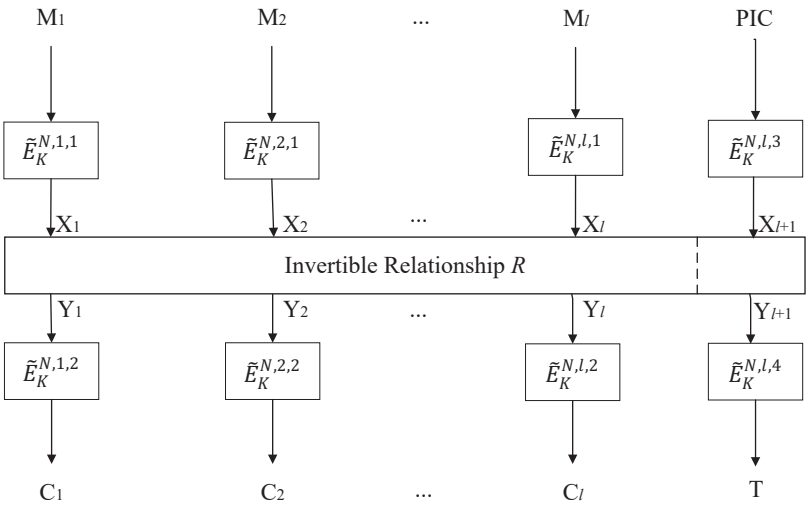

Figure 1. "Encryption-Mix-Encryption"-type nonce-based authenticated encryption modes with polynomial intermediate checksum (PIC).

Let $X_1, X_2, \cdots, X_l$ be the encrypted internal states of the plaintext $M = (M_1, M_2, \cdots, M_l)$ and $Y_1, Y_2, \cdots, Y_l$ be the decrypted internal states of the ciphertext $C = (C_1, C_2, \cdots, C_l)$. There exists some invertible mathematical relationship R between $X_1, X_2, \cdots, X_l$ and

$Y_1, Y_2, \cdots, Y_l$, i.e., $(Y_1, Y_2, \cdots, Y_l) = R(X_1, X_2, \cdots, X_l)$ and for each Y_i, the following equation holds:

$$\begin{aligned} Y_i &= \begin{bmatrix} A_{i1} & A_{i2} & \cdots & A_{il} \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ \cdots \\ X_l \end{bmatrix} \oplus B_i \\ &= A_{i1}X_1 \oplus A_{i2}X_2 \oplus \cdots \oplus A_{il}X_l \oplus B_i \end{aligned}$$

where $A_{ii} \neq 0$ for $1 \leq i \leq l$ and B_i for $1 \leq i \leq l$ are arbitrary constants.

Let $PIC = a_0 \oplus a_1X_1 \oplus \cdots \oplus a_lX_l = b_0 \oplus b_1Y_1 \oplus b_2Y_2 \oplus \cdots \oplus b_lY_l$ be a polynomial intermediate checksum, where $a_i, b_i \neq 0$ for $1 \leq i \leq l$ and a_0, b_0 are arbitrary constants. Then,

$$\begin{aligned} PIC = g(Y_1, Y_2, \cdots, Y_l) &= b_0 \oplus b_1Y_1 \oplus b_2Y_2 \oplus \cdots \oplus b_lY_l \\ &= b_0 \oplus \sum_{i=1}^{l} b_iY_i \\ &= b_0 \oplus \sum_{i=1}^{l} b_i(A_{i1}X_1 \oplus A_{i2}X_2 \oplus \cdots \oplus A_{il}X_l \oplus B_i) \\ &= b_0 \oplus \sum_{i=1}^{l} b_iB_i \oplus \sum_{i=1}^{l} b_iA_{i1}X_1 \oplus \cdots \oplus \sum_{i=1}^{l} b_iA_{il}X_l \\ &= a_0 \oplus a_1X_1 \oplus \cdots \oplus a_lX_l = f(X_1, X_2, \cdots, X_l), \end{aligned}$$

where a_i and b_i $(0 \leq i \leq l)$ satisfy the following relationship:

$$(I) \begin{cases} a_0 = b_0 \oplus \sum_{j=1}^{l} b_jB_j, & i = 0 \\ a_i = \sum_{j=1}^{l} b_jA_{ji}, & 1 \leq i \leq l \end{cases}$$

In particular, if $A_{ij} = 0$ for any $j \neq i$, then $Y_i = A_{ii}X_i \oplus B_i$, where $1 \leq i \leq l$. It follows that the relationship (I) degenerates to

$$(II) \begin{cases} a_0 = b_0 \oplus \sum_{j=1}^{l} b_jB_j, & i = 0 \\ a_i = b_iA_{ii}, & 1 \leq i \leq l \end{cases}$$

OCB-IC [9] is a typical example when $A_{ii} = 1$ and $B_i = 0$. In this case, $Y_i = X_i$ for $1 \leq i \leq l$ and PIC degrades to IC (i.e., $PIC = f(X_1, X_2, \cdots, X_l) = g(Y_1, Y_2, \cdots, Y_l) = X_1 \oplus X_2 \oplus \cdots \oplus X_l = IC$).

If $A_{ij} = 0$ for any $j > i$, then $(Y_1, Y_2, \cdots, Y_l) = R(X_1, X_2, \cdots, X_l)$ is an online function (i.e., Y_i just depends on the first i inputs $X_1, X_2, \cdots, X_i$, where $1 \leq i \leq l$). It follows that, the relationship (I) degenerates to

$$(III) \begin{cases} a_0 = b_0 \oplus \sum_{j=1}^{l} b_jB_j, & i = 0 \\ a_i = \sum_{j=i}^{l} b_jA_{ji}, & 1 \leq i \leq l \end{cases}$$

In this case, authenticated encryption schemes are also called authenticated online ciphers. The typical authenticated online ciphers include ELmE [25], ELmD [24], and COLM [13]. Similar checksum techniques are actually used in their design. To take it one step further, if $A_{i1} = \cdots = A_{ii} = 1, B_i = c$, then $Y_i = X_1 \oplus X_2 \oplus \cdots \oplus X_i \oplus c$ for $1 \leq i \leq l$, where c is an arbitrary constant. In this case, PIC must satisfy the following equation:

$$\begin{aligned} PIC = f(X_1, \cdots, X_l) &= a_0 \oplus a_1X_1 \oplus \cdots \oplus a_lX_l \\ &= g(Y_1, \cdots, Y_l) = b_0 \oplus b_1Y_1 \oplus \cdots \oplus b_lY_l, \end{aligned}$$

where a_i and b_i $(0 \le i \le l)$ satisfy the following relationship:

$$(IV)\begin{cases} a_0 = b_0 \oplus \sum_{j=1}^{l} b_j c, & i = 0 \\ a_i = \sum_{j=i}^{l} b_j = b_i \oplus \cdots \oplus b_l, & 1 \le i \le l \end{cases}$$

Theorem 1. *For "Encryption-Mix-Encryption"-type AE modes with PIC, if PIC is generated by all terms of the plaintext blocks and it can also be generated by all terms of the ciphertext blocks, then the INT-RUP security can be guaranteed.*

Proof. Let $\Pi = (\mathcal{E}_K, \mathcal{D}_K, \mathcal{V}_K)$ be "Encryption-Mix-Encryption"-type AE modes with PIC. Assume that the adversary $\mathcal{A}$ makes q_e encryption queries $\{(N^i, M^i)\}_{i=1}^{q_e}$ to the encryption oracle $\mathcal{E}_K(\cdot,\cdot)$ and receives $(C^i, T^i) = \mathcal{E}_K(N^i, M^i)$, where $1 \le i \le q_e$, and makes q_d decryption queries $\{(N^{*j}, C^{*j}, T^{*j})\}_{j=1}^{q_d}$ to the decryption oracle $\mathcal{D}_K(\cdot,\cdot,\cdot)$ and obtains the unverified plaintext $M^{*j} = \mathcal{D}_K(N^{*j}, C^{*j}, T^{*j})$, where $1 \le j \le q_d$. Note that $(N^{*j}, C^{*j}, T^{*j}) \ne (N^i, C^i, T^i), 1 \le i \le q_e, 1 \le j \le q_d$ and $q_e + q_d = q$. Then, $\mathcal{A}$ forges q_v challenge queries $\{(N'^1, C'^1, T'^1), (N'^2, C'^2, T'^2), \cdots, (N'^{q_v}, C'^{q_v}, T'^{q_v})\} \not\subset \{(N^1, C^1, T^1), \cdots, (N^{q_e}, C^{q_e}, T^{q_e})\}$ to the verification oracle $\mathcal{V}_K(\cdot,\cdot,\cdot)$, where $C'^k = C'^k_1 C'^k_2 \cdots C'^k_{l'^k}, C^i = C^i_1 C^i_2 \cdots C^i_{l^i}, 1 \le k \le q_v, 1 \le i \le q_e$.

All TBCs of Π are replaced with tweakable random permutations to obtain $\Pi[\widetilde{\pi}]$, where $\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n)$ and Γ is a tweak space. Then the INT-RUP-advantage of $\mathcal{A}$ is

$$\begin{aligned} Adv^{int-rup}_{\Pi}(\mathcal{A}) =& Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \mathcal{V}_K} forges] \\ \le& |Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \mathcal{V}_K} forges] - Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\mathcal{E}, \mathcal{D}, \mathcal{V}} forges]| \\ & + Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\mathcal{E}, \mathcal{D}, \mathcal{V}} forges] \\ =& Adv^{\widetilde{mprp}}_{\widetilde{E}}(\mathcal{B}) + Pr[\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n) : \mathcal{A}^{\mathcal{E}, \mathcal{D}, \mathcal{V}} forges] \\ =& Adv^{\widetilde{mprp}}_{\widetilde{E}}(\mathcal{B}) + Adv^{int-rup}_{\Pi[\widetilde{\pi}]}(\mathcal{A}), \end{aligned}$$

where $\mathcal{B}$ is an MTPRP adversary against $\widetilde{E}$.

Let **F** be an event that at least one forgery attempt in all q_v forgery attempts succeeds. Then, the INT-RUP-advantage of $\mathcal{A}$ is

$$Adv^{int-rup}_{\Pi[\widetilde{\pi}]}(\mathcal{A}) = Pr[\mathcal{A}^{\mathcal{E}, \mathcal{D}, \mathcal{V}} forges] = Pr[\mathcal{A}^{\mathcal{E}, \mathcal{D}, \mathcal{V}} sets\ \mathbf{F}] = Pr[\mathbf{F}].$$

Define a collision as the same output from distinct inputs. Let **T** be the event that a collision of the authentication tag occurs for the encryption queries.

