Received: 5 August 2022 | Revised: 23 January 2023 | Accepted: 25 January 2023

DOI: 10.1049/ise2.12110

IET Information Security

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Nonce-misuse resilience of Romulus-N and GIFT-COFB

Akiko Inoue[1] | Chun Guo[2,3,4] | Kazuhiko Minematsu[1]

[1]NEC, Kawasaki, Japan

[2]School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China

[3]Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, China

[4]Shandong Research Institute of Industrial Technology, Jinan, Shandong, China

Correspondence

Kazuhiko Minematsu.
Email: k-minematsu@nec.com

Funding information

National Natural Science Foundation of China, Grant/Award Number: 62002202; Shandong Nature Science Foundation of China, Grant/Award Number: ZR2020MF053

Abstract

Nonce-misuse resilience (NMRL) security of Romulus-N and GIFT-COFB is analysed, the two finalists of NIST Lightweight Cryptography project for standardising lightweight authenticated encryption. NMRL, introduced by Ashur et al. at CRYPTO 2017, is a relaxed security notion from a stronger, nonce-misuse resistance notion. The authors have proved that Romulus-N and GIFT- COFB have nonce-misuse resilience. For Romulus-N, the perfect privacy (NMRL-PRIV) and $n/2$-bit authenticity (NMRL-AUTH) with graceful degradation with respect to nonce repetition are showed. For GIFT-COFB, $n/4$-bit security for both NMRL-PRIV and NMRL-AUTH notions is showed.

KEYWORDS

authenticated encryption, GIFT-COFB, NIST lightweight cryptography, nonce misuse, Romulus-N

1 | INTRODUCTION

Authenticated encryption (AE) is a symmetric-key cryptographic function that provides simultaneously confidentiality and message integrity. Popular AE schemes, such as *GCM* [1] and *OCB* [2–4], are nonce-based AE (NAE), where a nonce is a value that never repeats at encryptions. In principle, the nonce uniqueness is maintained, say by using a counter. However, the nonce may repeat in practice due to various reasons. The problem of repeating nonce is typically called *nonce-misuse* and has been recognised as a real threat shown by many practical attacks, such as [5, 6].

Nonce-misuse attacks against NAE can be devastating. Most notably, *GCM* reveals its authentication key even with a single nonce-misuse [7], which implies universal forgery attacks. Although these attacks do not invalidate the original security proofs assuming a nonce-respecting adversary, they are extensively studied for various NAE algorithms due to their practical relevance [8–11].

The problem of nonce-misuse has been formally studied by Rogaway and Shrimpton [12]. They defined Misuse-resistant AE (MRAE), which ensures the maximum security against nonce-misuse, called nonce-misuse resistance (NMR). In essence, MRAE ensures that a repeat of nonce in encryption queries does not reveal anything as long as the entire input tuple of (nonce, associated data (AD), plaintext) is unique. Authenticity is also maintained even if a nonce is repeated. This is very strong protection; however, inherently requires off-line, two-pass computation.

Reflecting the increasing need for protection for resource-constrained devices, NIST is conducting a lightweight cryptography (LWC) project aiming at standardising lightweight AE schemes from 2018[1]. After two selection rounds, NIST announced 10 finalists in March 2022. To make lightweight AE schemes, it is natural to focus on NAE. In fact, NIST did not explicitly require any form of security against nonce reuse/misuse, just mentioning that any security property maintained even when nonce repeats could be advertised as a feature. As a

[1]https://csrc.nist.gov/Projects/lightweight-cryptography

result, a large fraction of the initial submissions to NIST LWC are NAEs, and among the 10 finalists, only one finalist (Romulus [13, 14]) includes an MRAE (Romulus-M, a secondary member). Considering the aforementioned potential risk of nonce-misuse, investigating the effect of nonce-misuse on the finalists is practically relevant. Although there is some progress, still nonce-misuse analysis is scarce as pointed out by [15], in particular within a formal provable security framework (see Related Work below for a detailed discussion).

In this paper, we study two NIST LWC finalists, Romulus-N (the primary member of Romulus) and GIFT- COFB [16]. They are NAEs and not MRAEs. Instead, we focus on a relaxed security notion against nonce-misuse, called *Nonce-Misuse ResiLience* (NMRL)[2], introduced by Ashur et al. at CRYPTO 2017 [11]. They defined privacy (NMRL-PRIV) and authenticity (NMRL-AUTH) notions. Intuitively, NMRL notions tell if a repeat of a nonce N can affect messages using nonces different from N. See [11] (also Section 2) for the definitions and its relevance, security of popular schemes etc. For example, GCM and OCB (of the first version) meet neither NMRL-PRIV nor NMRL-AUTH [11]. For example, Vanhoef and Piessen [17] mentioned the importance of resilience against nonce-misuse as mitigation of their attack against WPA2 and suggested CCM and MRAEs as alternatives to GCM. NIST also mentioned Ashur et al. in their status report [18].

Besides being finalists, our motivation to study Romulus-N and GIFT-COFB is based on the fact that they share structural similarity (namely, COFB [19]). Their serial structure has also some similarity to Sponges but it lacks 'capacity' part; thus, most of the output blocks of a primitive are given to the adversary. NMRL security analysis of such structure has not been done before, and we cannot reuse any results on Sponges or other finalists. Regarding the original proofs of Romulus-N and GIFT-COFB, some of them could be reused; however, we need dedicated analysis for the major remaining parts (see below).

We first show that Romulus-N and GIFT-COFB are not misuse resistant (Sect. 4). Under the NMR setting, the privacy notion (NMR-PRIV) is impossible to meet for their online computations, and the authenticity notion (NMR-AUTH) is broken with few queries with a repeated nonce, which we call the chain transition attack.

A natural question here is their NMRL security. We answer this positively by showing that Romulus-N and GIFT-COFB have NMRL-PRIV and NMRL-AUTH security. In particular, Romulus-N has perfect NMRL-PRIV security and $n/2$-bit NMRL-AUTH security with graceful degradation with respect to the maximum number of a nonce repeat (i.e., if nonce does not repeat too much it achieves almost ideal, about n-bit authenticity) for $n = 128$. This means that Romulus-N maintains a strong resilience against nonce-misuse. This result is particularly relevant since Romulus-N is a primary member of Romulus and shows the completeness of Romulus as a family of AEs having different levels of protection against nonce-misuse. For Romulus-N, while NMRL-PRIV security proof is obvious thanks to the explicit domain separation via tweak, our NMRL-AUTH proof together with graceful degradation requires a detailed analysis.

For GIFT- COFB, the original security bound is $(n/2 - \log n)$-bit for both privacy and authenticity. We showed $n/4$-bit NMRL-PRIV and NMRL-AUTH security for $n = 128$. These bounds are quantitatively weak, however still not pointless in some use cases. Say, if nonce repeat is fairly infrequent and can be detected within a short period, the administrator can take action, for example, by resetting the devices, before the damage gets too large. In contrast, when nonce repeat occurs for GCM, the adversary *immediately* mounts a universal forgery with probability one.

We stress that our proofs for GIFT-COFB are quite different from the original proofs for nonce-respecting adversary, which crucially depend on the fact that nonces in the encryption queries are unique. Moreover, the short input mask of $n/2$ bits prohibits a modular analysis via tweakable block cipher (TBC) such as the proofs of OCB [3, 4] to achieve the desired bound. We found that, for NMRL analysis, such a modular analysis indeed works from the nature of the attack. After an abstraction by the TBC, NMRL-PRIV proof is immediate, while NMRL-AUTH proof is largely similar to the proof of Romulus-N but the difference in the usage of tweak requires a dedicated analysis (indeed, this difference enables the full n-bit NMRL-AUTH security for the TBC-abstracted version). We also would like to remark that our NMRL proofs provide alternative nonce-respecting security proofs for GIFT- COFB as a byproduct. The bounds are weak, only $n/4$ bits, but its modular structure makes the proof more intuitive. The resulting analysis reveals that the case analysis is indeed subtle to avoid attacks (even in the nonce respecting scenario), which has not been explicitly shown in the specification documents. We think this is a part of our contributions: our proof eventually helps understanding the design and implies the soundness of the construction (i.e. if n is large enough it implements a secure NAE with sufficient NMRL security). The original proofs are rather complex [20], and ours complement them by showing a more detailed analysis of the domain separation, supporting its correctness.

Related Work. Two NIST LWC finalists, Ascon [21] and ISAP [22], have been shown to have nonce-misuse resilient privacy and misuse resistant authenticity [23, 24]. NMRL security has been shown for a 2nd-round candidate Spook [25]. Elephant showed the NMR authenticity [26, 27].

2 | PRELIMINARIES

Let $\{0,1\}^*$ be the set of all finite bit strings, including the empty string ε. For $X \in \{0,1\}^*$, let $|X|$ denote its bit length. Here, $|\varepsilon| = 0$. For integer $n \geq 0$, let $\{0,1\}^n$ be the set of n-bit strings, and let $\{0,1\}^{\leq n} = \bigcup_{i \in \{0,\ldots,n\}} \{0,1\}^i$, where $\{0,1\}^0 = \{\varepsilon\}$. Let $[n] = \{1, \ldots, n\}$ and $[\,[n]\,] = \{0, 1, \ldots, n-1\}$. If X is uniformly distributed over a set $\mathcal{X}$, we write

[2] This acronym is to avoid confusion with nonce-misuse resistance.

$X \xleftarrow{\$} \mathcal{X}$. For two bit strings X and Y, $X \| Y$ is their concatenation. We also write this as XY if it is clear from the context. Let 0^i (1^i) be the string of i zero bits (i one bits), and for instance, we write 10^i for $1 \| 0^i$. We write $\mathtt{msb}_i(X)$ (respectively, $\mathtt{lsb}_i(X)$) to denote the i most (respectively, least) significant bits of X. For $X \in \{0,1\}^*$, let $|X|_n = \max\{1, \lceil |X|/n \rceil\}$. Let $(X[1], \ldots, X[x]) \xleftarrow{n} X$ be the parsing of X into n-bit blocks. Here $X[1] \| X[2] \| \ldots \| X[x] = X$ and $x = |X|_n$. When $X = \varepsilon$, we have $X[1] \xleftarrow{n} X$ and $X[1] = \varepsilon$. Let $X \lll i$ denote the left rotation shift of X by i bits.

Following [3], by writing $2a$ for $a \in \{0,1\}^s$, we mean a GF (2^s) multiplication by the polynomial $\mathtt{x}$, also called a doubling. Similarly, $3a$ means a multiplication by $\mathtt{x}+\mathtt{1}$, that is, $3a = 2a \oplus a$. They are used by GIFT-COFB with $s = 64$ [20].

(Tweakable) Block Cipher. A TBC is a keyed function $\tilde{E} : \mathcal{K} \times \mathcal{T}_{\mathcal{W}} \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{K}$ is the key space, $\mathcal{T}_{\mathcal{W}}$ is the tweak space, and $\mathcal{M} = \{0,1\}^n$ is the message space, such that for any $(K, T_w) \in \mathcal{K} \times \mathcal{T}_{\mathcal{W}}$, $\tilde{E}(K, T_w, \cdot)$ is a permutation over $\mathcal{M}$. We interchangeably write $\tilde{E}(K, T_w, M)$ or $\tilde{E}_K(T_w, M)$ or $\tilde{E}_K^{T_w}(M)$. The decryption routine is written as $\left(\tilde{E}_K^{T_w}\right)^{-1}(\cdot)$, where if $C = \tilde{E}_K^{T_w}(M)$ holds for some (K, T_w, M) we have $M = \left(\tilde{E}_K^{T_w}\right)^{-1}(C)$. When $\mathcal{T}_{\mathcal{W}}$ is a singleton, it is essentially a block cipher and is simply written as $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$.