With the total probability formula and the probability inequality, one has

$$\begin{aligned} Pr[\mathbf{F}] &= Pr[\mathbf{F} \wedge \neg\mathbf{T}] + Pr[\mathbf{F} \wedge \mathbf{T}] = Pr[\mathbf{F}|\neg\mathbf{T}]Pr[\neg\mathbf{T}] + Pr[\mathbf{F}|\mathbf{T}]Pr[\mathbf{T}] \\ &\le Pr[\mathbf{F}|\neg\mathbf{T}] + Pr[\mathbf{T}]. \end{aligned}$$

Step 1: Bound the probability of event **T** occurring: $Pr[\mathbf{T}] \le \frac{q^2}{2^n}$.

Step 2: Evaluate the upper bound of the probability that event **F** occurs under the condition $\neg\mathbf{T}$: $Pr[\mathbf{F}|\neg\mathbf{T}]$. For simplicity, a single forgery attempt $(N', C', T') \notin \{(N^1, C^1, T^1), \cdots, (N^{q_e}, C^{q_e}, T^{q_e})\}$ is first considered, where C' is divided into l' blocks and C^i is divided into l^i blocks for $1 \le i \le q_e$. Let $\mathcal{T}_e = \{T^1, T^2, \cdots, T^{q_e}\}$ be a set of the authentication tags generated by the encryption oracle (Under the condition $\neg\mathbf{T}$, $T^1, T^2, \cdots, T^{q_e}$ are distinct from each other.).

Case 1: T' is new, i.e., $T' \notin \mathcal{T}_e$. In this case, the adversary $\mathcal{A}$ already knows the value of T^i, where $1 \le i \le q_e$, and with this knowledge, the adversary tries to guess the preimage of another new tag. Therefore, the probability that the adversary $\mathcal{A}$ correctly guesses this

value is at most $1/(2^n - q_e)$, which is also the probability that the adversary's forgery attempt succeeds.

Case 2: T' is old, i.e., $T' \in \mathcal{T}_e$. Let us say $T' = T^u$, where $u \in \{1, \cdots, q_e\}$. According to the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ of the authentication tag generation, a further analysis is discussed as follows.

Case 2-1: If $N' \neq N^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ are new. The adversary tries to forge an identical tag $(T' = T^u)$ using a new nonce N'. The image of a single point under a tweakable random permutation is uniform, so the generated tag is an independent and uniform random value. Thus, the probability that the adversary correctly forges an identical tag $(T' = T^u)$ is $1/2^n$.

Case 2-2: If $N' = N^u$ and $l' \neq l^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ are new. The adversary tries to forge an identical tag $(T' = T^u)$ using a new block-length l'. The image of a single point under a tweakable random permutation is uniform, so the generated tag is an independent and uniform random value. Thus, the probability that the adversary correctly forges an identical tag $(T' = T^u)$ is $1/2^n$.

Case 2-3: If $N' = N^u$ and $l' = l^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ in this case are the same as those of previous query–response pairs (N^u, M^u, C^u, T^u). According to $PIC' = b_0 \oplus b_1 Y'_1 \oplus b_2 Y'_2 \oplus \cdots \oplus b_l Y'_l$, where $Y'_i = (\widetilde{\pi}^{N',i,2})^{-1}(C'_i)$ for all $1 \leq i \leq l'$, a further discussion is shown as follows.

1. C' is new and PIC' is new, i.e., $PIC' \neq PIC^u$. The probability that this case occurs is about $1 - 1/2^n$. The adversary tries to forge an identical tag $(T' = T^u)$ using a new checksum PIC'. Thus, the probability that the adversary's forgery attempt succeeds is $1/2^n$.
2. C' is new and PIC' is old, i.e., $PIC' = PIC^u$. According to the fact that $Pr[b_1 Y'_1 \oplus b_2 Y'_2 \oplus \cdots \oplus b_l Y'_l = c] = 1/2^n$ for any $Y'_1, Y'_2, \cdots, Y'_{l'} \in \{0,1\}^n$, where c is a constant from $\{0,1\}^n$, the probability that PIC' is old is at most $1/2^n$. Therefore, the probability that the adversary can guess the correct value in this case is the probability that PIC' is old, which is at most $1/2^n$.
3. C' is old. This contradicts $(N', C', T') \not\subset \{(N^1, C^1, T^1), \cdots, (N^{q_e}, C^{q_e}, T^{q_e})\}$.

Summarizing all cases above, the successful probability of the single forgery attempt is upper-bounded by

$$max\{1/(2^n - q_e), 1/2^n\} \leq 2/2^n.$$

Therefore, for q_v forgery attempts, it is easy to bound the probability that event **F** occurs under the condition $\neg$**T**:

$$Pr[\mathbf{F}|\neg\mathbf{T}] \leq 2q_v/2^n.$$

The INT-RUP advantage of $\mathcal{A}$, after q encryption and decryption queries, and q_v forgery queries, is

$$Adv_{\Pi}^{int-rup}(\mathcal{A}) \leq Adv_{\widetilde{E}}^{\widetilde{mprp}}(\mathcal{B}) + \frac{q^2}{2^n} + \frac{2q_v}{2^n},$$

where $\mathcal{B}$ is an MTPRP adversary against $\widetilde{E}$. If $\widetilde{E}$ is a secure MTPRP, then Π with PIC guarantees the INT-RUP security. □

Here, PIC just focuses on the authentication of the plaintext. The authentication of the associated data should be included in the verification algorithm. This paper directly utilizes PMAC1 algorithm [6] to generate the authentication of the associated data A, i.e., $c = T_A = PMAC1(A)$. In addition, the associated data can also be treated in a similar way to messages, just saving the final output as its authentication tag.

4. COPA-PIC: COPA with Polynomial Intermediate Checksum for INT-RUP Security

To solve the INT-RUP security defect of COPA, the PIC technique is applied to COPA, and an improved variant, COPA-PIC, is proposed. In this section, the top-level design of COPA-PIC is first described from the angle of TBCs, and then blockcipher-based and permutation-based COPA-PIC instances are presented.

4.1. TBC-Based COPA-PIC: COPA-PIC[$\widetilde{E}$]

At the beginning of the design, the idea was to retain as much of the COPA structure as possible. Therefore, the mainly structure of COPA-PIC is the same as that of COPA except that the plaintext checksum used in the encryption and verification algorithms is replaced with PIC. For PIC, a polynomial sum with full terms of internal intermediate states is utilized to ensure INT-RUP security. Therefore, the verification algorithm and the decryption algorithm of COPA-PIC share parts of computing resources such that the cost of the authentication tag is minimal.

Let $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\mathcal{K}$ is a key space, $\Gamma = \mathcal{N} \times \mathcal{I} \times \mathcal{J}$ is a tweak space, $\mathcal{N}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set. We assume that COPA-PIC takes a key K, a nonce N, associated data A, and a plaintext $M = M_1||M_2||\cdots||M_l$ as input and returns the corresponding ciphertext $C = C_1||C_2||\cdots||C_l$ and an authentication tag T. Then, the checksum of COPA-PIC is $PIC = 2^{l-1}X_1 \oplus 2^{l-2}X_2 \oplus \cdots \oplus 2X_{l-1} \oplus X_l = g(Y_1, Y_2, \cdots, Y_l)$, where $X_i = \widetilde{E}_K^{N,i,1}(M_i)$ and $Y_i = \widetilde{D}_K^{N,i,2}(C_i)$ for all $1 \le i \le l$, and g is a full-term polynomial function. It is essential to call two extra TBCs in the tag-generating process (let $N = N'$ and $M = M'$; then, $PIC = PIC'$; for two distinct associated data $A \neq A'$, if the final authentication tag is generated by calling once extra primitive, we can get the difference in the authentication tag of associated data and the difference in the final authentication tag, which can be easily used to obtain a forgery attack).

The overview of COPA-PIC[$\widetilde{E}$] is shown in Figure 2, and its authentication component of the associated data is depicted in Figure 3. The authentication of associated data utilizes the TBC-based PMAC1 algorithm, which is shown in Algorithm 1. COPA-PIC[$\widetilde{E}$] consists of an encryption algorithm $\mathcal{E}$, a decryption algorithm $\mathcal{D}$, and a verification algorithm $\mathcal{V}$, which are shown in Algorithms 2–4.

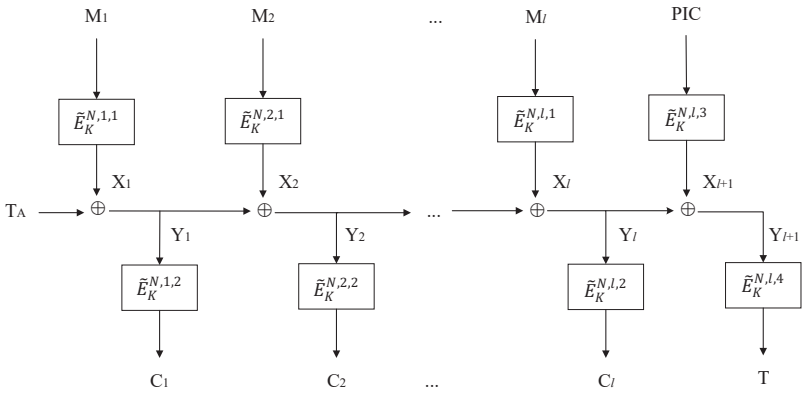

Figure 2. TBC-based COPA-PIC: COPA-PIC[$\widetilde{E}$], where $\widetilde{E}$ is a TBC and T_A is the authentication of associated data A, i.e., $T_A = PMAC1[\widetilde{E}](A)$. If there are no associated data, then set $T_A = 0$.