Random Primitives. Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{T}_w$ be non-empty finite sets. Let $\mathrm{Func}(\mathcal{X}, \mathcal{Y})$ be the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$, and let $\mathrm{Perm}(\mathcal{X})$ be the set of all permutations over $\mathcal{X}$. Moreover, let $\mathrm{Perm}(\mathcal{T}_w, \mathcal{X})$ be the set of all functions $f : \mathcal{T}_w \times \mathcal{X} \to \mathcal{X}$ such that for any $T \in \mathcal{T}_w$, $f(T, \cdot)$ is a permutation over $\mathcal{X}$. A uniform random permutation (URP) over $\mathcal{X}$, $\mathsf{P} : \mathcal{X} \to \mathcal{X}$, is a random permutation with uniform distribution over $\mathrm{Perm}(\mathcal{X})$. An n-bit URP is a URP over $\{0,1\}^n$. A tweakable URP (TURP) with a tweak space $\mathcal{T}_w$ and a message space $\mathcal{X}$, $\tilde{\mathsf{P}} : \mathcal{T}_w \times \mathcal{X} \to \mathcal{X}$, is a random tweakable permutation with uniform distribution over $\mathrm{Perm}(\mathcal{T}_w, \mathcal{X})$. The decryption is written as $\mathsf{P}^{-1}(*)$ for URP and $\left(\tilde{\mathsf{P}}^{-1}\right)^T(*)$ for TURP given tweak T.

Definition 1 *A nonce-based authenticated encryption (NAE) is a tuple $\Pi = (\mathcal{E}, \mathcal{D})$. For key space $\mathcal{K}$, nonce space $\mathcal{N}$, message space $\mathcal{M}$ and associated data (AD) space $\mathcal{A}$, the encryption algorithm $\mathcal{E}$ takes a key $K \in \mathcal{K}$ and a tuple (N, A, M) of a nonce $N \in \mathcal{N}$, an AD $A \in \mathcal{A}$, and a plaintext $M \in \mathcal{M}$ as input, and returns a ciphertext $C \in \mathcal{M}$ and a tag $T \in \mathcal{T}$. Typically, $\mathcal{T} = \{0,1\}^\tau$ for a fixed, small τ. The decryption algorithm $\mathcal{D}$ takes $K \in \mathcal{K}$ and the tuple (N, A, C, T) as input and returns $M \in \mathcal{M}$ or the reject symbol $\perp$. The corresponding encryption and decryption oracles are written as $\mathcal{E}_K$ and $\mathcal{D}_K$.*

An NAE scheme usually assumes each nonce in encryption queries to be distinct. However, our security definitions consider the case that nonces may be reused (misused) in encryption queries.

2.1 | Security definitions

Let A be an adversary that queries an oracle $\mathcal{O}$ and outputs a bit $x \in \{0,1\}$. We write $\mathsf{A}^{\mathcal{O}} \Rightarrow 1$ to denote the event that $x = 1$. It is a probabilistic event whose randomness comes from those of A and $\mathcal{O}$. Queries of A may be adaptive unless otherwise specified. If there are multiple oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, $\mathsf{A}^{\mathcal{O}_1, \mathcal{O}_2, \ldots}$ means that A can query any oracle in an arbitrary order unless otherwise specified.

Definition 2 *For a TBC $\tilde{E} : \mathcal{K} \times \mathcal{T}_w \times \mathcal{M} \to \mathcal{M}$, its Tweakable Pseudorandom Permutation (TPRP)-advantage against A is defined as*

$$\mathbf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\tilde{E}_K} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\tilde{\mathsf{P}}} \Rightarrow 1\right] \right|,$$

where $\tilde{\mathsf{P}} : \mathcal{T}_w \times \mathcal{M} \to \mathcal{M}$ is a TURP and A may query any $(T, M) \in \mathcal{T}_w \times \mathcal{M}$. The PRP advantage of a block cipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ $\left(\mathbf{Adv}_E^{\mathsf{prp}}(\mathsf{A})\right)$ is similarly defined by assuming $\mathcal{T}_w$ is a singleton.

We write (q, t)-(T)PRP adversary to mean an adversary using q queries and t time against the (tweakable) block cipher.

2.1.1 | Security notions for Authenticated encryption.

Let $\Pi = (\mathcal{E}, \mathcal{D})$ be an NAE scheme (Def. 1). We define \$oracle that takes any valid input (N, A, M) for $\mathcal{E}_K$ and returns a random string of $|\mathcal{E}_K(N, A, M)|$ bits, and $\perp$ oracle that takes any valid input (N, A, C, T) for $\mathcal{D}_K$ and returns $\perp$.

Definition 3 (PRIV and AUTH). *The (nonce-respecting) privacy and authenticity notions for Π are as follows [28].*

$$\mathbf{Adv}_{\Pi}^{\mathsf{priv}}(\mathsf{A}_1) := \left| \Pr\left[\mathsf{A}_1^{\mathcal{E}_K} \Rightarrow 1\right] - \Pr\left[\mathsf{A}_1^{\$} \Rightarrow 1\right] \right|,$$

$$\mathbf{Adv}_{\Pi}^{\mathsf{auth}}(\mathsf{A}_2) := \left| \Pr\left[\mathsf{A}_2^{\mathcal{E}_K, \mathcal{D}_K} \Rightarrow 1\right] - \Pr\left[\mathsf{A}_2^{\mathcal{E}_K, \perp} \Rightarrow 1\right] \right|$$

The adversary in the both notions are nonce-respecting, that is, the left oracle $\mathcal{O}_1$ takes a distinct nonce for each query. For AUTH notion, if (C, T) is returned by the left oracle $\mathcal{O}_1(N, A, M)$, then A_2 cannot query the right oracle $\mathcal{O}_2(N, A, C, T)$.

We use the term *effective blocks* to mean the number of actual primitive calls invoked in a query.

2.1.2 | Misuse resistance

The security notions in the sense of NMR are obtained by modifying the above notions. In particular, the privacy notion

(NMR-PRIV, $\mathbf{Adv}_{\Pi}^{\mathsf{nmr-priv}}(\mathsf{A}_1)$) is obtained by allowing A_1 to arbitrarily reuse nonce in encryption queries, but A_1 must make the entire query (N, A, M) distinct. The authenticity notion (NMR-AUTH, $\mathbf{Adv}_{\Pi}^{\mathsf{nmr-auth}}(\mathsf{A}_2)$) is obtained similarly by allowing A_2 to arbitrarily reuse nonce in encryption queries, and there is no restriction on nonces in decryption, as in the original AUTH notion. Two-pass, off-line schemes, such as SIV, [12] fulfill these notions and are called Misuse-resistant AE (MRAE). See [12] for more details.

2.1.3 | Misuse resilience

Nonce-Misuse ResiLience (NMRL) [11] is a relaxation of NMR. Specifically, the privacy and authenticity notions under NMRL divide encryption queries into *challenge* and *non-challenge* ones and only require the adversary to be nonce-respecting among the former type of queries. The nonce-misuse in non-challenge queries should not break the challenge ciphertexts (for privacy) or enable forgery with the challenge nonce (for authenticity). The definitions of [11] are as follows, where \$ and $\perp$ oracles as defined earlier.

Definition 4 (NMRL-PRIV). *The nonce-misuse resilience privacy advantage against* A *is defined as follows.*

$$\mathbf{Adv}_{\Pi}^{\mathsf{nmrl-priv}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathcal{E}_K,\mathcal{E}_K} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$,\mathcal{E}_K} \Rightarrow 1\right]\right|,$$

A *may re-use nonces with its right oracle* $\mathcal{O}_2$*, but it may not re-use nonces with its left oracle* $\mathcal{O}_1$*, nor may it use a nonce already queried to* $\mathcal{O}_2$ *for an* $\mathcal{O}_1$*-query and* vice versa.

Definition 5 (NMRL-AUTH). *The nonce-misuse resilience authenticity advantage against* A *is defined as follows.*

$$\mathbf{Adv}_{\Pi}^{\mathsf{nmrl-auth}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathcal{E}_K,\mathcal{D}_K} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathcal{E}_K,\perp} \Rightarrow 1\right]\right|,$$

where (i) nonces in $\mathcal{O}_1$ *may repeat, and (ii) after* $\mathcal{O}_1(N,A,M)$ *returns* (C, T), $\mathcal{O}_2(N,A,C,T)$ *cannot be queried, and (iii) each nonce appeared in* $\mathcal{O}_2$ *must appear at* $\mathcal{O}_1$ *at most once, irrespective of the order of queries.*

We remark that efficient single-pass AE schemes anyway cannot achieve full misuse resistance. Therefore, NMRL somehow reflects 'best possible' security for such schemes against nonce-reuse. This may increase the lifetime of keys. For example, when using 128-bit random nonces, the fraction of collided nonces remain small even if the number of encrypted messages goes beyond 2^{64}. Therefore, if a large proposition of encrypted messages quickly become obsolescent, then key update may be deferred (since the small proposition of critical messages remains secure w.h.p.).

Meanwhile, NMRL reflects a sort of forward security: even if nonce is repeated, the future nonces are secure (as long as they do not repeat). For example, consider some plant sensors sending messages. Then, a repeat of nonces would harm messages encrypted with that nonce, but the damage would be mitigated by replay protection or generally a stateful decryptor. In contrast, if GCM is used that does not ensure NMRL (auth), then the damage cannot be mitigated.

Remark. At EUROCRYPT 2019, Dutta et al. [29] introduced the *faulty nonce model*. Roughly speaking, this model adds an additional parameter quantifying maximum repetition of nonce to the ordinary NMR definition, and this enables fine-grained understanding of the effects of nonce-reuse. The model of nonce-misuse resilience is weaker, since it only ensures security at fresh nonces. On the other hand, misuse resistance is not achievable by single-pass AEs even in the faulty nonce model.

3 | BRIEF DESCRIPTIONS OF ROMULUS-N AND GIFT-COFB

3.1 | Romulus-N

Romulus-Nis the primary member of Romulus [13, 14]. It is based on Skinny-128-384+(the 40-round variant of SKINNY [30] TBC having 128-bit block and 384-bit tweakey). The specification of Romulus-N is given in Figure 1. As shown in Figure 1, Romulus-N uses an $n \times n$ binary matrix G defined as an $n/8 \times n/8$ diagonal matrix of 8×8 binary sub-matrices:

$$G = \begin{pmatrix} G_s & 0 & 0 & \dots & 0 \\ 0 & G_s & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & 0 & G_s & 0 \\ 0 & \dots & 0 & 0 & G_s \end{pmatrix},$$

where 0 here represents the 8×8 zero matrix, and G_s is an 8×8 binary matrix, defined as

$$G_s = \begin{pmatrix} 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&1 \end{pmatrix}.$$

Let $G^{(i)}$ for $i = 0, 8, 16, \dots, n$ be the matrix equal to G except the $(i+1)$-st to nth rows, which are set to all zero[3]. For our security proof, we just need the property that G *is sound*:

Definition 6 *A matrix* G *is sound, if: (1)* G *is regular (full-rank), and (2)* $G^{(i)} \oplus I$ *is regular for all* $i = 8, 16, \dots, n$*, where* I *denotes the identity matrix.*

[3]This definition comes from that Romulusis defined on byte strings.

Algorithm $\textsf{Romulus-N}[\widetilde{E}_K]\text{-}\mathcal{E}(N, A, M)$

$H \leftarrow \textsf{HashN}[\widetilde{E}_K](A)$
if $|A[a]| < n$ **then** $w_A \leftarrow 26$ **else** 24
$S \leftarrow \widetilde{E}_K^{(N, w_A, \overline{a})}(H)$
return $\textsf{Encrypt}[\widetilde{E}_K](N, S, M)$

Algorithm $\rho(S, M)$

$C \leftarrow M \oplus G(S)$
$S' \leftarrow S \oplus M$
return (S', C)

Algorithm $\textsf{HashN}[\widetilde{E}_K](A)$

$H \leftarrow 0^n$
$(A[1], \ldots, A[a]) \xleftarrow{n} A$
$A[a] \leftarrow \texttt{pad}_n(A[a])$
for $i = 1$ **to** $\lfloor a/2 \rfloor$
  $(H, \eta) \leftarrow \rho(H, A[2i-1])$
  $H \leftarrow \widetilde{E}_K^{(A[2i], 8, \overline{2i-1})}(H)$
end for
if $a \bmod 2 = 0$ **then** $V \leftarrow 0^n$ **else** $A[a]$
$(H, \eta) \leftarrow \rho(H, V)$
return H

Algorithm $\textsf{Encrypt}[\widetilde{E}_K](N, S, M)$

$(M[1], \ldots, M[m]) \xleftarrow{n} M$
if $|M[m]| < n$ **then** $w_M \leftarrow 21$ **else** 20
for $i = 1$ **to** $m - 1$
  $(S, C[i]) \leftarrow \rho(S, M[i])$
  $S \leftarrow \widetilde{E}_K^{(N, 4, \overline{i})}(S)$
end for
$M'[m] \leftarrow \texttt{pad}_n(M[m])$
$(S, C'[m]) \leftarrow \rho(S, M'[m])$
$C[m] \leftarrow \textsf{lsb}_{|M[m]|}(C'[m])$
$S \leftarrow \widetilde{E}_K^{(N, w_M, \overline{m})}(S)$
$(\eta, T) \leftarrow \rho(S, 0^n)$
$C \leftarrow C[1] \,\|\, \ldots \,\|\, C[m-1] \,\|\, C[m]$
return (C, T)

Algorithm $\textsf{Romulus-N}[\widetilde{E}_K]\text{-}\mathcal{D}(N, A, C, T)$

$H \leftarrow \textsf{HashN}[\widetilde{E}_K](A)$
if $|A[a]| < n$ **then** $w_A \leftarrow 26$ **else** 24
$S \leftarrow \widetilde{E}_K^{(N, w_A, \overline{a})}(H)$
return $\textsf{Decrypt}[\widetilde{E}_K](N, S, C)$

Algorithm $\rho^{-1}(S, C)$

$M \leftarrow C \oplus G(S)$
$S' \leftarrow S \oplus M$
return (S', M)

Algorithm $\textsf{Decrypt}[\widetilde{E}_K](N, S, C)$

$(C[1], \ldots, C[m]) \xleftarrow{n} C$
if $|C[m]| < n$ **then** $w_C \leftarrow 21$ **else** 20
for $i = 1$ **to** $m - 1$
  $(S, M[i]) \leftarrow \rho^{-1}(S, C[i])$
  $S \leftarrow \widetilde{E}_K^{(N, 4, \overline{i})}(S)$
end for
$\widetilde{S} \leftarrow (0^{|C[m]|} \,\|\, \textsf{msb}_{n-|C[m]|}(G(S)))$
$C'[m] \leftarrow \texttt{pad}_n(C[m]) \oplus \widetilde{S}$
$(S, M'[m]) \leftarrow \rho^{-1}(S, C'[m])$
$M[m] \leftarrow \textsf{lsb}_{|C[m]|}(M'[m])$
$S \leftarrow \widetilde{E}_K^{(N, w_C, \overline{m})}(S)$
$(\eta, T^*) \leftarrow \rho(S, 0^n)$
$M \leftarrow M[1] \,\|\, \ldots \,\|\, M[m-1] \,\|\, M[m]$
if $T^* = T$ **then return** M **else** $\perp$

FIGURE 1 The algorithms of Romulus-N [13]. Lines of [**if (statement) then** $X \leftarrow x$ **else** x'] are shorthand for [**if (statement) then** $X \leftarrow x$ **else** $X \leftarrow x'$]. The dummy variable η is always discarded. Let n be a multiple of 8. For $X \in \{0,1\}^{\leq n}$ of length multiple of 8, we define $\texttt{pad}_n(X) := qX$ if $|X| = n$, and $\texttt{pad}_n(X) := qX \,\|\, 0^{n-|X|-8} \,\|\, \texttt{len}_8(X)$ if $0 \leq |X| < n$, where $\texttt{len}_8(X)$ denotes the one-byte encoding of the byte-length of X. Note that $\texttt{pad}_n(\varepsilon) = 0^n$. For integer i, $\overline{i}$ denotes the LFSR encoding expression of i.

The paper [14, Theorem 1] showed the perfect (nonce-respecting) PRIV bound and n-bit AUTH bound for Romulus-N. Despite being the primary member, no nonce-misuse security analysis has not been shown for Romulus-N in the literature.

3.2 | GIFT-COFB

GIFT-COFB [16] is a block cipher-based AE that combines a variant of COFB mode [19] and the lightweight 128-bit block cipher GIFT [31]. GIFT-COFB is a rate-one scheme that has a quite small footprint. The specification is shown in Figure 2 in the Appendix. See also Figure 3 for illustration. The padding $\texttt{padc} : \{0,1\}^* \to \{0,1\}^n$ is $\texttt{padc}(x) = x$ if $x \neq \varepsilon$ and $|x| \bmod n = 0$, and $\texttt{padc}(x) = x \,\|\, 10^{n-(|x| \bmod n)-1}$ otherwise. Note that $\texttt{padc}(\varepsilon) = 10^{n-1}$. The $G_{\mathtt{C}}$ in Figure 2 is an $n \times n$ binary matrix different from G of Romulus-N. It is defined as $G_{\mathtt{C}} \cdot X := (X[2], X[1] \lll 1)$ for $X[1], X[2] \xleftarrow{n/2} X$, $X \in \{0,1\}^n$. Here, $n = 128$.

While not explicit in Figure 2, the block process can be represented by the following functions. Let $\{0,1\}^{\leq \tilde{n}} = \bigcup_{i \in [n]} \{0,1\}^i$.

Definition 7 *Let* $\rho_{\mathtt{C}_1} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *such that* $\rho_{\mathtt{C}_1}(Y, M) = G_{\mathtt{C}} \cdot Y \oplus M$. *We define* $\rho_{\mathtt{C}}, \rho'_{\mathtt{C}} : \{0,1\}^n \times \{0,1\}^{\leq \tilde{n}} \to \{0,1\}^n \times \{0,1\}^{\leq \tilde{n}}$ *as*

$$\rho_{\mathtt{C}}(Y, M) := \left(\rho_{\mathtt{C}_1}(Y, \texttt{padc}(M)), \texttt{msb}_{|M|}(Y) \oplus M\right),$$
$$\rho'_{\mathtt{C}}(Y, C) := \left(\rho_{\mathtt{C}_1}\left(Y, \texttt{padc}\left(\texttt{msb}_{|C|}(Y) \oplus C\right)\right), \texttt{msb}_{|C|}(Y) \oplus C\right).$$

The $\rho_{\mathtt{C}}$ is used for encryption and $\rho'_{\mathtt{C}}$ is used for decryption. Note that when $(X, M) = \rho'_{\mathtt{C}}(Y, C)$, then $X = (G_{\mathtt{C}} \oplus I) \cdot Y \oplus C$, where I is the $n \times n$ identity matrix. We note that the matrix $G_{\mathtt{C}} \oplus I$ has rank $n - 1$.

Algorithm GIFT-COFB-$\mathcal{E}_K(N, A, M)$

$Y[0] \leftarrow E_K(N),\ L \leftarrow \mathtt{msb}_{n/2}(Y[0])$
$(A[1], \ldots, A[a]) \xleftarrow{n} \mathtt{padc}(A)$
if $M \neq \varepsilon$ **then**
  $(M[1], \ldots, M[m]) \xleftarrow{n} \mathtt{padc}(M)$
for $i = 1$ **to** $a - 1$
  $L \leftarrow 2 \cdot L$
  $X[i] \leftarrow A[i] \oplus G \cdot Y[i-1] \oplus L \| 0^{n/2}$
  $Y[i] \leftarrow E_K(X[i])$
if $|A| \bmod n = 0$ **and** $A \neq \varepsilon$ **then** $L \leftarrow 3 \cdot L$
else $L \leftarrow 3^2 \cdot L$
if $M = \varepsilon$ **then** $L \leftarrow 3^2 \cdot L$
$X[a] \leftarrow A[a] \oplus G \cdot Y[a-1] \oplus L \| 0^{n/2}$
$Y[a] \leftarrow E_K(X[a])$
for $i = 1$ **to** $m - 1$
  $L \leftarrow 2 \cdot L$
  $C[i] \leftarrow M[i] \oplus Y[i+a-1]$
  $X[i+a] \leftarrow M[i] \oplus G \cdot Y[i+a-1] \oplus L \| 0^{n/2}$
  $Y[i+a] \leftarrow E_K(X[i+a])$
if $M \neq \varepsilon$ **then**
  if $|M| \bmod n = 0$ **then** $L \leftarrow 3 \cdot L$
  else $L \leftarrow 3^2 \cdot L$
  $C[m] \leftarrow M[m] \oplus Y[a+m-1]$
  $X[a+m] \leftarrow M[m] \oplus G \cdot Y[a+m-1] \oplus L \| 0^{n/2}$
  $Y[a+m] \leftarrow E_K(X[a+m])$
  $C \leftarrow \mathtt{msb}_{|M|}(C[1] \| \ldots \| C[m])$
  $T \leftarrow \mathtt{msb}_\tau(Y[a+m])$
else $C \leftarrow \varepsilon,\ T \leftarrow \mathtt{msb}_\tau(Y[a])$
return (C, T)

Algorithm GIFT-COFB-$\mathcal{D}_K(N, A, C, T)$

$Y[0] \leftarrow E_K(N),\ L \leftarrow \mathtt{msb}_{n/2}(Y[0])$
$(A[1], \ldots, A[a]) \xleftarrow{n} \mathtt{padc}(A)$
if $C \neq \varepsilon$ **then**
  $(C[1], \ldots, C[c]) \xleftarrow{n} \mathtt{padc}(C)$
for $i = 1$ **to** $a - 1$
  $L \leftarrow 2 \cdot L$
  $X[i] \leftarrow A[i] \oplus G \cdot Y[i-1] \oplus L \| 0^{n/2}$
  $Y[i] \leftarrow E_K(X[i])$
if $|A| \bmod n = 0$ **and** $A \neq \varepsilon$ **then** $L \leftarrow 3 \cdot L$
else $L \leftarrow 3^2 \cdot L$
if $C = \varepsilon$ **then** $L \leftarrow 3^2 \cdot L$
$X[a] \leftarrow A[a] \oplus G \cdot Y[a-1] \oplus L \| 0^{n/2}$
$Y[a] \leftarrow E_K(X[a])$
for $i = 1$ **to** $c - 1$
  $L \leftarrow 2 \cdot L$
  $M[i] \leftarrow Y[i+a-1] \oplus C[i]$
  $X[i+a] \leftarrow M[i] \oplus G \cdot Y[i+a-1] \oplus L \| 0^{n/2}$
  $Y[i+a] \leftarrow E_K(X[i+a])$
if $C \neq \varepsilon$ **then**
  if $|C| \bmod n = 0$ **then**
    $L \leftarrow 3 \cdot L$
    $M[c] \leftarrow Y[a+c-1] \oplus C[c]$
  else
    $L \leftarrow 3^2 \cdot L,\ c' \leftarrow |C| \bmod n$
    $M[c] \leftarrow \mathtt{msb}_{c'}(Y[a+c-1] \oplus C[c]) \| 10^{n-c'-1}$
  $X[a+c] \leftarrow M[c] \oplus G \cdot Y[a+c-1] \oplus L \| 0^{n/2}$
  $Y[a+c] \leftarrow E_K(X[a+c])$
  $M \leftarrow \mathtt{msb}_{|C|}(M[1] \| \ldots \| M[c])$
  $T' \leftarrow \mathtt{msb}_\tau(Y[a+c])$
else $M \leftarrow \varepsilon,\ T' \leftarrow \mathtt{msb}_\tau(Y[a])$
if $T' = T$ **then return** M, **else return** $\perp$

FIGURE 2 The algorithms of GIFT-COFB [16] with minor notation modifications. $\mathtt{padc}(x) = x$ if x is not empty and $|x| \bmod n = 0$, and $\mathtt{padc}(x) = x \| 10^{n-(|x| \bmod n)-1}$ otherwise. Note that $\mathtt{padc}(\varepsilon) = 10^{n-1}$.