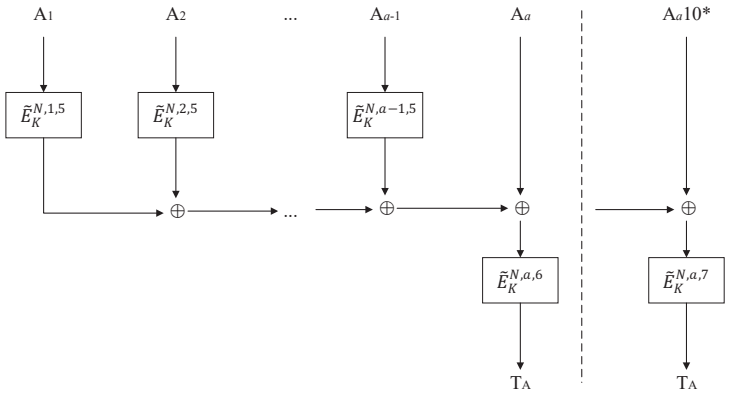

Figure 3. TBC-based PMAC1: PMAC1[$\tilde{E}$].

Algorithm 1 PMAC1 algorithm $PMAC1_K^N(A)$

Input: Key K, nonce N, associated data A;
Output: Tag of associated data T_A;
1: Partition A into $A_1\| \cdots \|A_a$, $|A_i| = n, 1 \le i \le a-1, 0 < |A_a| \le n$;
2: **for** $i = 1$ to $i = a-1$ **do**
3: $S_i \leftarrow \tilde{E}_K^{N,i,5}(A_i)$;
4: **end for**
5: **if** $|A_a| = n$ **then**
6: $\Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a$;
7: $T_A = \tilde{E}_K^{N,a,6}(\Sigma)$;
8: **else**
9: $\Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a 10^*$;
10: $T_A = \tilde{E}_K^{N,a,7}(\Sigma)$;
11: **end if**
12: **return** T_A

Algorithm 2 Encryption algorithm $COPA - PIC.\mathcal{E}_K^N(A, M)$

Input: Key K, nonce N, associated data A, and plaintext M;
Output: Ciphertext C and authentication tag T;
1: Partition M into $M_1\| \cdots \|M_l$, $|M_i| = n, 1 \le i \le l$;
2: $Y_0 = T_A$;
3: **for** $i = 1$ to $i = l$ **do**
4: $X_i \leftarrow \tilde{E}_K^{N,i,1}(M_i)$;
5: $Y_i = Y_{i-1} \oplus X_i$;
6: $C_i \leftarrow \tilde{E}_K^{N,i,2}(Y_i)$;
7: **end for**
8: $PIC \leftarrow 2^{l-1}X_1 \oplus 2^{l-2}X_2 \oplus \cdots \oplus 2X_{l-1} \oplus X_l$;
9: $\Sigma = \tilde{E}_K^{N,l,3}(PIC)$;
10: $T = \tilde{E}_K^{N,l,4}(\Sigma \oplus Y_l)$;
11: **return** $(C_1||C_2|| \cdots ||C_l, T)$

Algorithm 3 Decryption algorithm $COPA - PIC.\mathcal{D}_K^N(A, C, T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Plaintext M;
1: Partition C into $C_1\| \cdots \|C_l$, $|C_i| = n, 1 \le i \le l$;
2: $Y_0 = T_A$;
3: **for** $i = 1$ to $i = l$ **do**
4: $Y_i \leftarrow \tilde{D}_K^{N,i,2}(C_i)$;
5: $X_i = Y_{i-1} \oplus Y_i$;
6: $M_i \leftarrow \tilde{D}_K^{N,i,1}(X_i)$;
7: **end for**
8: **return** $M = M_1||M_2|| \cdots ||M_l$

Algorithm 4 Verification algorithm $COPA-PIC.\mathcal{V}_K^N(A,C,T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Success or failure $\top/\perp$;
Partition C into $C_1\|\cdots\|C_l$, $|C_i|=n, 1\le i\le l$;
$Y_0 = T_A$;
for $i=1$ to $i=l$ **do**
  $Y_i \leftarrow \widetilde{D}_K^{N,i,2}(C_i)$;
end for
$PIC = 2^{l-1}Y_0 \oplus 3\cdot 2^{l-2}Y_1 \oplus 3\cdot 2^{l-3}Y_2 \oplus \cdots \oplus 3Y_{l-1} \oplus Y_l$;
$\Sigma = \widetilde{E}_K^{N,l,3}(PIC)$;
$T' = \widetilde{E}_K^{N,l,4}(\Sigma \oplus Y_l)$;
if $T' = T$ **then**
  return $\top$;
else
  return $\perp$;
end if

For COPA-PIC, we check the correctness as follows:

$$\begin{aligned} PIC =& f(X_1, X_2, \cdots, X_l) = 2^{l-1}X_1 \oplus 2^{l-2}X_2 \oplus \cdots \oplus X_l \\ =& 2^{l-1}(T_A \oplus Y_1) \oplus 2^{l-2}(Y_1 \oplus Y_2) \oplus \cdots \oplus (Y_{l-1} \oplus Y_l) \\ =& 2^{l-1}T_A \oplus 3\cdot 2^{l-2}Y_1 \oplus \cdots \oplus 3Y_{l-1} \oplus Y_l \\ =& g(Y_1, Y_2, \cdots, Y_l). \end{aligned}$$

Thus, PIC is both a polynomial function with full terms of the plaintext blocks and a polynomial function with full terms of the ciphertext blocks, which meets Conditions 1 and 2. Therefore, according to Theorem 1, COPA-PIC[$\widetilde{E}$] ensures INT-RUP security.

Next, the strict INT-RUP security of COPA-PIC[$\widetilde{E}$] is given in the following theorems.

Theorem 2 (INT-RUP security of COPA-PIC based on ideal TBCs)**.** *For COPA-PIC[$\widetilde{E}$], real TBCs are replaced with tweakable random permutations $\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n)$ to obtain COPA-PIC[$\widetilde{\pi}$]. Let $\mathcal{A}$ be a nonce-misusing adversary with q encryption and decryption queries and q_v forgery attempts. Then, one has*

$$Adv^{int-rup}_{COPA-PIC[\widetilde{\pi}]}(\mathcal{A}) \le \frac{q^2}{2^n} + \frac{(l+2)(q-1)^2}{2^n} + \frac{2q_v}{2^n}.$$

Proof. Similar to the proof of Theorem 1, assume that $\mathcal{A}$ makes q_e encryption queries $\{(N^i, A^i, M^i)\}_{i=1}^{q_e}$ to $\mathcal{E}(\cdot,\cdot,\cdot)$ and receives $(C^i, T^i) = \mathcal{E}(N^i, A^i, M^i)$, where $1 \le i \le q_e$, and makes q_d decryption queries $\{(N^{*j}, A^{*j}, C^{*j}, T^{*j})\}_{j=1}^{q_d}$ to $\mathcal{D}(\cdot,\cdot,\cdot,\cdot)$ and obtains the unverified plaintext $M^{*j} = \mathcal{D}(N^{*j}, A^{*j}, C^{*j}, T^{*j})$, where $1 \le j \le q_d$. Note that $(N^{*j}, A^{*j}, C^{*j}, T^{*j}) \ne (N^i, A^i, C^i, T^i), 1 \le i \le q_e, 1 \le j \le q_d$ and $q_e + q_d = q$. Then, $\mathcal{A}$ forges q_v challenge queries $\{(N'^1, A'^1, C'^1, T'^1), (N'^2, A'^2, C'^2, T'^2), \cdots, (N'^{q_v}, A'^{q_v}, C'^{q_v}, T'^{q_v})\} \notin \{(N^1, A^1, C^1, T^1), \cdots, (N^{q_e}, A^{q_e}, C^{q_e}, T^{q_e})\}$ to $\mathcal{V}(\cdot,\cdot,\cdot,\cdot)$, where $C'^k = C'^k_1 C'^k_2 \cdots C'^k_{l'^k}, C^i = C^i_1 C^i_2 \cdots C^i_{l^i}, 1 \le k \le q_v, 1 \le i \le q_e$.

Let **F** be an event that at least one forgery attempt in all q_v forgery attempts succeeds. Then, the INT-RUP-advantage of $\mathcal{A}$ is

$$Adv^{int-rup}_{COPA-PIC[\widetilde{\pi}]}(\mathcal{A}) = Pr[\mathcal{A}^{\mathcal{E},\mathcal{D},\mathcal{V}} \ forges] = Pr[\mathcal{A}^{\mathcal{E},\mathcal{D},\mathcal{V}} \ sets \ \mathbf{F}] = Pr[\mathbf{F}]. \quad (1)$$

Denote variables Y_α of internal state values as $Y_\alpha = \bigoplus_{i=1}^{\alpha} \widetilde{\pi}^{N,i,1}(M_i) \oplus T_A$, which is also equal to $(\widetilde{\pi}^{N,\alpha,2})^{-1}(C_\alpha)$, where $1 \le \alpha \le l$ and T_A is the authentication of the associated data A. Define a collision as the same value Y_α from different prefixes $AM_1M_2\cdots M_\alpha$ and $A'M'_1M'_2\cdots M'_\alpha$. More precisely, $Y_{\alpha-1} \ne Y'_{\alpha-1}$ and $Y_\alpha = Y'_\alpha$, which means $M_\alpha \ne M'_\alpha$. Let **C** be the event that a collision of Y_α occurs for some α. Similarity, let **T** be the event that a collision of the tag occurs for the encryption queries. Let **A** be the event that a collision of

T_A occurs for two different associated data. Let **E** be the union of events **C**, **T**, and **A**; then, $\mathbf{E} = \mathbf{A} \vee \mathbf{C} \vee \mathbf{T}$.

With the total probability formula and the probability inequality, one has

$$Pr[\mathbf{F}] = Pr[\mathbf{F}|\neg\mathbf{E}]Pr[\neg\mathbf{E}] + Pr[\mathbf{F}|\mathbf{E}]Pr[\mathbf{E}] \leq Pr[\mathbf{F}|\neg\mathbf{E}] + Pr[\mathbf{E}]. \quad (2)$$

Step 1: Bound the probability of event **E** occurring: $Pr[\mathbf{E}]$. As COPA-PIC and COPA have the same encryption and decryption structures, the events **E**, **A**, and **C** are exactly the same as those of COPA. Moreover, COPA-PIC and COPA use different methods for generating tags, but their authentication tags are all generated through the randomization of the checksum and the last ciphertext block. The only difference is whether the checksum has been randomized before. This does not make much difference in authentication processing, but it needs to be carefully considered in verification processing. Therefore, the event **T** is exactly the same as that of COPA.