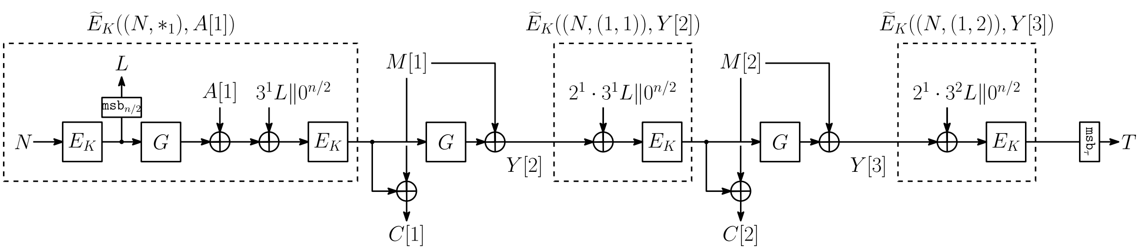

FIGURE 3 Example of GIFT-COFB encryption for n-bit associated data (AD) and $2n$-bit plaintext. Dashed boxes denote the tweakable block cipher (TBC) instantiated by E_K, which is identical to the TBC defined at Definition 8 $\left(\mathsf{gXE}^{\mathsf{cofb}}[E_K]\right)$. See also Figure 4.

The designers [20] showed the security bound for the combined nonce-respecting PRIV and AUTH notions, which is about $(n/2 - \log\ n)$-bit security[4]. Security property against nonce-misusing adversary has not been shown.

4 | NONCE-MISUSE RESISTANCE OF ROMULUS-N AND GIFT-COFB

Both Romulus-N and GIFT- COFB do not have NMR-PRIV and NMR-AUTH. The lack of NMR-PRIV is clear from their online computation. To break NMR-AUTH of Romulus-N, we just need two encryptions of repeating nonce and one decryption query, which we call 'chain transition' (CT) attack. The attack is described by the following algorithm. Note that in the description, we follow the formalism of Definition 5 and view the adversary as interacting with a pair of oracles $(\mathcal{O}_1, \mathcal{O}_2)$ that is either $(\mathcal{E}_K, \mathcal{D}_K)$ or $(\mathcal{E}_K, \perp)$.

Algorithm 'Chain transition' (CT) attack on Romulus-N

1. $(C_1 \| C_2, T) \leftarrow \mathcal{O}_1(N, A, M_1 \| M_2)$
2. $(C'_1 \| C'_2, T') \leftarrow \mathcal{O}_1(N, A, M'_1 \| M'_2)$
3. $C''_2 \leftarrow M'_2 \oplus G^{-1}(M'_2 \oplus C'_2) \oplus (G^{-1} \oplus I)(M_2 \oplus C_2)$
4. Query $\mathcal{O}_2(N, A, C_1 \| C''_2, T')$, and outputs 1 iff the response is not $\perp$.

Here, M_i, M'_i, C'_i for $i = 1, 2$, and C'', are all n bits. To understand the attack idea, let $S = \widetilde{E}_K^{(N, w_A, \bar{a})}\left(\mathsf{HashN}^{\widetilde{E}_K}(A)\right)$, $(X_1, C_1) = \rho(S, M_1)$, $Y_1 = \widetilde{E}_K^{(N,4,\bar{1})}(X_1)$, $(X_2, C_2) = \rho(Y_1, M_2)$, $Y_2 = \widetilde{E}_K^{(N, w_M, \bar{2})}(X_2)$, $(X_3, T) = \rho(Y_2, 0^n)$; $(X'_1, C'_1) = \rho(S, M'_1)$, $Y'_1 = \widetilde{E}_K^{(N,4,\bar{1})}(X'_1)$, $(X'_2, C'_2) = \rho(Y'_1, M'_2)$, $Y'_2 = \widetilde{E}_K^{(N, w_M, \bar{2})}$

[4]Reflecting Inoue et al. [36], the bound was revised, maintaining the original bit security.

(X_2'), $(X_3', T') = \rho(Y_2', 0^n)$ be the (intermediate) values appeared during Romulus-N encrypting $(N, A, M_1\|M_2)$ and $(N, A, M_1'\|M_2')$. By these and by the definition of ρ, the n-bit states X_2, Y_2, X_2', Y_2' can be completely recovered, that is,

$$\begin{aligned}
Y_1 &= G^{-1}(M_2 \oplus C_2),\\
X_2 &= Y_1 \oplus M_2 = M_2 \oplus G^{-1}(M_2 \oplus C_2),\\
Y_1' &= G^{-1}(M_2' \oplus C_2'),\\
X_2' &= Y_1' \oplus M_2' = M_2' \oplus G^{-1}(M_2' \oplus C_2').
\end{aligned}$$

By these, the decryption of $(N, C_1\|C_2'', T')$ will compute $S \leftarrow \tilde{E}_K^{(N, w_A, \overline{a})}\left(\mathsf{HashN}^{\tilde{E}_K}(A)\right)$, $(X_1, M_1) \leftarrow \rho(S, C_1)$, $Y_1 \leftarrow \tilde{E}_K^{(N,4,\overline{1})}(X_1)$, and then $(X_2'', M_2'') = \rho(Y_1, C_2'')$. It now holds $X_2'' = Y_1 \oplus C_2'' \oplus G(Y_1) = (G^{-1} \oplus I)(M_2 \oplus C_2) \oplus M_2' \oplus G^{-1}(M_2' \oplus C_2') \oplus (G^{-1} \oplus I)(M_2 \oplus C_2) = X_2'$. By these, it necessarily proceeds with $Y_2 = \tilde{E}_K^{(N, w_M, \overline{2})}(X_2)$, $(X_3, T^*) = \rho(Y_2, 0^n)$, and finally finds $T^* = T'$ and returns $M_1\|M_2'' \neq \perp$. This deviates from the ideal world response, and the attack advantage against Definition 5 is 1.

Almost the same attack can break NMR-AUTH of GIFT-COFB. This arises the natural question: *do they maintain any security property when nonce is misused?* From the next sections, we answer positively by showing concrete security in the sense of nonce-misuse resilience.

5 | NONCE-MISUSE RESILIENCE OF ROMULUS-N

We establish misuse resilience security for Romulus-N in this section.

Theorem 1 *Let* A_1 *be a privacy adversary against Romulus-N using* q_e *encryption queries with a total number of effective blocks* $\sigma_{\mathtt{priv}}$*, each nonce reused at most* μ *times and time complexity* t_{A_1}*. Let* A_2 *be an authenticity adversary using* q_e *encryption and* q_d *decryption queries with a total number of effective blocks* $\sigma_{\mathtt{auth}}$ *for encryption and decryption queries, each nonce reused at most* μ *times, and time complexity* t_{A_2}*. Further assuming* $\mu q_e \le 2^n/6$*. Then*

$$\mathbf{Adv}^{\mathsf{nmrl-priv}}_{\mathsf{Romulus\text{-}N}[\tilde{E}]}(\mathsf{A}_1) \le \mathbf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathsf{B}_1),$$

$$\mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{Romulus\text{-}N}[\tilde{E}]}(\mathsf{A}_2) \le \mathbf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathsf{B}_2) + \frac{4\mu q_e}{2^n} + \frac{6q_d}{2^n} + \frac{2q_d}{2^\tau}.$$

hold for some $(\sigma_{\mathtt{priv}}, t_A + O(\sigma_{\mathtt{priv}}))$-TPRP adversary B_1, and for some $(\sigma_{\mathtt{auth}}, t_B + O(\sigma_{\mathtt{auth}}))$-TPRP adversary B_2.

Here, $\tau \in [n]$ is the tag length. NIST submission document [13] specifies $\tau = n$, thus untruncated.

5.1 | Proof intuition

For the analysis, we focus on the idealised Romulus-Noracles $\mathcal{E}[\tilde{\mathsf{P}}]$ and $\mathcal{D}[\tilde{\mathsf{P}}]$ that are obtained from the real encryption and decryption oracles of Romulus-N via replacing the TBC $\tilde{E}_K$ with a TURP $\tilde{\mathsf{P}}$. This (standard approach) introduces the gaps $\mathbf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathsf{B}_1)$ and $\mathbf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathsf{B}_2)$ into the bounds as indicated by Theorem 1.

Then, the NMRL-PRIV proof just follows the nonce-respecting setting [14], and the bound remains optimal thanks to the uniqueness of the challenge nonces. For NMRL-AUTH, the bounds match intuitions from our attack: for every pair of nonce-reusing encryption queries $((N, A, M), (N, A', M'))$ with $w_A = w_{A'}$ and $a = a'$, the distinguisher may have the equality $\mathsf{HashN}[\tilde{\mathsf{P}}](A) = \mathsf{HashN}[\tilde{\mathsf{P}}](A')$ once observing $\tilde{\mathsf{P}}^{(N, w_A, \overline{a})}(\mathsf{HashN}[\tilde{\mathsf{P}}](A)) = \tilde{\mathsf{P}}^{(N, w_{A'}, \overline{a'})}(\mathsf{HashN}[\tilde{\mathsf{P}}](A'))$ from the ciphertexts, the probability of which should be $O(\mu q_e/2^n)$.

Such collisions 'leak' useful information about the TBC $\tilde{\mathsf{P}}$, which turns out helpful for forgery. Therefore, (intuitively) the proof should argue that such collisions/equalities are the 'only' that can be obtained by reusing nonces. For rigorously characterisation, we employ the H-coefficient technique (see Appendix A for its general idea), one of the standard techniques for symmetric provable security. In a nutshell, we show that the derived intermediate values $S_i = \tilde{\mathsf{P}}^{(N_i, w_{A_i}, \overline{a_i})}(\mathsf{HashN}[\tilde{\mathsf{P}}](A_i))$, $i = 1, \ldots, q_e$, are *pseudorandom modulo the collisions*. This will establish the intuition rigorously.

In the subsequent two subsections, we analyse NMRL-PRIV and NMRL-AUTH bounds for the aforementioned idealised Romulus-N, respectively.

5.2 | Proof for NMRL-PRIV bound of theorem 1

Proof for the optimal privacy security bound just follows the nonce-respecting setting [14]: each block in $\{C_1, \ldots, C_{q_e}, T_1, \ldots, T_{q_e}\}$ produced by the idealised challenge encryption oracle $\mathcal{E}[\tilde{\mathsf{P}}]$ is generated from the output of $\tilde{\mathsf{P}}$ given to G taking tweak unique to each block, since each nonce used by the challenge encryption oracle $\mathcal{E}[\tilde{\mathsf{P}}]$ is unique. As G is sound (Definition 6), if Y is independent and random, so is $G(Y)$. The soundness of G also ensures the uniformity of the last ciphertext block $C[m]$ and the tag T.

5.3 | Proof for NMRL-AUTH bound of theorem 1

To apply the H-coefficient method, we fix a distinguisher D interacting either with the real world $(\mathcal{E}[\tilde{\mathsf{P}}], \mathcal{D}[\tilde{\mathsf{P}}])$ or the ideal world $(\mathcal{E}[\tilde{\mathsf{P}}], \perp)$. We summarise the transcript of adversarial queries and responses in two lists $\mathcal{Q}_E$ and $\mathcal{Q}_D$. The former list

$$\mathcal{Q}_E = \big((N_1, A_1, M_1, C_1, T_1), \ldots, (N_{q_e}, A_{q_e}, M_{q_e}, C_{q_e}, T_{q_e})\big)$$

summarises the queries to the encryption oracle, where the ith tuple indicates encrypting (N_i, A_i, M_i) yielding $(C_i, T_i) \in \{0,1\}^{|M_i|} \times \{0,1\}^{\tau}$. Let a_i and m_i be the number of AD and plaintext blocks in the ith encryption query $(N_i, A_i, S_i, M_i, C_i, T_i)$, and let w_{A_i} be the corresponding w_A value. The latter list

$$\mathcal{Q}_D = \big((\mathtt{N}_1, \mathtt{A}_1, \mathtt{C}_1, \mathtt{T}_1, b_1), \ldots, (\mathtt{N}_{q_d}, \mathtt{A}_{q_d}, \mathtt{C}_{q_d}, \mathtt{T}_{q_d}, b_{q_d})\big),$$

where the ith tuple indicates decrypting $(\mathtt{N}_i, \mathtt{A}_i, \mathtt{C}_i, \mathtt{T}_i)$ yielding $b_i \in \{0,1\}^* \cup \{\perp\}$. Note that if $\mathcal{Q}_D$ is attainable (i.e., can be generated in the ideal world with non-zero probability), it has to be $b_i = \perp$ for all i.

At the end of the interaction, we reveal certain intermediate values to D:

- In the real world, for every encryption query $(N_i, A_i, M_i, C_i, T_i)$, we reveal the intermediate value $S_i \leftarrow \tilde{\mathsf{P}}^{(N_i, w_{A_i}, \overline{a_i})}\big(\mathsf{HashN}[\tilde{\mathsf{P}}](A_i)\big)$ at line 3 (see Figure 1) and append it to the list $\mathcal{Q}_E$.
- In the ideal world, for every pair (N_i, A_i) that appears in encryption queries, we associate a uniformly distributed n-bit string S_i and append it to the list $\mathcal{Q}_E$.

We thus obtain an extended list

$$\mathcal{Q}_E = \big((N_1, A_1, S_1, M_1, C_1, T_1), \ldots, (N_{q_e}, A_{q_e}, S_{q_e}, M_{q_e}, C_{q_e}, T_{q_e})\big),$$

and define the adversarial transcript of queries and responses as $\mathcal{Q} = (\mathcal{Q}_E, \mathcal{Q}_D)$.

Following the standard approach to applying the H-coefficient technique, below we first define *bad transcripts* and derive the probability of obtaining bad transcripts in the ideal world. Then, we establish the desired ratio in Equation (9) to complete the analysis.

5.3.1 | Bad transcripts

An attainable transcript $\mathcal{Q}$ is *bad*, if there exist two distinct tuples $(N_i, A_i, S_i, M_i, C_i, T_i), (N_j, A_j, S_j, M_j, C_j, T_j) \in \mathcal{Q}_E$ such that $N_i = N_j$, $A_i \neq A_j$, $(a_i, w_{A_i}) = (a_j, w_{A_j})$, though $S_i = S_j$. Such transcripts are bad, since they indicate collisions on $\mathsf{HashN}[\tilde{\mathsf{P}}]$ and leak non-trivial information about $\tilde{\mathsf{P}}$.

For each (i, j) such that $N_i = N_j$ and $A_i \neq A_j$, the strings S_i and S_j are uniform and independent in the ideal world, and the probability to have $S_i = S_j$ is $1/2^n$. For each $(N_i, A_i, S_i, M_i, C_i, T_i)$, the number of choices of $(N_j, A_j, S_j, M_j, C_j, T_j)$ with $N_j = N_i$ is at most μ by assumption. Therefore,

$$\Pr[T_{\mathsf{id}} \text{ is bad}] \leq \frac{\mu q_e}{2^n}.$$

5.3.2 | Ratio for good transcripts

For this part, consider an arbitrary attainable transcript $\mathcal{Q} = (\mathcal{Q}_E, \mathcal{Q}_D)$. For any i, let $H_i = \mathsf{HashN}[\tilde{\mathsf{P}}](A_i)$. In the ideal world, each pair (N_i, A_i) is associated with a uniformly distributed n-bit string S_i. Let α be the number of distinct pairs (N_i, A_i) in $\mathcal{Q}_E$. Then,

$$\begin{aligned}
&\Pr[T_{\mathsf{id}} = \mathcal{Q}] \\
&= \Pr[S_i, i = 1, \ldots, q_e] \\
&\quad \times \Pr\big[\mathsf{Encrypt}[\tilde{\mathsf{P}}](N_i, S_i, M_i) = (C_i, T_i) | S_i, i = 1, \ldots, q_e\big] \\
&\quad \times \underbrace{\Pr[T_{\mathsf{id}} = \mathcal{Q}_D | \mathcal{Q}_E]}_{=1} \\
&= \frac{1}{2^{\alpha n}} \times \Pr\big[\mathsf{Encrypt}[\tilde{\mathsf{P}}](N_i, S_i, M_i) = (C_i, T_i) | S_i, i = 1, \ldots, q_e\big].
\end{aligned}$$

The equality $\Pr[T_{\mathsf{id}} = \mathcal{Q}_D | \mathcal{Q}_E] = 1$ holds because if $\mathcal{Q}_D$ is attainable then all the responses $b_1, \ldots, b_{q_d}$ in $\mathcal{Q}_D$ are $\perp$ and because the ideal world right oracle $\perp$ always returns $\perp$.

On the other hand, in the real world, we have

$$\begin{aligned}
&\Pr[T_{\mathsf{re}} = \mathcal{Q}] \\
&= \Pr\Big[\tilde{\mathsf{P}}^{(N_i, w_{A_i}, \overline{a_i})}\big(\mathsf{HashN}[\tilde{\mathsf{P}}](A_i)\big) = S_i, i = 1, \ldots, q_e\Big] \\
&\quad \times \Pr\big[\mathsf{Encrypt}[\tilde{\mathsf{P}}](N_i, S_i, M_i) = (C_i, T_i) | S_i, i = 1, \ldots, q_e\big] \\
&\quad \times \Pr[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E].
\end{aligned}$$

Thus,

$$\begin{aligned}
&\frac{\Pr[T_{\mathsf{re}} = \mathcal{Q}]}{\Pr[T_{\mathsf{id}} = \mathcal{Q}]} \\
&= 2^{\alpha n} \times \Pr\Big[\tilde{\mathsf{P}}^{(N_i, w_{A_i}, \overline{a_i})}\big(\mathsf{HashN}[\tilde{\mathsf{P}}](A_i)\big) = S_i, i = 1, \ldots, q_e\Big] \\
&\quad \times \Pr[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E].
\end{aligned} \tag{1}$$

5.3.3 | $\Pr\Big[\tilde{\mathsf{P}}^{(N_i, w_{A_i}, \overline{a_i})}\big(\mathsf{HashN}[\tilde{\mathsf{P}}](A_i)\big) = S_i, i = 1, \ldots, q_e\Big]$

We follow the approach of [32]. Given $\tilde{\mathsf{P}}$, we define a 'bad predicate' BadH on $\tilde{\mathsf{P}}$: $\mathsf{BadH}(\tilde{\mathsf{P}})$ holds if there exist $(N_i, A_i, S_i, M_i, C_i, T_i)$, $(N_j, A_j, S_j, M_j, C_j, T_j) \in \mathcal{Q}_E$ such that $N_i = N_j$, $A_i \neq A_j$, $(a_i, a_{A_i}) = (a_j, a_{A_j})$, though $H_i = \mathsf{HashN}[\tilde{\mathsf{P}}](A_i) = \mathsf{HashN}[\tilde{\mathsf{P}}](A_j) = H_j$.

In [14] (Case 3–2, page 78),[5] it was proved that

$$\Pr_{\tilde{\mathsf{P}}}\left[H_i = H_j | N_i = N_j \wedge A_i \neq A_j \wedge (a_i, a_{A_i}) = \left(a_j, a_{A_j}\right)\right] \leq \frac{3}{2^n}$$

for any (i, j). Therefore,

$$\Pr\left[\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)\right] \leq \sum_{(N_i,A_i,S_i,M_i,C_i,T_i)} \sum_{\left(N_j,A_j,S_j,M_j,C_j,T_j\right):N_j=N_i} \frac{3}{2^n} \leq \frac{3\mu q_e}{2^n}.$$

It is easy to see that, conditioned on $\neg\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)$, $H_i = H_j \Leftrightarrow S_i = S_j$ holds for any (i, j) with $N_i = N_j \wedge A_j \neq A_j \wedge (a_i, w_{A_i}) = \left(a_j, w_{A_j}\right)$. By this,

$$\begin{aligned}
&\Pr\left[\tilde{\mathsf{P}}^{\left(N_i, w_{A_i}, \overline{a_i}\right)}(H_i) = S_i, i = 1, \ldots, q_e\right] \\
&\geq \Pr\left[\tilde{\mathsf{P}}^{\left(N_i, w_{A_i}, \overline{a_i}\right)}(H_i) = S_i, i = 1, \ldots, q_e \wedge \neg\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)\right] \\
&\geq \left(1 - \Pr\left[\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)\right]\right) \\
&\quad \times \prod_{i=1}^{q_e} \underbrace{\Pr\left[\tilde{\mathsf{P}}^{\left(N_i, w_{A_i}, \overline{a_i}\right)}(H_i) = S_i | \tilde{\mathsf{P}}^{\left(N_j, w_{A_j}, \overline{a_j}\right)}(H_j) = S_j, j = 1, \ldots, i-1 \wedge \neg\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)\right]}_{p_i}.
\end{aligned}$$

Now:

- If $\left(N_i, w_{A_i}, \overline{a_i}\right) \neq \left(N_j, w_{A_j}, \overline{a_j}\right)$ for all $j \in [i-1]$, then clearly $p_i = 1/2^n$;
- If $(N_i, A_i) = (N_j, A_j)$ for some $j \in [i-1]$, then $p_i = 1$;
- Finally, if $\left(N_i, w_{A_i}, \overline{a_i}\right) = \left(N_j, w_{A_j}, \overline{a_j}\right)$ (though $A_i \neq A_j$) for some $j \in [i-1]$, then:
  - $H_i \neq H_j$ conditioned on $\neg\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)$;
  - $S_i \neq S_j$ conditioned on $\neg$(B-1);
  - The number of $j \in [i-1]$ such that $\left(N_i, w_{A_i}, \overline{a_i}\right) = \left(N_j, w_{A_j}, \overline{a_j}\right)$ is at most μ by our assumption on nonce reuse.

Thus, conditioned on $\tilde{\mathsf{P}}^{\left(N_j, w_{A_j}, \overline{a_j}\right)}(H_j) = S_j, j = 1, \ldots, i-1$, $\tilde{\mathsf{P}}^{\left(N_i, w_{A_i}, \overline{a_i}\right)(H_i)}$ remains uniformly distributed in a set of size at least $2^n - \mu$, and the set includes the 'target' S_i. By these, $1/2^n < p_i \leq 1/(2^n - \mu)$ in this case.