According to two claims $Pr[\mathbf{A}] \leq q^2/2^n$ and $Pr[\mathbf{C} \vee \mathbf{T}|\neg\mathbf{A}] \leq (l+2)(q-1)^2/2^n$ in COPA and the total probability formula, one has

$$Pr[\mathbf{E}] = Pr[\mathbf{A} \vee \mathbf{C} \vee \mathbf{T}] \leq Pr[\mathbf{A}] + Pr[\mathbf{C} \vee \mathbf{T}|\neg\mathbf{A}] \leq q^2/2^n + (l+2)(q-1)^2/2^n. \quad (3)$$

Step 2: Evaluate the upper bound of the probability that event **F** occurs under the condition $\neg\mathbf{E}$: $Pr[\mathbf{F}|\neg\mathbf{E}]$. For simplicity, a single forgery attempt $(N', A', C', T') \notin \{(N^1, A^1, C^1, T^1), \cdots, (N^{q_e}, A^{q_e}, C^{q_e}, T^{q_e})\}$ is considered, where C' is divided into l' blocks and C^i is divided into l^i blocks for $1 \leq i \leq q_e$. Let $\mathcal{T}_e = \{T^1, T^2, \cdots, T^{q_e}\}$ be a set of the authentication tags generated by the encryption oracle.

Case 1: T' is new, i.e., $T' \notin \mathcal{T}_e$. In this case, the adversary $\mathcal{A}$ already knows the value of T^i, where $1 \leq i \leq q_e$, and with this knowledge, the adversary tries to guess the preimage of another new tag. Therefore, the probability that the adversary $\mathcal{A}$ correctly guesses this value is at most $1/(2^n - q_e)$, which is also the probability that the adversary's forgery attempt succeeds.

Case 2: T' is old, i.e., $T' \in \mathcal{T}_e$. Let us say $T' = T^u$, where $u \in \{1, \cdots, q_e\}$. According to the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ of generating the authentication tag, a further analysis should be discussed as follows.

Case 2-1: If $N' \neq N^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ are new. The adversary tries to forge an identical tag ($T' = T^u$) using a new nonce N'. The image of a single point under a tweakable random permutation is uniform, so the generated tag is an independent and uniform random value. Thus, the probability that the adversary correctly forges an identical tag ($T' = T^u$) is $1/2^n$.

Case 2-2: If $N' = N^u$ and $l' \neq l^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ are new. The adversary tries to forge an identical tag ($T' = T^u$) using a new block length l'. The image of a single point under a tweakable random permutation is uniform, so the generated tag is an independent and uniform random value. Thus, the probability that the adversary correctly forges an identical tag ($T' = T^u$) is $1/2^n$.

Case 2-3: If $N' = N^u$ and $l' = l^u$, the last two tweaks $(N', l', 3)$ and $(N', l', 4)$ in this case are the same as those of the previous query–response pair $(N^u, A^u, M^u, C^u, T^u)$. According to $PIC' = 2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} \oplus Y'_{l'}$, where $T'_{A'} = PMAC1(A')$ and $Y'_i = (\widetilde{\pi}^{N',i,2})^{-1}(C'_i)$ for all $1 \leq i \leq l'$, a further discussion should be considered as follows.

1. $A' \neq A^u$. Let $T_{A^i} = PMAC1(A^i)$, where $1 \leq i \leq q_e$. Under the condition that $\neg\mathbf{E}$ ($\neg\mathbf{A}$), $T_{A^1}, T_{A^2}, \cdots, T_{A^{q_e}}$ are distinct from each other. According to $T'_{A'} = PMAC1(A')$, we consider the following two cases.
   (a) $T'_{A'}$ is new, i.e., $T'_{A'} \neq T_{A^u}$. The probability that this case occurs is $1 - 1/2^n$.
      i. $C'_{l'}$ is new. Then, $Y'_{l'}$ is new. The adversary tries to forge an identical tag ($T' = T^u$) using a new ciphertext block $C'_{l'}$. Therefore, the probability that the adversary correctly forges an identical tag ($T' = T^u$) is $1/2^n$.

ii. $C'_{l'}$ is old and C' is new. Then, $Y'_{l'}$ is old and there exists at least one more fresh value in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$. According to whether $PIC' = 2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} \oplus Y'_{l'}$ is new or not, the following subcases are discussed.

- PIC' is new, i.e., $PIC' \neq PIC^u$. The probability that this case occurs is about $1 - 1/2^n$. The adversary tries to forge an identical tag $(T' = T^u)$ using a new checksum PIC'. Thus, the probability that the adversary's forgery attempt succeeds is $(1 - 1/2^n) \times 1/2^n \leq 1/2^n$.
- PIC' is old, i.e., $PIC' = PIC^u$. According to the fact that $Pr[2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus \cdots \oplus 3Y'_{l'-1} = c] = 1/2^n$ for any $T'_{A'}, Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, where c is a constant from $\{0,1\}^n$, the probability that PIC' is old is at most $1/2^n$. As PIC', $Y'_{l'}$, and (N', l') are old, the probability of obtaining an identical tag $(T' = T^u)$ is 1. Therefore, the probability that the adversary can guess the correct value in this case is the probability that PIC' is old, which is at most $1/2^n$.

iii. C' is old. Then, Y'_i is old, where $1 \leq i \leq l'$. According to $PIC' = 2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} \oplus Y'_{l'}$; then, PIC' is a fresh random value. The adversary tries to forge an identical tag $(T' = T^u)$ using new associated data A' (or a new checksum PIC'). Therefore, the probability that the adversary can guess the correct value is $1/2^n$.

Summarizing the cases of (a), the probability that the adversary can guess the correct value is at most $(1 - 1/2^n) \times 1/2^n \leq 1/2^n$.

(b) $T'_{A'}$ is old, i.e., $T'_{A'} = T_{A^u}$. The probability that this case occurs is $1/2^n$.

i. $C'_{l'}$ is new. Then, $Y'_{l'}$ is new. The adversary tries to forge an identical tag $(T' = T^u)$ using a new ciphertext block $C'_{l'}$. Therefore, the probability that the adversary correctly forges an identical tag $(T' = T^u)$ is $1/2^n$.

ii. $C'_{l'}$ is old and C' is new. Then, $Y'_{l'}$ is old and there exists at least one more fresh value in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$. If there only exists one fresh value in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, according to $PIC' = 2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} \oplus Y'_{l'}$, then PIC' is new. Therefore, the probability that the adversary's forgery attempt succeeds is $1/2^n$. If there exist at least two more fresh values in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, according to whether PIC' is new or not, the following subcases are discussed.

- PIC' is new, i.e., $PIC' \neq PIC^u$. The probability that this case occurs is about $1 - 1/2^n$. The adversary tries to forge an identical tag $(T' = T^u)$ using a new checksum PIC'. Thus, the probability that the adversary's forgery attempt succeeds is $(1 - 1/2^n) \times 1/2^n \leq 1/2^n$.
- PIC' is old, i.e., $PIC' = PIC^u$. According to the fact that $Pr[3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} = c] = 1/2^n$ for any $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, where c is a constant from $\{0,1\}^n$, the probability that PIC' is old is at most $1/2^n$. As PIC', $Y'_{l'}$ and (N', l') are old, the probability of obtaining an identical tag $(T' = T^u)$ is 1. Therefore, the probability that the adversary can guess the correct value in this case is the probability that PIC' is old, which is at most $1/2^n$.

iii. C' is old. Then, Y'_i is old, where $1 \leq i \leq l'$. As PIC', $Y'_{l'}$, and (N', l') are old, the probability that the adversary can guess the correct value is 1.

Summarizing the cases of (b), the probability that the adversary can guess the correct value is at most $1/2^n \times \max\{1/2^n, 1\} \leq 1/2^n$.

2. $A' = A^u$; then, $T'_{A'} = T_{A^u}$. As $(N', A', C', T') \notin \{(N^i, A^i, C^i, T^i)\}_{i=1}^{q_e}$; therefore, C' must be new.

(a) $C'_{l'}$ is new. Then, $Y'_{l'}$ is new. The adversary tries to forge an identical tag ($T' = T^u$) using a new ciphertext block $C'_{l'}$. Therefore, the probability that the adversary correctly forges an identical tag ($T' = T^u$) is $1/2^n$.

(b) $C'_{l'}$ is old and C' is new. Then, $Y'_{l'}$ is old and there exists at least one more fresh value in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$.

i. If there only exists one fresh value in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, according to $PIC' = 2^{l'-1}T'_{A'} \oplus 3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} \oplus Y'_{l'}$, then PIC' is new. The adversary tries to forge an identical tag ($T' = T^u$) using a new checksum PIC'. Therefore, the probability that the adversary's forgery attempt succeeds is $1/2^n$.

ii. If there exist at least two more fresh values in $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, according to whether PIC' is new or not, the following subcases are discussed.

- PIC' is new, i.e., $PIC' \neq PIC^u$. The probability that this case occurs is about $1 - 1/2^n$. The adversary tries to forge an identical tag ($T' = T^u$) using a new checksum PIC'. Thus, the probability that the adversary's forgery attempt succeeds is $(1 - 1/2^n) \times 1/2^n \leq 1/2^n$.
- PIC' is old, i.e., $PIC' = PIC^u$. According to the fact that $Pr[3 \cdot 2^{l'-2}Y'_1 \oplus 3 \cdot 2^{l'-3}Y'_2 \oplus \cdots \oplus 3Y'_{l'-1} = c] = 1/2^n$ for any $Y'_1, Y'_2, \cdots, Y'_{l'-1} \in \{0,1\}^n$, where c is a constant from $\{0,1\}^n$, the probability that PIC' is old is at most $1/2^n$. As PIC', $Y'_{l'}$, and (N', l') are old, the probability of obtaining $T' = T^u$ is 1. Therefore, the probability that the adversary can guess the correct value in this case is the probability that PIC' is old, which is at most $1/2^n$.