[5] More clearly, their Case 3-2 considers the probability to have $\tilde{\mathsf{P}}^{(N, w_A, \overline{a})}(\mathsf{HashN}[\tilde{\mathsf{P}}](A)) = \tilde{\mathsf{P}}^{\left(N', w_{A'}, \overline{a'}\right)}(\mathsf{HashN}[\tilde{\mathsf{P}}](A'))$ for an encryption query (N, A, M, C, T) and a decryption query (N', A', C', T') such that $N = N'$, $C = C'$, $A \neq A'$ though $(a, w_A) = (a', w_{A'})$. This equals the probability to have the hash collision $\mathsf{HashN}[\tilde{\mathsf{P}}](A) = \mathsf{HashN}[\tilde{\mathsf{P}}](A')$, and the probability $3/2^n$ can be extracted from [14].

As per our assumption, the number of distinct pairs (N, A) in the encryption queries is α. This also provides the number of i such that $p_i < 1$. By this, Equation (1) is simplified to

$$\begin{aligned}
&\frac{\Pr[T_{\mathsf{re}} = \mathcal{Q}]}{\Pr[T_{\mathsf{id}} = \mathcal{Q}]} \\
&\geq 2^{\alpha n} \times \left(1 - \Pr\left[\mathsf{BadH}\left(\tilde{\mathsf{P}}\right)\right]\right) \times \left(\frac{1}{2^n}\right)^{\alpha} \times \Pr[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E] \\
&\geq \left(1 - \frac{3\mu q_e}{2^n}\right) \times \Pr[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E].
\end{aligned}$$

5.3.4 | Analysing $\mathcal{Q}_D$

It remains to bound $\Pr[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E]$. For this, we use

$$\begin{aligned}
\Pr\left[T_{\mathsf{re}} = \mathcal{Q}_D | \mathcal{Q}_E\right] &= 1 - \Pr\left[\mathcal{D}\left[\tilde{\mathsf{P}}\right](\mathtt{N}_i, \mathtt{A}_i, \mathtt{C}_i, \mathtt{T}_i) \neq \bot\right. \\
&\qquad \left.\text{for some } (\mathtt{N}_i, \mathtt{A}_i, \mathtt{C}_i, \mathtt{T}_i, b_i) \in \mathcal{Q}_D | \mathcal{Q}_E\right] \\
&\geq 1 - q_d \times \max_{i \in [q_d]} \Pr\left[\mathcal{D}\left[\tilde{\mathsf{P}}\right](\mathtt{N}_i, \mathtt{A}_i, \mathtt{C}_i, \mathtt{T}_i) \neq \bot | \mathcal{Q}_E\right].
\end{aligned} \tag{2}$$

To analyse $\max_{i \in [q_d]} \Pr\left[\mathcal{D}\left[\tilde{\mathsf{P}}\right](\mathtt{N}_i, \mathtt{A}_i, \mathtt{C}_i, \mathtt{T}_i) \neq \bot | \mathcal{Q}_E\right]$, we consider an arbitrary decryption query $(\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$ (omitting the subscript) and follow the analysis in [14]. Our analysis deviates from [14] in that our condition that encryption queries yield the extended transcript $\mathcal{Q}_E$ has a non-negligible impact on the randomness $\tilde{\mathsf{P}}$, and this will be reflected in the subsequent Case 3. Concretely, let a' and m' be AD and ciphertext block lengths of the single decryption query $(\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$, and let $w_{\mathtt{A}}$ and $w_{\mathtt{C}}$ be the corresponding constants. Let $\mathtt{T}^*$ be the true tag value for $(\mathtt{N}, \mathtt{A}, \mathtt{C})$, that is,

$$\Pr\left[\mathcal{D}\left[\tilde{\mathsf{P}}\right](\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T}) \neq \bot | \mathcal{Q}_E\right] = \Pr_{\tilde{\mathsf{P}}}[\mathtt{T}^* = \mathtt{T} | \mathcal{Q}_E].$$

Following Iwata et al. [14], [pages 76–79], we consider three cases.

Case 1 $\mathtt{N} \neq N_i$ for all $i \in [q_e]$.

The analysis just follows Case 1 of [14, page 76]. Briefly, during $\mathcal{D}[\tilde{\mathsf{P}}](\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$, the final 'tag generation' TBC-call (line 11 in Figure 1) will use a unique tweak $(\mathtt{N}, w_{\mathtt{C}}, \overline{m'})$ that is different from all the tweaks used in the q_e encryption queries. This means the produced true tag $\mathtt{T}^*$ is uniformly distributed, and $\Pr_{\tilde{\mathsf{P}}}[\mathtt{T}^* = \mathtt{T}|\mathcal{Q}_E] = 1/2^\tau$.

Case 2 $\mathtt{N} = N_i$ for some $i \in [q_e]$, though $\mathtt{C} \neq C_i$

Let $H_i = \mathsf{HashN}[\tilde{\mathsf{P}}](A_i)$, $\mathtt{H} = \mathsf{HashN}[\tilde{\mathsf{P}}](\mathtt{A})$, $\mathtt{S} = \tilde{\mathsf{P}}^{(\mathtt{N}, w_{\mathtt{A}}, \overline{a'})(\mathtt{H})}$. We are able to follow the analysis of Case 2 of [14, page 76]. The core idea is that, to have $\mathtt{T} = \mathtt{T}^*$ for the true tag $\mathtt{T}^*$ for $(\mathtt{N}, \mathtt{A}, \mathtt{C})$, it has to be either $H_i \neq \mathtt{H}$ and $H_i, \mathtt{H}$ satisfy certain 'non-trivial' relations, or the two processes $\mathsf{Encrypt}[\tilde{\mathsf{P}}](N_i, S_i, M_i)$ and $\mathsf{Decrypt}[\tilde{\mathsf{P}}](\mathtt{N}, \mathtt{S}, \mathtt{C})$ made distinct calls to $\tilde{\mathsf{P}}$ with outputs satisfy certain 'non-trivial' relations. But in both cases, distinct calls to $\tilde{\mathsf{P}}$ give rise to two random n-bit intermediate values, and the probability to have such relations is $O\ (1/2^\tau)$. More precisely, it holds $\Pr_{\tilde{\mathsf{P}}}[\mathtt{T}^* = \mathtt{T}|\mathcal{Q}_E] = 2/2^\tau + 2/2^n$.

Case 3 $\mathtt{N} = N_i$ for some $i \in [q_e]$, and $\mathtt{C} = C_i$.

This means $\mathtt{A} \neq A_i$. For simplicity, we omit the index i and abbreviate $N_i, A_i, S_i, M_i, \ldots$ as $N, A, S, M, \ldots$ and so on. We define $X\ [j]$ and $Y\ [j]$ as the jth $\tilde{\mathsf{P}}$ input and output in the message encryption of this encryption query. Since the number of blocks in M is m, we have $j \in \{1, \ldots, m\}$. Moreover, when $j < m$, $Y\ [j]$ is to encrypt $M\ [j+1]$, and $X\ [m]$ is given to $\tilde{\mathsf{P}}$ with tweak $(N, w_M, \overline{m})$ to create $Y\ [m]$ which further yields the tag T. Recall that $S = \tilde{\mathsf{P}}^{(N, w_A, \overline{a})}(\mathsf{HashN}[\tilde{\mathsf{P}}](A))$. Similarly, define $\mathtt{X}[j]$ and $\mathtt{Y}[j]$ as the jth $\tilde{\mathsf{P}}$ input and output in the message encryption of the decryption query $(\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$, and let $\mathtt{S} = \tilde{\mathsf{P}}^{(\mathtt{N}, w_{\mathtt{A}}, \overline{a'})}(\mathsf{HashN}[\tilde{\mathsf{P}}](\mathtt{A}))$. Note that $\mathtt{C} = C$ as we assumed, which means

$$X[m] = \mathtt{X}[m] \Leftrightarrow S = \mathtt{S}.$$

Thus,

$$\begin{aligned}
&\Pr[\mathtt{T}^* = \mathtt{T}|\mathcal{Q}_E] \\
&\leq \Pr[\mathtt{T}^* = \mathtt{T}|X[m] \neq \mathtt{X}[m] \wedge \mathcal{Q}_E] + \Pr[X[m] = \mathtt{X}[m]|\mathcal{Q}_E] \\
&\leq \frac{2}{2^\tau} + \Pr[X[m] = \mathtt{X}[m]|\mathcal{Q}_E] \\
&\leq \frac{2}{2^\tau} + \Pr[S = \mathtt{S}|\mathcal{Q}_E].
\end{aligned}$$

Following Case 3 in [14, page 78], we further distinguish two subcases.

- Subcase 3.1: $(a, w_A) \neq (a', w_{\mathtt{A}})$. Then, $\mathtt{S}$ is random and independent of S as tweaks are different. This means $\Pr[S = \mathtt{S}|\mathcal{Q}_E] = 1/2^n$. This is the same as Case 3-1 in [14, page 78].
- Subcase 3.2: $(a, w_A) = (a', w_{\mathtt{A}})$. This is the same as Case 3-2 in [14, page 78]. In this subcase, the event $S = \mathtt{S}$ is equivalent with $H = \mathtt{H}$. The event $H = \mathtt{H}$ only depends on $\tilde{\mathsf{P}}^{T_w}$ with tweak T_w of the form (★, 8, ★), which is independent of $\tilde{\mathsf{P}}^{T_w}$ with $T_w \in$ {(★, 24, ★), (★, 26, ★), (★, 4, ★), (★, 20, ★), (★, 21, ★)} used for encryption. Iwata et al. [14, page 79] proved that when an ('unextended') encryption query transcript $\mathcal{Q}_E$ has no nonce repetition, it holds[6]

$$\Pr_{\tilde{\mathsf{P}}}[H = \mathtt{H}|\mathcal{Q}_E] \leq \frac{3}{2^n}.$$

When $\mathcal{Q}_E$ has no nonce repetition, all the ciphertexts $C_1, \ldots, C_{q_e}$ and tags $T_1, \ldots, T_{q_e}$ are uniform and independent strings, and actually no information on the partial tweakable random permutation $\tilde{\mathsf{P}}^{T_w}$ with tweak T_w of the form (★, 8, ★) can be gained from $\mathcal{Q}_E$. In other words, Iwata et al. actually proved

$$\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}[H = \mathtt{H}] \leq \frac{3}{2^n}. \tag{3}$$

In our case, the situation deviates: conditioned on a good transcript $\mathcal{Q}_E = ((N_1, A_1, S_1, M_1, C_1, T_1), \ldots, (N_{q_e}, A_{q_e}, S_{q_e}, M_{q_e}, C_{q_e}, T_{q_e}))$, it holds $S_j \neq S_{j'}$ for any pair of indices (j, j') with $N_j = N_{j'}$, $A_j \neq A_{j'}$ and $(a_j, w_{A_j}) = (a_{j'}, w_{A_{j'}})$. This means $\tilde{\mathsf{P}}$ satisfies $\mathsf{HashN}[\tilde{\mathsf{P}}](A_j) \neq \mathsf{HashN}[\tilde{\mathsf{P}}](A_{j'})$ for any pair (j, j') such that $N_j = N_{j'}$, $A_j \neq A_{j'}$ and $(a_j, w_{A_j}) = (a_{j'}, w_{A_{j'}})$, that is, the bad predicate $\mathsf{BadH}(\tilde{\mathsf{P}})$ is *not* fulfilled. Thus,

$$\Pr_{\tilde{\mathsf{P}}}[H = \mathtt{H}|\mathcal{Q}_E] = \Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H = \mathtt{H}| \neg \mathsf{BadH}(\tilde{\mathsf{P}})\right].$$

This affects the concrete bound. Though, we have

$$\begin{aligned}
\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}[H = \mathtt{H}] = &\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H = \mathtt{H} \wedge \mathsf{BadH}(\tilde{\mathsf{P}})\right] \\
&+ \Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H = \mathtt{H} \wedge \neg\mathsf{BadH}(\tilde{\mathsf{P}})\right],
\end{aligned}$$

meaning that

[6] This can be derived from [14], Equation (10) and the subsequent bound $p_e \leq 2/2^\tau + 3/2^n$.

$$\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H=\mathtt{H} \mid \neg\,\mathsf{BadH}(\tilde{\mathsf{P}})\right]=\frac{\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H=\mathtt{H}\wedge\neg\mathsf{BadH}(\tilde{\mathsf{P}})\right]}{\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[\neg\mathsf{BadH}(\tilde{\mathsf{P}})\right]}$$

$$\leq \Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}[H=\mathtt{H}]\Big/\left(1-\frac{3\mu q_e}{2^n}\right).$$

Under the condition that $\mu q_e \leq 2^n/6$ and using Equation (3), we finally obtain

$$\Pr_{\tilde{\mathsf{P}}^{(\star,8,\star)}}\left[H=\mathtt{H} \mid \neg\,\mathsf{BadH}(\tilde{\mathsf{P}})\right]\leq\frac{6}{2^n}.$$

Injecting the above results into Equation (2) finally yields

$$\Pr[\mathcal{T}_{\mathsf{re}}=\mathcal{Q}_D|\mathcal{Q}_E]\geq 1-\frac{6q_d}{2^n}-\frac{2q_d}{2^\tau}$$

and

$$\frac{\Pr[\mathcal{T}_{\mathsf{re}}=\mathcal{Q}]}{\Pr[\mathcal{T}_{\mathsf{id}}=\mathcal{Q}]}\geq\left(1-\frac{3\mu q_e}{2^n}\right)\times\left(1-\frac{6q_d}{2^n}-\frac{2q_d}{2^\tau}\right)$$

$$\geq 1-\left(\frac{3\mu q_e}{2^n}+\frac{6q_d}{2^n}+\frac{2q_d}{2^\tau}\right),$$

and thus the final bound.

6 | NONCE-MISUSE RESILIENCE OF GIFT-COFB

We establish misuse resilience security for GIFT-COFB.

Theorem 2 *Let* A_1 *be a privacy adversary against GIFT-COFB using* q_e *encryption queries with a total number of effective blocks* $\sigma_{\mathtt{priv}}$*, and time complexity* t_{A_1}*, and let* A_2 *be an authenticity adversary using* q_e *encryption and* q_d *decryption queries with a total number of effective blocks for encryption and decryption queries* $\sigma_{\mathtt{auth}}$ *and time complexity* t_{A_2}*. Let* $\ell_{\max}$ *denote the maximum number of effective blocks in one query of* A_2*. Then*

$$\mathbf{Adv}^{\mathsf{nmrl-priv}}_{\mathsf{GIFT-COFB}[E_K]}(\mathsf{A}_1)\ \leq \mathbf{Adv}^{\mathsf{prp}}_{E}(\mathsf{B}_1)+\frac{5\sigma^2_{\mathtt{priv}}}{2^{n/2}},$$

$$\mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{GIFT-COFB}[E_K]}(\mathsf{A}_2)\ \leq \mathbf{Adv}^{\mathsf{prp}}_{E}(\mathsf{B}_2)+\frac{5\sigma^2_{\mathtt{auth}}}{2^{n/2}}+\frac{4q_d\ell_{\max}}{2^n}$$

hold for some $(\sigma_{\mathtt{priv}}, t_{A_1}+O(\sigma_{\mathtt{priv}}))$*-PRP adversary* B_1*, and for some* $(\sigma_{\mathtt{auth}}, t_{A_2}+O(\sigma_{\mathtt{auth}}))$*-PRP adversary* B_2.

6.1 | Proof overview of Theorem 2

Our proofs have two steps. At the first step, we introduce a TBC called $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$ based on E_K. This definition is not explicitly shown in the specification document; however, we present an equivalent representation to $\mathsf{GIFT-COFB}[E_K]$ using $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$. We show $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$ has $n/4$-bit TPRP security. In the second step, we analyse the NMRL-PRIV/-AUTH advantage for the idealised variant of GIFT-COFB that uses a TURP instead of $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$. We also note that it seems infeasible to reuse the original proof [20] for our purpose as its non-modular approach. This requires us to take a different approach.

The underlying TBC. Let $n = 128$, $\mathcal{M}=\{0,1\}^n$, $\mathcal{T}^{\mathsf{cofb}}_w=\{0,1\}^n\times\mathcal{B}$, where $\mathcal{B}=(\mathcal{I}\times\mathcal{J})\cup\mathcal{H}$, $\mathcal{I}=[\![2^{51}+1]\!]$, $\mathcal{J}=[\![5]\!]$, $\mathcal{H}=\{*_0,*_1,*_2,*_3,*_4\}$ be the tweak space. For any valid tweak (N, B) for $B\in\mathcal{I}\times\mathcal{J}$, we assume $B\notin\{(0, 0), (0, 1)\}$.

Definition 8 *Let* $\mathsf{gXE}^{\mathsf{cofb}}[E_K]:\mathcal{T}^{\mathsf{cofb}}_w\times\mathcal{M}\to\mathcal{M}$ *be a TBC based on an n-bit block cipher* $E:\mathcal{K}\times\mathcal{M}\to\mathcal{M}$*, where* $\mathcal{T}^{\mathsf{cofb}}_w$ *and* $\mathcal{M}$ *are as defined above. For plaintext* $M\in\mathcal{M}$ *and tweak* $T=(N,B)\in\mathcal{T}^{\mathsf{cofb}}_w$*, the ciphertext* $C=\mathsf{gXE}^{\mathsf{cofb}}[E_K](T,M)$ *is such that*

$$C=\begin{cases}E_K\left(M\oplus\left(2L\parallel 0^{n/2}\right)\oplus G_{\mathtt{C}}(E_K(N))\right), & \text{if } B=*_0\in\mathcal{H}\\ E_K\left(M\oplus\left(3^iL\parallel 0^{n/2}\right)\oplus G_{\mathtt{C}}(E_K(N))\right), & \text{if } B=*_i\in\mathcal{H}, i\in[4],\\ E_K\left(M\oplus\left(2^i3^jL\parallel 0^{n/2}\right)\right) & \text{if } B=(i,j)\in\mathcal{I}\times\mathcal{J}\end{cases}$$

where $L=\mathtt{msb}_{n/2}(E_K(N))$ *and* $G_{\mathtt{C}}$ *are as defined at* 3.2.

Definition 8 is a variant of generalised XE/XEX mode [3]. The TPRP advantage of $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$ is proved as follows, using [33, Theorem 4.1].

Theorem 3 *For any adversary* A *using* q *encryption queries,*

$$\mathbf{Adv}^{\mathsf{tprp}}_{\mathsf{gXE^{COFB}}}[\mathsf{P}](\mathsf{A})\leq\frac{5q^2}{2^{n/2}},$$

where P *is an n-bit URP.*

We devote to prove Theorem 3 in the remaining of this subsection. We observe that Definition 8 is a variant of generalised XE/XEX mode [3]. To prove its security, we rely on the following theorem, which is obtained by simplifying [33, Theorem 4.1]. The scheme in [33] is as follows[7]. Let $\mathsf{gXE}[E_K] : \mathcal{T}_w \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{T}_w = \{0,1\}^n \times \mathcal{B}$ for a finite set $\mathcal{B}$, be a generalised XE mode such that, for plaintext $M \in \{0,1\}^n$ and tweak $T = (N, B) \in \mathcal{T}_w$, the ciphertext C is

$$C = E_K(M \oplus S),$$

where $V = E_K(N)$ and $S = F(B, V)$ for some (deterministic) functions $F : \mathcal{B} \times \{0,1\}^n \to \{0,1\}^n$.

Definition 9 *[33] Let $F : \mathcal{B} \times \{0,1\}^n \to \{0,1\}^n$. F is said to be (ϵ, γ, ξ)-uniform if*

$$\max\left\{\max_{B \neq B, \delta \in \{0,1\}^n} \Pr[F(B,V) \oplus F(B',V) = \delta],\right.$$

$$\left.\max_{B,B',\delta \in \{0,1\}^n} \Pr[F(B,V) \oplus F(B',V') = \delta]\right\} \leq \epsilon,$$

$$\max_{B,\delta \in \{0,1\}^n} \Pr[F(B,V) = \delta] \leq \gamma,$$

$$\max_{B,\delta \in \{0,1\}^n} \Pr[F(B,V) \oplus V = \delta] \leq \xi$$

hold, where the probability is defined by V and V' (if exists), independently and uniformly distributed over $\{0,1\}^n$.

Theorem 4 *If F is (ϵ, γ, ξ)-uniform and P is an n-bit URP, we have*

$$\mathbf{Adv}^{\mathsf{tprp}}_{\mathsf{gXE[P]}}(\mathsf{A}) \leq q^2\left(2\epsilon + \gamma + \xi + \frac{1}{2^n + 1}\right).$$

for adversary A using q encryption queries.

Theorem 4 is a simplified version of [33, Theorem 4.1] obtained by removing the decryption oracle and the 'optional encryption' oracle[8].

The TBC $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$ of Def. 8 is an instantiation of $\mathsf{gXE}[E_K]$ using F defined as follows, using $L = \mathtt{msb}_{n/2}(V)$.

$$F(B,V) = \begin{cases} G_{\mathtt{C}}(V) \oplus 2L \,\|\, 0^{n/2} & \text{if} B = *_0 \in \mathcal{H} \\ G_{\mathtt{C}}(V) \oplus 3^i L \,\|\, 0^{n/2} & \text{if} B = *_i \in \mathcal{H}, \text{for} i \in [4] \\ 2^i 3^j L \,\|\, 0^{n/2} & \text{if} B = (i,j) \in \mathcal{I} \times \mathcal{J}. \end{cases} \quad (4)$$

Lemma 1 *The F of (4) is $(1/2^{n/2}, 1/2^{n/2}, 1/2^{n/2})$-uniform.*

Proof Let $L = \mathtt{msb}_{n/2}(V)$ and $\overline{L} = \mathtt{lsb}_{n/2}(V)$. When $B \in \mathcal{H}$, let $\beta \in \{2, 3, 3^2, 3^3, 3^4\}$ be the associated coefficient of L. From the definition of $G_{\mathtt{C}}$ in GIFT-COFB, we observe that $H(V) := G_{\mathtt{C}}(V) \oplus \beta L \,\|\, 0^{n/2}$ is equal to a pair of 64 bits, $(\beta L \oplus \overline{L}, L \lll 1)$. Note that, when V is uniform $H(V)$ is also uniform because $L \lll 1$ is uniform, and that $\beta L \oplus \overline{L}$ is also uniform given L. From this fact and the injectivity of $2^i 3^j$ mapping for $n = 128$ shown by Rogaway [3], for γ, we have

$$\Pr[F(B,V) = \delta] = \begin{cases} \Pr\left[G_{\mathtt{C}}(V) \oplus \beta L \,\|\, 0^{n/2} = \delta\right] \leq \dfrac{1}{2^n} & \text{if} B \in \mathcal{H} \\ \Pr\left[2^i 3^j L \,\|\, 0^{n/2} = \delta\right] \leq \dfrac{1}{2^{n/2}} & \text{if} B = (i,j) \in \mathcal{I} \times \mathcal{J} \end{cases}$$

For ϵ, let $B \neq B'$ and we have

$$\Pr[F(B,V) \oplus F(B',V) = \delta] = \begin{cases} \Pr\left[\beta L \,\|\, 0^{n/2} \oplus \beta' L \,\|\, 0^{n/2} = \delta\right] \leq \dfrac{1}{2^{n/2}} & \text{if} B, B' \in \mathcal{H} \\ \Pr\left[G_{\mathtt{C}}(V) \oplus \beta L \,\|\, 0^{n/2} \oplus 2^i 3^j L \,\|\, 0^{n/2} = \delta\right] \leq \dfrac{1}{2^n} & \text{if} B \in \mathcal{H}, B' = (i,j) \\ \Pr\left[2^i 3^j L \oplus 2^{i'} 3^{j'} L \,\|\, 0^{n/2} = \delta\right] \leq \dfrac{1}{2^{n/2}} & \text{if} B = (i,j), B' = (i',j'), \end{cases} \quad (5)$$

where β and β' are associated coefficients of B and B' when they are in $\mathcal{H}$. The first case of Equation (5) follows from the uniformity of the first $n/2$-bit part, given L and $\beta \neq \beta'$. The second case follows from the uniformity of $G_{\mathtt{C}}(V)$. The third

[7] The paper [33] defines a generalised XEX mode with 'optional encryption', a form of even more generalised TBC. Our presentation here is reduced to what we just need.