Summarizing all cases above, the successful probability of the single forgery attempt is upper-bounded by

$$max\{1/(2^n - q_e), 1/2^n\} \leq 2/2^n.$$

Therefore, for q_v forgery attempts, the probability that event **F** occurs under the condition $\neg$**E** is

$$Pr[\mathbf{F}|\neg\mathbf{E}] \leq 2q_v/2^n. \tag{4}$$

Combining Equations (1)–(4), the INT-RUP advantage of $\mathcal{A}$, after q encryption and decryption queries, and q_v forgery queries, is

$$Adv^{int-rup}_{COPA-PIC[\widetilde{\pi}]}(\mathcal{A}) \leq \frac{q^2}{2^n} + \frac{(l+2)(q-1)^2}{2^n} + \frac{2q_v}{2^n}.$$

The proof of Theorem 2 is finished. □

Theorem 3 (INT-RUP security of COPA-PIC based on TBCs). *Let $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\Gamma = \mathcal{N} \times \mathcal{I} \times \mathcal{J}$ is a tweak space, $\mathcal{N}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set. Let $\mathcal{A}$ be a nonce-misusing adversary with q encryption and decryption queries and q_v forgery attempts. For COPA-PIC[$\widetilde{E}$], one has*

$$Adv^{int-rup}_{COPA-PIC[\widetilde{E}]}(t, q+q_v, l, \sigma) \leq Adv^{\widetilde{mprp}}_{\widetilde{E}}(t', 2\sigma) + \frac{q^2}{2^n} + \frac{(l+2)(q-1)^2}{2^n} + \frac{2q_v}{2^n},$$

where $t' = t + cn\sigma$ for some absolute constant c, and l is the maximum block length.

Proof. For COPA-PIC[$\widetilde{E}$], all TBCs are replaced with tweakable random permutations to obtain COPA-PIC[$\widetilde{\pi}$], where $\widetilde{\pi} \xleftarrow{\$} Perm(\Gamma, n)$ and Γ is a tweak space.

Let σ be the total query complexity of message blocks for $(q + q_v)$ queries. According to the MTPRP advantage, COPA-PIC[$\widetilde{E}$] can be replaced with COPA-PIC[$\widetilde{\pi}$], which together cost at most $Adv^{\widetilde{mprp}}_{\widetilde{E}}(t', 2\sigma)$ (here, 2σ comes from the queries of TBCs in the upper and lower layers; in other words, 2σ is the query complexity of TBCs), i.e.,

$$Adv^{int-rup}_{COPA-PIC[\widetilde{E}]}(t, q + q_v, l, \sigma) \leq Adv^{\widetilde{mprp}}_{\widetilde{E}}(t', 2\sigma) + Adv^{int-rup}_{COPA-PIC[\widetilde{\pi}]}(t, q + q_v, l, \sigma). \quad (5)$$

Therefore, combining Equation (5) and Theorem 2, it is easy to obtain the bound of Theorem 3. □

4.2. Blockcipher-Based COPA-PIC Instance: COPA-PIC[E]

Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\mathcal{K}$ is a key space and Γ is a tweak space. This section presents a blockcipher-based instance of COPA-PIC[$\widetilde{E}$] by the XEX* construction $\widetilde{E} = XEX^*[E, 2^{\mathcal{I}}3^{\mathcal{J}}]$ [6] and renames it as COPA-PIC[E].

The overviews of COPA-PIC[E] and blockcipher-based PMAC1 are depicted in Figures 4 and 5, respectively. The blockcipher-based PMAC1 algorithm, and an encryption algorithm $\mathcal{E}_K$, a decryption algorithm $\mathcal{D}_K$, and a verification algorithm $\mathcal{V}_K$ of COPA-PIC[E] are shown in Algorithms 5, 6, 7, and 8, respectively.

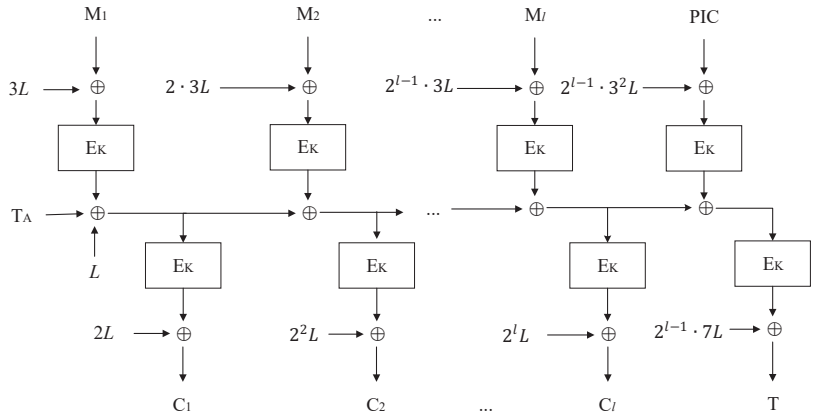

Figure 4. Blockcipher-based COPA-PIC: COPA-PIC[E], where $T_A = PMAC1(A)$ and $L = E_K(N)$.

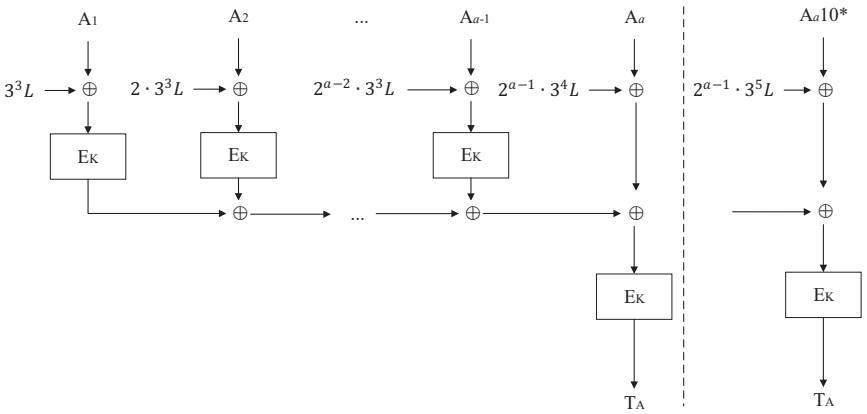

Figure 5. Blockcipher-based PMAC1: $T_A = PMAC1(A)$, where $L = E_K(N)$.

Algorithm 5 Blockcipher-based PMAC1 algorithm $PMAC1[E]_K^N(A)$

Input: Key K, nonce N, associated data A;
Output: Tag of associated data T_A;
Partition A into $A_1\|\cdots\|A_a$, $|A_i| = n, 1 \le i \le a-1, 0 < |A_a| \le n$;
$L = E_K(N)$;
for $i = 1$ to $i = a-1$ **do**
  $S_i \leftarrow E_K(A_i \oplus 2^{i-1} \cdot 3^3 L)$;
end for
if $|A_a| = n$ **then**
  $\Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a$;
  $T_A = E_K(\Sigma \oplus 2^{a-1} \cdot 3^4 L)$;
else
  $\Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a 10^*$;
  $T_A = E_K(\Sigma \oplus 2^{a-1} \cdot 3^5 L)$;
end if
return T_A

Algorithm 6 Encryption algorithm $COPA - PIC[E].\mathcal{E}_K^N(A, M)$

Input: Key K, nonce N, associated data A, and plaintext M;
Output: Ciphertext C and authentication tag T;
Partition M into $M_1\|\cdots\|M_l$, $|M_i| = n, 1 \le i \le l$;
$L = E_K(N)$ and $y_0 = T_A \oplus L$;
for $i = 1$ to $i = l$ **do**
  $x_i \leftarrow E_K(M_i \oplus 2^{i-1} \cdot 3L)$ and X_i=$x_i \oplus 2^{i-1} \cdot 3L$;
  $y_i = y_{i-1} \oplus x_i$ and $Y_i = y_i \oplus 2^i L$;
  $C_i \leftarrow E_K(y_i) \oplus 2^i L$;
end for
$PIC \leftarrow 2^{l-1}X_1 \oplus 2^{l-2}X_2 \oplus \cdots \oplus 2X_{l-1} \oplus X_l$;
$\Sigma = E_K(PIC \oplus 2^{l-1} \cdot 3^2 L)$;
$T = E_K(\Sigma \oplus y_l) \oplus 2^{l-1} \cdot 7L$;
return $(C_1||C_2||\cdots||C_l, T)$

Algorithm 7 Decryption algorithm $COPA - PIC[E].\mathcal{D}_K^N(A, C, T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Plaintext M;
Partition C into $C_1\|\cdots\|C_l$, $|C_i| = n, 1 \le i \le l$;
$L = E_K(N)$ and $y_0 = T_A \oplus L$;
for $i = 1$ to $i = l$ **do**
  $y_i \leftarrow D_K(C_i \oplus 2^i L)$;
  $x_i = y_{i-1} \oplus y_i$;
  $M_i \leftarrow D_K(x_i) \oplus 2^{i-1} \cdot 3L$;
end for
return $M = M_1||M_2||\cdots||M_l$

Theorem 4 (INT-RUP security of COPA-PIC based on block ciphers). *Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $\widetilde{E} : \mathcal{K} \times \Gamma \times \{0,1\}^n \to \{0,1\}^n$ be a TBC, where $\mathcal{K}$ is a key space, $\Gamma = \mathcal{N} \times \mathcal{I} \times \mathcal{J}$ is a tweak space, $\mathcal{N}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set. Let $\widetilde{E} = XEX^*[E, 2^{\mathcal{I}}3^{\mathcal{J}}]$ and assume that $2^i 3^j \neq 1$ for all $(i,j) \in \mathcal{I} \times \mathcal{J}$. Then, for a nonce-misusing adversary $\mathcal{A}$, one has*

$$Adv^{int-rup}_{COPA-PIC[E]}(\mathcal{A}) \le Adv^{sprp}_{E}(\mathcal{B}) + \frac{39(\sigma+q)^2}{2^n} + \frac{(l+2)(q-1)^2}{2^n} + \frac{2q_v}{2^n},$$

where a new adversary $\mathcal{B}$ has an additional running time equal to the time needed to process the queries from $\mathcal{A}$.

Proof. The security proof includes two steps. First, COPA-PIC[E] is converted to COPA-PIC[$\widetilde{E}$]. The dummy masks $\{3L, 2 \cdot 3L, \cdots, 2^{l-1} \cdot 3L, 2^{l-1} \cdot 3^2 L\}$ and $\{2L, 2^2 L, \cdots, 2^l \cdot L, 2^{l-1} \cdot 7L\}$ are introduced to the upper and lower layers of COPA-PIC[E], respectively, in terms of the XEX* construction, where $L = E_K(N)$. Therefore, distinct TBCs $\widetilde{E}_K^{N,i,1}$, $\widetilde{E}_K^{N,i,2}$, $\widetilde{E}_K^{N,l,3}$, and $\widetilde{E}_K^{N,l,4}$ are utilized to replace the block ciphers with distinct masks, where $i = 1, \cdots, l$. For the blockcipher-based PMAC1, distinct TBCs $\widetilde{E}_K^{N,i,5}$, $\widetilde{E}_K^{N,a,6}$, and $\widetilde{E}_K^{N,a,7}$ are utilized to replace the block ciphers with distinct masks, where $i = 1, \cdots, a-1$. According to Lemma 1 and the blockcipher-based PMAC1 [6], COPA-PIC[E] can be replaced with COPA-PIC[$\widetilde{E}$], which together cost

$$\frac{9.5(2\sigma + 2q)^2}{2^n} + Adv_E^{sprp}(t', 2 \cdot 2(\sigma + q)) + \frac{\sigma^2}{2^n} \tag{6}$$

Then, combining Equation (6) and Theorem 3, the bound of Theorem 4 is obtained. □

Algorithm 8 Verification algorithm $COPA - PIC[E].\mathcal{V}_K^N(A, C, T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Success or failure $\top / \bot$;
1: Partition C into $C_1 \| \cdots \| C_l$, $|C_i| = n, 1 \le i \le l$;
2: $L = E_K(N)$ and $Y_0 = T_A$;
3: **for** $i = 1$ to $i = l$ **do**
4: $\quad y_i \leftarrow D_K(C_i \oplus 2^i L)$ and $Y_i = y_i \oplus 2^i L$;
5: **end for**
6: $PIC = 2^{l-1} Y_0 \oplus 3 \cdot 2^{l-2} Y_1 \oplus 3 \cdot 2^{l-3} Y_2 \oplus \cdots \oplus 3 Y_{l-1} \oplus Y_l$;
7: $\Sigma = E_K(PIC \oplus 2^{l-1} \cdot 3^2 L)$;
8: $T' = E_K(\Sigma \oplus y_l) \oplus 2^{l-1} \cdot 7L$;
9: **if** $T' = T$ **then**
10: $\quad$ **return** $\top$;
11: **else**
12: $\quad$ **return** $\bot$;
13: **end if**

4.3. Permutation-Based COPA-PIC Instance: COPA-PIC[π]

Let $\pi : \{0,1\}^n \to \{0,1\}^n$ be a public n-bit permutation, $\mathcal{K} = \{0,1\}^k$ be a set of k-bit keys, $\mathcal{T} = \{0,1\}^{n-k} \times \mathcal{I} \times \mathcal{J}$ be a tweak space, $\mathcal{I}$ be a set of large integers, and $\mathcal{J}$ be a set of small integers, we reload COPA-PIC[$\widetilde{E}$] by $\widetilde{E} = MEM[\pi, 2^{\mathcal{I}} 3^{\mathcal{J}}]$ [22] to obtain an instance called COPA-PIC[π].

Let K, N, A, M, C, and T be the key, the nonce, the associated data, the plaintext, the ciphertext, and the authentication tag, respectively. The overviews of COPA-PIC[π] and PMAC1 are depicted in Figures 6 and 7, respectively. The PMAC1 algorithm and an encryption algorithm $\mathcal{E}_K$, a decryption algorithm $\mathcal{D}_K$, and a verification algorithm $\mathcal{V}_K$ of COPA-PIC[π] are shown in Algorithms 9, 10, 11, and 12, respectively.

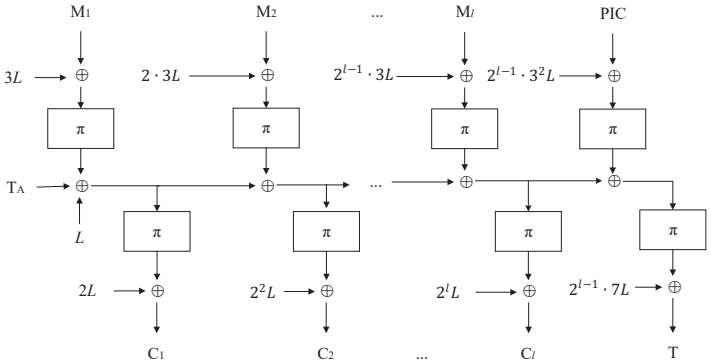

Figure 6. Permutation-based COPA-PIC: COPA-PIC[π], where $T_A = PMAC1[\pi](A)$ and $L = \pi(N||K)$.

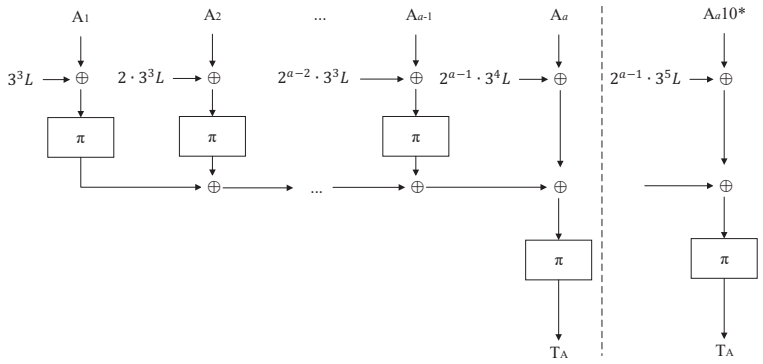

Figure 7. Permutation-based PMAC1: $T_A = PMAC1[\pi](A)$, where $L = \pi(N||K)$.

Algorithm 9 Permutation-based PMAC1 algorithm $PMAC1[\pi]^N_K(A)$

Input: Key K, nonce N, associated data A;
Output: Tag of associated data T_A;
1: Partition A into $A_1\| \cdots \|A_a$, $|A_i| = n, 1 \le i \le a-1, 0 < |A_a| \le n$;
2: $L = \pi(N||K)$;
3: **for** $i = 1$ to $i = a-1$ **do**
4: $\quad S_i \leftarrow \pi(A_i \oplus 2^{i-1} \cdot 3^3 L)$;
5: **end for**
6: **if** $|A_a| = n$ **then**
7: $\quad \Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a$;
8: $\quad T_A = \pi(\Sigma \oplus 2^{a-1} \cdot 3^4 L)$;
9: **else**
10: $\quad \Sigma \leftarrow S_1 \oplus S_2 \oplus \cdots \oplus S_{a-1} \oplus A_a 10^*$;
11: $\quad T_A = \pi(\Sigma \oplus 2^{a-1} \cdot 3^5 L)$;
12: **end if**
13: **return** T_A

Algorithm 10 Encryption algorithm $COPA - PIC[\pi].\mathcal{E}^N_K(A, M)$

Input: Key K, nonce N, associated data A, and plaintext M;
Output: Ciphertext C and authentication tag T;
1: Partition M into $M_1\| \cdots \|M_l$, $|M_i| = n, 1 \le i \le l$;
2: $L = \pi(N||K)$ and $y_0 = T_A \oplus L$;
3: **for** $i = 1$ to $i = l$ **do**
4: $\quad x_i \leftarrow \pi(M_i \oplus 2^{i-1} \cdot 3L)$ and X_i=$x_i \oplus 2^{i-1} \cdot 3L$;
5: $\quad y_i = y_{i-1} \oplus x_i$ and $Y_i = y_i \oplus 2^i L$;
6: $\quad C_i \leftarrow \pi(y_i) \oplus 2^i L$;
7: **end for**
8: $PIC \leftarrow 2^{l-1} X_1 \oplus 2^{l-2} X_2 \oplus \cdots \oplus 2X_{l-1} \oplus X_l$;
9: $\Sigma = \pi(PIC \oplus 2^{l-1} \cdot 3^2 L)$;
10: $T = \pi(\Sigma \oplus y_l) \oplus 2^{l-1} \cdot 7L$;
11: **return** $(C_1||C_2|| \cdots ||C_l, T)$

Algorithm 11 Decryption algorithm $COPA - PIC[\pi].\mathcal{D}^N_K(A, C, T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Plaintext M;
1: Partition C into $C_1\| \cdots \|C_l$, $|C_i| = n, 1 \le i \le l$;
2: $L = \pi(N||K)$ and $y_0 = T_A \oplus L$;
3: **for** $i = 1$ to $i = l$ **do**
4: $\quad y_i \leftarrow \pi^{-1}(C_i \oplus 2^i L)$;
5: $\quad x_i = y_{i-1} \oplus y_i$;
6: $\quad M_i \leftarrow \pi^{-1}(x_i) \oplus 2^{i-1} \cdot 3L$;
7: **end for**
8: **return** $M = M_1||M_2|| \cdots ||M_l$

Algorithm 12 Verification algorithm $COPA-PIC[\pi].\mathcal{V}_K^N(A,C,T)$

Input: Key K, nonce N, associated data A, ciphertext C, and authentication tag T;
Output: Success or failure $\top/\perp$;
1: Partition C into $C_1\|\cdots\|C_l$, $|C_i|=n, 1\le i\le l$;
2: $L=\pi(N||K)$ and $Y_0=T_A$;
3: **for** $i=1$ to $i=l$ **do**
4: $\quad y_i\leftarrow\pi^{-1}(C_i\oplus 2^iL)$ and $Y_i=y_i\oplus 2^iL$;
5: **end for**
6: $PIC=2^{l-1}Y_0\oplus 3\cdot 2^{l-2}Y_1\oplus 3\cdot 2^{l-3}Y_2\oplus\cdots\oplus 3Y_{l-1}\oplus Y_l$;
7: $\Sigma=\pi(PIC\oplus 2^{l-1}\cdot 3^2L)$;
8: $T'=\pi(\Sigma\oplus y_l)\oplus 2^{l-1}\cdot 7L$;
9: **if** $T'=T$ **then**
10: $\quad$ **return** $\top$;
11: **else**
12: $\quad$ **return** $\perp$;
13: **end if**

For an INT-RUP security model with a permutation, the adversary is allowed to make $\pi^{\pm1}$ queries in addition to the previous oracle queries; then, the INT-RUP-advantage of $\mathcal{A}$ against $\Pi=(\mathcal{E},\mathcal{D},\mathcal{V})$ is defined as

$$Adv_{\Pi}^{int-rup}(\mathcal{A})=Pr[K\xleftarrow{\$}\mathcal{K}:\mathcal{A}^{\mathcal{E}_K,\mathcal{D}_K,\mathcal{V}_K;\pi^{\pm1}}\ forges].$$

Theorem 5 (INT-RUP security of COPA-PIC based on permutations)**.** *Let $\pi:\{0,1\}^n\to\{0,1\}^n$ be a public n-bit permutation and $\widetilde{E}:\mathcal{K}\times\Gamma\times\{0,1\}^n\to\{0,1\}^n$ be a TBC, where $\mathcal{K}=\{0,1\}^k$ is a key space, $\Gamma=\mathcal{N}\times\mathcal{I}\times\mathcal{J}$ is a tweak space, $\mathcal{N}=\{0,1\}^{n-k}$ is a nonce space, $\mathcal{I}$ is a large-integer set, and $\mathcal{J}$ is a small-integer set. Assume that $2^i3^j\neq1$ for all $(i,j)\in\mathcal{I}\times\mathcal{J}$. Let $\widetilde{E}=MEM[\pi,2^{\mathcal{I}}3^{\mathcal{J}}]$. For a nonce-misusing adversary $\mathcal{A}$, one has*

$$Adv_{COPA-PIC[\pi]}^{int-rup}(\mathcal{A})\le\frac{19(\sigma+q)^2}{2^n}+\frac{6(\sigma+q)p}{2^n}+\frac{p}{2^k}+\frac{(l+2)(q-1)^2}{2^n}+\frac{2q_v}{2^n}.$$

Proof. Similar to the proof of Theorem 4, the security proof includes two steps. First, COPA-PIC[π] is converted to COPA-PIC[$\widetilde{E}$]. The dummy masks $\{3L,2\cdot3L,\cdots,2^{l-1}\cdot3L,2^{l-1}\cdot3^2L\}$ and $\{2L,2^2L,\cdots,2^l\cdot L,2^{l-1}\cdot7L\}$ are introduced to the upper and lower layers of COPA-PIC[π], respectively, in terms of the MEM construction, where $L=\pi(N||K)$. Therefore, distinct TBCs $\widetilde{E}_K^{N,i,1}$, $\widetilde{E}_K^{N,i,2}$, $\widetilde{E}_K^{N,l,3}$, and $\widetilde{E}_K^{N,l,4}$ are utilized to replace permutations with distinct masks, where $i=1,\cdots,l$. For the permutation-based PMAC1, distinct TBCs $\widetilde{E}_K^{N,i,5}$, $\widetilde{E}_K^{N,a,6}$, and $\widetilde{E}_K^{N,a,7}$ are utilized to replace permutations with distinct masks, where $i=1,\cdots,a-1$. According to Lemma 2 and the permutation-based PMAC1 [6], COPA-PIC[π] can be replaced with COPA-PIC[$\widetilde{E}$], which together cost

$$\frac{4.5(2\sigma+2q)^2}{2^n}+\frac{3(2\sigma+2q)p}{2^n}+\frac{p}{2^k}+\frac{\sigma^2}{2^n}=\frac{18(\sigma+q)^2}{2^n}+\frac{6(\sigma+q)p}{2^n}+\frac{p}{2^k}+\frac{\sigma^2}{2^n}. \quad (7)$$

Then, combining Equation (7) and Theorem 3, the bound of Theorem 5 is obtained. □

5. Discussions and Future Works

COPA-PIC is a secure "rate-1/2" parallelizable delayed authenticated online cipher with nonce-misuse resistance. The structure of COPA-PIC is the same as that of COPA except that the authentication checksum is replaced with PIC. Therefore, COPA-PIC inherits all the advantages of COPA and calculates the authentication tag ahead of time in the verification oracle. It can be viewed as an instance of the generic B1 scheme introduced by Namprempre et al. [40]. At the beginning of the design, TBCs are used to improve COPA from the perspective of a top-level design, and the updating of the tweaks is as simple as possible. Then, by using the XEX* construction [6] and the MEM construction [22], provably secure block-cipher-based and permutation-based instances are presented. For the update of tweaks, a simple and efficient technique—point doubling is used to update tweaks.

This technique follows the framework of the XEX* and MEM constructions, which makes proposed instances and proofs very simple. This paper considers the message whose length is a positive multiple of the block size n. In fact, for any length message, it also works.

There have been many studies on COPA in recent years [1,13,41,42]. Among them, the INT-RUP security is one of the most important research contents. COPA-PIC enjoys INT-RUP security up to the birthday bound in the nonce-misuse setting if the underlying primitive (including TBC, block cipher, and permutation) is secure. Of course, COPA-PIC just settles the problem of INT-RUP in the nonce-misuse setting, while the problem of privacy in the RUP setting still exists. It is left as an open problem to settle the privacy of COPA-PIC in the RUP setting.

COPA-PIC utilizes a new checksum technique—polynomial intermediate checksum (PIC)—to fix the INT-RUP security. PIC is a very vital technique which guarantees no information leakage and the same level between the plaintext and the ciphertext. In the AE schemes with PIC, the adversary cannot obtain any useful information to make a successful forgery even if given the additional power of access to an unverified decryption oracle. mCPFB with INT-RUP security combines a distance 4 error correcting code and delayed dislocation technique which is essentially a similar PIC technique. LOCUS and LOTUS are based on OCB and OTR, and their final checksum utilizes IC, which is a degenerated version of PIC. Table 2 shows the comparison of AE modes with distinct checksum techniques. Our work finds a new technique, PIC, and we believe that PIC can settle the INT-RUP security defects of any "rate < 1" and "Encryption-Mix-Encryption"-type checksum-based AE schemes. In addition, the mixing function of COLM (ELmE/ELmD) essentially provides an implementation of PIC for the authentication part, but COLM (ELmE/ELmD) also utilizes PCC in the authentication part. In fact, COLM (ELmE/ELmD) could have been designed entirely using PIC.

Table 2. Comparison of AE modes with distinct checksum techniques.

Scheme	Security	Checksum Technique	Rate	Reference
OCB	INT-CTXT	PCC	1	[5–7]
CPFB	INT-CTXT	PCC	3/4	[11]
COPA	INT-CTXT	PCC	1/2	[8]
OCBt	tag-INT	PCC	1	[14]
OCB-IC	INT-RUP	IC	1/2	[9]
mCPFB	INT-RUP	similar PIC	3/4	[11]
COLM	INT-RUP	PIC	1/2	[13]
LOCUS	INT-RUP	IC	1/2	[15]
LOTUS	INT-RUP	IC	1/2	[15]
COPA-PIC	INT-RUP	PIC	1/2	This paper

The proposed work is of high practical significance to establish a rapid feedback mechanism for third-party error authentication. The computational costs of COPA-PIC's encryption and decryption algorithms are about the same as those of COPA, but the verification cost is close to one half of COPA (see Table 1). Thus, in practical applications, the receiver first verifies whether the received message is valid or not, and then determines whether to perform the next action (decrypt and obtain the correct plaintext or reject and return an error symbol). The proposed work supports Chakraborti et al.'s works and Zhang and Wu's views, introduces a new intermediate checksum technique, PIC, and gives a possible direction for settling the security of all one-pass checksum-based AE schemes in the RUP setting. Recently, Andreeva et al. focused on SAEF which is a rate-1 online AE mode using a forkcipher as a building block, and they showed that SAEF is INT-RUP-secure up to the birthday bound by the H-coefficient technique [17]. Therefore, forkcipher is a hot future research direction. Additionally, there have been some achievements in RUP security for two-pass AE schemes in recent years, such as GCM-RUP [43] and its variant [44]. This is also a direction to watch in the future.

Funding: This work was supported by National Natural Science Foundation of China (Grant Nos. 61902195, 62272238 and U23B2002) and NUPTSF (Grant Nos. NY219131 and NY2019004).

Data Availability Statement: The data used to support the findings of the study are available within the article.

Acknowledgments: I am grateful to Peng Wang and Honggang Hu et al. for providing some good suggestions on PIC and COPA-PIC. I would also like to express my sincere thanks to the editors and the anonymous reviewers for the valuable comments and suggestions.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

$\mathcal{K}$	the nonempty set of keys (the key space)
Γ	the nonempty set of tweaks (the tweak space)
$\mathcal{N}$	the nonempty set of nonces (the nonce space)
$\mathcal{H}$	the nonempty set of associated data (the associated data space)
$\mathcal{M}$	the nonempty set of plaintexts (the plaintext space)
$\mathcal{C}$	the nonempty set of ciphertexts (the ciphertext space)
$\mathcal{T}$	the nonempty set of authentication tags (the authentication tag space)
E_K	the encryption of block ciphers with a key K
D_K, E_K^{-1}	the decryption of block ciphers with a key K
$E_K^{\pm 1}$	the encryption and decryption oracles of block ciphers with a key K
$\widetilde{E}_K$	the encryption of tweakable blockciphers with a key K
$\widetilde{D}_K, \widetilde{E}_K^{-1}$	the decryption of tweakable blockciphers with a key K
$\widetilde{E}_K^{\pm 1}$	the encryption and decryption oracles of tweakable blockciphers with a key K
$Perm(n)$	the set of all n-bit permutations
$\pi^{\pm 1}$	the permutation and its inverse
$Perm(\Gamma, n)$	the set of all n-bit tweakable permutations with the tweak space Γ
$\widetilde{\pi}^{\pm 1}$	the tweakable permutation and its inverse
$\{0,1\}^*$	the set containing all finite bit strings (including the empty string)
$\{0,1\}^n$	the nonempty set containing all n-bit strings
$\mathcal{A}^O \Rightarrow 1$	the adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O
$x \xleftarrow{\$} X$	the value x randomly chosen from the set X
$Pr[\mathbf{A}]$	the probability of the event $\mathbf{A}$
$\mathcal{E}$	the encryption algorithm
$\mathcal{D}$	the decryption algorithm
$\mathcal{V}$	the verification algorithm
$\lvert x \rvert$	the bit length of the finite string x
$x \Vert y$ or xy	the concatenation of two finite strings x and y
$\oplus$	the XOR/addition operation over the finite field $GF(2^n)$
$\cdot$	the multiplication operation over the finite field $GF(2^n)$
$\mathcal{I}$	a set of large integers, such as $\mathcal{I} = \{0, 1, 2, \cdots, 2^n - 1\}$
$\mathcal{J}$	a set of small integers, such as $\mathcal{J} = \{0, 1, \cdots, 10\}$

References

1. Andreeva, E.; Bogdanov, A.; Luykx, A.; Mennink, B.; Mouha, N.; Yasuda, K. How to Securely Release Unverified Plaintext in Authenticated Encryption. In Proceedings of the Advances in Cryptology-ASIACRYPT 2014-20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, 7–11 December 2014; Sarkar, P., Iwata, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8873, pp. 105–125. [CrossRef]
2. Vaudenay, S. Security Flaws Induced by CBC Padding-Applications to SSL, IPSEC, WTLS. In Proceedings of the Advances in Cryptology-EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002; Knudsen, L.R., Ed.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2332, pp. 534–546. [CrossRef]

3. Canvel, B.; Hiltgen, A.P.; Vaudenay, S.; Vuagnoux, M. Password Interception in a SSL/TLS Channel. In Proceedings of the Advances in Cryptology-CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; Boneh, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 583–599. [CrossRef]
4. AlFardan, N.J.; Paterson, K.G. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, 19–22 May 2013; pp. 526–540. [CrossRef]
5. Rogaway, P.; Bellare, M.; Black, J. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.* **2003**, *6*, 365–403. [CrossRef]
6. Rogaway, P. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Proceedings of the Advances in Cryptology-ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Republic of Korea, 5–9 December 2004; Lee, P.J., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3329, pp. 16–31. [CrossRef]
7. Krovetz, T.; Rogaway, P. The Software Performance of Authenticated-Encryption Modes. In Proceedings of the Fast Software Encryption-18th International Workshop, FSE 2011, Lyngby, Denmark, 13–16 February 2011; Joux, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6733, pp. 306–327. [CrossRef]
8. Andreeva, E.; Bogdanov, A.; Luykx, A.; Mennink, B.; Tischhauser, E.; Yasuda, K. Parallelizable and Authenticated Online Ciphers. In Proceedings of the Advances in Cryptology-ASIACRYPT 2013-19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, 1–5 December 2013; Sako, K., Sarkar, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8269, pp. 424–443. [CrossRef]
9. Zhang, P.; Wang, P.; Hu, H.; Cheng, C.; Kuai, W. INT-RUP Security of Checksum-Based Authenticated Encryption. In Proceedings of the Provable Security-11th International Conference, ProvSec 2017, Xi'an, China, 23–25 October 2017; Okamoto, T., Yu, Y., Au, M.H., Li, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10592, pp. 147–166. [CrossRef]
10. Zhang, P.; Wang, P.; Hu, H. The INT-RUP Security of OCB with Intermediate (Parity) Checksum. *IACR Cryptol. ePrint Arch.* **2016**, 1059. Available online: https://eprint.iacr.org/2016/1059 (accessed on 25 March 2024).
11. Chakraborti, A.; Datta, N.; Nandi, M. INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes. In Proceedings of the Topics in Cryptology-CT-RSA 2016-The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, 29 February–4 March 2016; Sako, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9610, pp. 39–54. [CrossRef]
12. Zhang, J.; Wu, W. Security of Online AE Schemes in RUP Setting. In Proceedings of the Cryptology and Network Security-15th International Conference, CANS 2016, Milan, Italy, 14–16 November 2016; Foresti, S., Persiano, G., Eds.; 2016; Volume 10052, pp. 319–334. [CrossRef]
13. Datta, N.; Luykx, A.; Mennink, B.; Nandi, M. Understanding RUP Integrity of COLM. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 143–161. [CrossRef]
14. Hirose, S.; Sasaki, Y.; Yasuda, K. Rate-One AE with Security Under RUP. In Proceedings of the Information Security-20th International Conference, ISC 2017, Ho Chi Minh City, Vietnam, 22–24 November 2017; Nguyen, P.Q., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10599, pp. 3–20. [CrossRef]
15. Chakraborti, A.; Datta, N.; Jha, A.; Mancillas-López, C.; Nandi, M.; Sasaki, Y. INT-RUP Secure Lightweight Parallel AE Modes. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 81–118. [CrossRef]
16. Chang, D.; Datta, N.; Dutta, A.; Mennink, B.; Nandi, M.; Sanadhya, S.; Sibleyras, F. Release of Unverified Plaintext: Tight Unified Model and Application to ANYDAE. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 119–146. [CrossRef]
17. Andreeva, E.; Bhati, A.S.; Vizár, D. RUP Security of the SAEF Authenticated Encryption mode. *IACR Cryptol. ePrint Arch.* **2021**, *2021*, 103.
18. Datta, N.; Dutta, A.; Ghosh, S. INT-RUP Security of SAEB and TinyJAMBU. In Proceedings of the Progress in Cryptology-INDOCRYPT 2022-23rd International Conference on Cryptology in India, Kolkata, India, 11–14 December 2022; Isobe, T., Sarkar, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2022; Volume 13774, pp. 146–170. [CrossRef]
19. Bao, Z.; Guo, J.; Iwata, T.; Minematsu, K. ZOCB and ZOTR: Tweakable Blockcipher Modes for Authenticated Encryption with Full Absorption. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 1–54. [CrossRef]
20. Inoue, A.; Iwata, T.; Minematsu, K.; Poettering, B. Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. In Proceedings of the Advances in Cryptology-CRYPTO 2019-39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Boldyreva, A., Micciancio, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11692, pp. 3–31. [CrossRef]
21. Chakraborty, D.; Nandi, M. Attacks on the Authenticated Encryption Mode of Operation PAE. *IEEE Trans. Inf. Theory* **2015**, *61*, 5636–5642. [CrossRef]
22. Granger, R.; Jovanovic, P.; Mennink, B.; Neves, S. Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption. In Proceedings of the Advances in Cryptology-EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 8–12 May 2016; Fischlin, M., Coron, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9665, pp. 263–293. [CrossRef]

23. Jutla, C.S. Encryption Modes with Almost Free Message Integrity. In Proceedings of the Advances in Cryptology-EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001; Pfitzmann, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 529–544. [CrossRef]
24. Bossuet, L.; Datta, N.; Mancillas-López, C.; Nandi, M. ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. *IEEE Trans. Comput.* **2016**, *65*, 3318–3331. [CrossRef]
25. Datta, N.; Nandi, M. ELmE: A Misuse Resistant Parallel Authenticated Encryption. In Proceedings of the Information Security and Privacy-19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, 7–9 July 2014; Susilo, W., Mu, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8544, pp. 306–321. [CrossRef]
26. Abed, F.; Fluhrer, S.R.; Forler, C.; List, E.; Lucks, S.; McGrew, D.A.; Wenzel, J. Pipelineable On-line Encryption. In Proceedings of the Fast Software Encryption-21st International Workshop, FSE 2014, London, UK, 3–5 March 2014; Cid, C., Rechberger, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8540, pp. 205–223. [CrossRef]
27. Fleischmann, E.; Forler, C.; Lucks, S. McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. In Proceedings of the Fast Software Encryption-19th International Workshop, FSE 2012, Washington, DC, USA, 19–21 March 2012; Canteaut, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7549, pp. 196–215. [CrossRef]
28. Naito, Y.; Sasaki, Y.; Sugawara, T. Lightweight Authenticated Encryption Mode Suitable for Threshold Implementation. In Proceedings of the Advances in Cryptology-EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10–14 May 2020; Canteaut, A., Ishai, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12106, pp. 705–735. [CrossRef]
29. Naito, Y.; Sugawara, T. Lightweight Authenticated Encryption Mode of Operation for Tweakable Block Ciphers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2020**, *2020*, 66–94. [CrossRef]
30. Naito, Y. Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 1–26. [CrossRef]
31. Peyrin, T.; Seurin, Y. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In Proceedings of the Advances in Cryptology-CRYPTO 2016-36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9814, pp. 33–63. [CrossRef]
32. Mennink, B. XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In Proceedings of the Advances in Cryptology-CRYPTO 2016-36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9814, pp. 64–94. [CrossRef]
33. Cogliati, B.; Lampe, R.; Seurin, Y. Tweaking Even-Mansour Ciphers. In Proceedings of the Advances in Cryptology-CRYPTO 2015-35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; Gennaro, R., Robshaw, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9215, pp. 189–208. [CrossRef]
34. Cogliati, B.; Seurin, Y. Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing. In Proceedings of the Advances in Cryptology-ASIACRYPT 2015-21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015; Iwata, T., Cheon, J.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9453, pp. 134–158. [CrossRef]
35. Landecker, W.; Shrimpton, T.; Terashima, R.S. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Proceedings of the Advances in Cryptology-CRYPTO 2012-32nd Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012; Safavi-Naini, R., Canetti, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7417, pp. 14–30. [CrossRef]
36. Liskov, M.D.; Rivest, R.L.; Wagner, D.A. Tweakable Block Ciphers. *J. Cryptol.* **2011**, *24*, 588–613. [CrossRef]
37. Minematsu, K. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Proceedings of the Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, 22–25 February 2009; Dunkelman, O., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5665, pp. 308–326. [CrossRef]
38. Chakraborty, D.; Sarkar, P. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. *IEEE Trans. Inf. Theory* **2008**, *54*, 1991–2006. [CrossRef]
39. Liskov, M.D.; Rivest, R.L.; Wagner, D.A. Tweakable Block Ciphers. In Proceedings of the Advances in Cryptology-CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002; Yung, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2442, pp. 31–46. [CrossRef]
40. Namprempre, C.; Rogaway, P.; Shrimpton, T. Reconsidering Generic Composition. In Proceedings of the Advances in Cryptology-EUROCRYPT 2014-33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; Nguyen, P.Q., Oswald, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8441, pp. 257–274. [CrossRef]
41. Xu, Y.; Liu, W.; Yu, W. Quantum forgery attacks on COPA, AES-COPA and marble authenticated encryption algorithms. *Quantum Inf. Process.* **2021**, *20*, 131. [CrossRef]
42. Bossuet, L.; Mancillas-López, C.; Ovilla-Martinez, B. Pipelined Hardware Implementation of COPA, ELmD, and COLM. *IEEE Trans. Comput.* **2020**, *69*, 1533–1543. [CrossRef]

43. Ashur, T.; Dunkelman, O.; Luykx, A. Boosting Authenticated Encryption Robustness with Minimal Modifications. In Proceedings of the Advances in Cryptology-CRYPTO 2017-37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Katz, J., Shacham, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10403, pp. 3–33. [CrossRef]
44. Li, Y.; Leurent, G.; Wang, M.; Wang, W.; Zhang, G.; Liu, Y. Universal Forgery Attack Against GCM-RUP. In Proceedings of the Topics in Cryptology-CT-RSA 2020-The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, 24–28 February 2020; Jarecki, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12006, pp. 15–34. [CrossRef]