[8] Since we only need a TPRP rather than a (CCA-secure) TSPRP, the conditions for F can be slightly relaxed, in particular for ξ. As this relaxation does not affect us (i.e. ξ is also small for our case), we keep the original condition.

case follows from the result of [3].

For ξ, when $B \in \mathcal{H}$,

$$\Pr[F(B,V) \oplus V = \delta] = \Pr\left[\left(\beta L \oplus \overline{L} \oplus L, (L \lll 1) \oplus \overline{L}\right) = \delta\right]$$

$$= \Pr\left[\left((\beta \oplus 1)L \oplus \overline{L}, (L \lll 1) \oplus \overline{L}\right) = \delta\right] \leq \frac{1}{2^{n/2}}$$

from the uniformity $\overline{L}$ (while $(\beta \oplus 1)L$ and $L \lll 1$ may agree on most of the bits). When $B = (i,j) \in \mathcal{I} \times \mathcal{J}$,

$$\Pr[F(B,V) \oplus V = \delta] = \Pr\left[\left(2^i 3^j \oplus 1\right)L, \overline{L}) = \delta\right] \leq \frac{1}{2^n}$$

from the uniformity $\overline{L}$ and independence from L. Thus, we have $\epsilon = \gamma = \xi = 1/2^{n/2}$. This proves Lemma 1.Combining Lemma 1 and Theorem 4, we obtain Theorem 3.

6.2 | Proof for NMRL-PRIV bound of Theorem 2

We observe that $\mathsf{GIFT-COFB}[E_K]$ can be seen as a mode of TBC $\mathsf{gXE}^{\mathsf{cofb}}[E_K]$, which we call idealised GIFT- COFB(iGC) shown in Figure 4 in the Appendix. As $\mathsf{iGC}\left[\mathsf{gXE}^{\mathsf{cofb}}[\mathsf{P}]\right]$ is equivalent to $\mathsf{GIFT-COFB}[\mathsf{P}]$ for URP P, and from Theorem 3, we have

$$\mathbf{Adv}^{\mathsf{nmrl-priv}}_{\mathsf{GIFT-COFB}[\mathsf{P}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathsf{tprp}}_{\mathsf{gXE}^{\mathsf{cofb}}[\mathsf{P}]}(\mathsf{B}) + \mathbf{Adv}^{\mathsf{nmrl-priv}}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}(\mathsf{A}) \quad (6)$$

$$\leq \frac{5\sigma^2_{\mathtt{priv}}}{2^{n/2}} + \mathbf{Adv}^{\mathsf{nmrl-priv}}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}(\mathsf{A}) \leq \frac{5\sigma^2_{\mathtt{priv}}}{2^{n/2}}$$

for an adversary B using $\sigma_{\mathtt{priv}}$ queries. The last inequality follows from the same reason as Romulus-N: all the ciphertext blocks and the tags are generated by $\tilde{\mathsf{P}}$ taking distinct tweak values.

6.3 | Proof for NMRL-AUTH bound of Theorem 2

Similar to Equation (6), we have

$$\mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{GIFT-COFB}[\mathsf{P}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathsf{tprp}}_{\mathsf{gXE}^{\mathsf{cofb}}[\mathsf{P}]}(\mathsf{B}) + \mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}(\mathsf{A}) \quad (7)$$

$$\leq \frac{5\sigma^2_{\mathtt{auth}}}{2^{n/2}} + \mathbf{Adv}_{\mathsf{iGC}[\tilde{\mathsf{P}}]^{\mathsf{nmrl-auth}}}(\mathsf{A})$$

for an adversary B using $\sigma_{\mathtt{auth}}$ queries.

Algorithm $\mathsf{iGC}[\widetilde{E}_K]$-$\mathcal{E}_K(N,A,M)$

$(A[1],\ldots,A[a]) \xleftarrow{n} \mathtt{padc}(A)$
if $M \neq \varepsilon$ **then**
  $(M[1],\ldots,M[m]) \xleftarrow{n} M$
if $a = 1$ **then**
  if $|A| \bmod n = 0$ **and** $A \neq \varepsilon$ **then**
    if $M \neq \varepsilon$ **then** $j \leftarrow 1$
    else $j \leftarrow 3$
  else
    if $M \neq \varepsilon$ **then** $j \leftarrow 2$
    else $j \leftarrow 4$
  $Y[1] \leftarrow \widetilde{E}_K((N,*_j),A[1])$
if $a \neq 1$ **then**
  $Y[1] \leftarrow \widetilde{E}_K((N,*_0),A[1])$
  for $i = 2$ **to** $a-1$
    $S[i] \leftarrow \rho_{\mathtt{c}_1}(Y[i-1],A[i])$
    $Y[i] \leftarrow \widetilde{E}_K((N,(i,0)),S[i])$
  if $|A| \bmod n = 0$ **and** $M \neq \varepsilon$ **then** $j \leftarrow 1$
  if $|A| \bmod n \neq 0$ **and** $M \neq \varepsilon$ **then** $j \leftarrow 2$
  if $|A| \bmod n = 0$ **and** $M = \varepsilon$ **then** $j \leftarrow 3$
  if $|A| \bmod n \neq 0$ **and** $M = \varepsilon$ **then** $j \leftarrow 4$
  $S[a] \leftarrow \rho_{\mathtt{c}_1}(Y[a-1],A[a])$
  $Y[a] \leftarrow \widetilde{E}_K((N,(a-1,j)),S[a])$
for $i = 1$ **to** $m-1$
  $(S[i+a],C[i]) \leftarrow \rho_{\mathtt{c}}(Y[i+a-1],M[i])$
  $Y[i+a] \leftarrow \widetilde{E}_K((N,(i+a-1,j)),S[i+a])$
if $M \neq \varepsilon$ **then**
  if $|M| \bmod n = 0$ **then** $j \leftarrow j+1$
  else $j \leftarrow j+2$
  $(S[a+m],C[m]) \leftarrow \rho_{\mathtt{c}}(Y[a+m-1],M[m])$
  $Y[a+m] \leftarrow \widetilde{E}_K((N,(a+m-2,j)),S[a+m])$
  $C \leftarrow C[1]\|\cdots\|C[m]$
  $T \leftarrow \mathtt{msb}_\tau(Y[a+m])$
else $C \leftarrow \varepsilon$, $T \leftarrow \mathtt{msb}_\tau(Y[a])$
return (C,T)

Algorithm $\mathsf{iGC}[\widetilde{E}_K]$-$\mathcal{D}_K(N,A,C,T)$

$(A[1],\ldots,A[a]) \xleftarrow{n} \mathtt{padc}(A)$
if $C \neq \varepsilon$ **then**
  $(C[1],\ldots,C[c]) \xleftarrow{n} C$
if $a = 1$ **then**
  if $|A| \bmod n = 0$ **and** $A \neq \varepsilon$ **then**
    if $C \neq \varepsilon$ **then** $j \leftarrow 1$
    else $j \leftarrow 3$
  else
    if $C \neq \varepsilon$ **then** $j \leftarrow 2$
    else $j \leftarrow 4$
  $Y[1] \leftarrow \widetilde{E}_K((N,*_j),A[1])$
if $a \neq 1$ **then**
  $Y[1] \leftarrow \widetilde{E}_K((N,*_0),A[1])$
  for $i = 2$ **to** $a-1$
    $S[i] \leftarrow \rho_{\mathtt{c}_1}(Y[i-1],A[i])$
    $Y[i] \leftarrow \widetilde{E}_K((N,(i,0)),S[i])$
  if $|A| \bmod n = 0$ **and** $C \neq \varepsilon$ **then** $j \leftarrow 1$
  if $|A| \bmod n \neq 0$ **and** $C \neq \varepsilon$ **then** $j \leftarrow 2$
  if $|A| \bmod n = 0$ **and** $C = \varepsilon$ **then** $j \leftarrow 3$
  if $|A| \bmod n \neq 0$ **and** $C = \varepsilon$ **then** $j \leftarrow 4$
  $S[a] \leftarrow \rho_{\mathtt{c}_1}(Y[a-1],A[a])$
  $Y[a] \leftarrow \widetilde{E}_K((N,(a-1,j)),S[a])$
for $i = 1$ **to** $c-1$
  $(S[i+a],M[i]) \leftarrow \rho'_{\mathtt{c}}(Y[i+a-1],C[i])$
  $Y[i+a] \leftarrow \widetilde{E}_K((N,(i+a-1,j)),S[i+a])$
if $C \neq \varepsilon$ **then**
  if $|C| \bmod n = 0$ **then** $j \leftarrow j+1$
  else $j \leftarrow j+2$
  $(S[a+c],M[c]) \leftarrow \rho'_{\mathtt{c}}(Y[a+c-1],C[c])$
  $Y[a+c] \leftarrow \widetilde{E}_K((N,(a+c-2,j)),S[a+c])$
  $M \leftarrow M[1]\|\ldots\|M[c]$
  $T' \leftarrow \mathtt{msb}_\tau(Y[a+c])$
else $M \leftarrow \varepsilon$, $T' \leftarrow \mathtt{msb}_\tau(Y[a])$
if $T' = T$ **then return** M, **else return** $\perp$

FIGURE 4 Algorithms of $\mathsf{iGC}[\widetilde{E}_K]$, an abstraction of GIFT- COFB using a TBC.

We evaluate $\mathbf{Adv}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}^{\mathsf{nmrl-auth}}(\mathsf{A})$. The tweak values used by $\mathsf{iGC}[\tilde{\mathsf{P}}]$ always contain the nonce. This significantly simplifies the security analysis.

Analysis for $q_d = 1$. We first study the case $q_d = 1$, given $\mathcal{Q}_E = \{(N_i, A_i, M_i, C_i, T_i), i \in [q_e]\}$. The NMRL-AUTH advantage is $\mathsf{pf} := q\Pr[\mathtt{T} = T^* | \mathcal{Q}_E]$, where T^* is the true tag for the decryption query $Q_D = (\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$[9]. If $\mathtt{N} \neq N_i$ for all $i \in [q_e]$, we simply observe $\mathsf{pf} = 1/2^n$. Thus, we assume that $\mathtt{N} = N_i$ holds for some (unique by definition) $i \in [q_e]$. In this case, other tuples of encryption transcript in $\mathcal{Q}_E$ are completely independent of T^* because all $\tilde{\mathsf{P}}$ calls in $\mathsf{iGC}[\tilde{\mathsf{P}}]$ take a nonce. This implies that we just need to think about the interactions between the Q_D and ith encryption query and eventually makes the analysis identical to the case of nonce-respecting AUTH adversary against $\mathsf{iGC}[\tilde{\mathsf{P}}]$. Due to the difference in the tweak usage for block counting and in the feedback function, we cannot follow the analysis of Romulus-N. We provide a case analysis below, which is similar (but somewhat more complex because of complex domain separation) to the proof for the idealised $\mathsf{Remus-N}$, called $\mathsf{TRemus-N}$ [14].

We will use the following lemma.

Lemma 2 *Let (Y, X, M, C) be a tuple of fixed values such that $\rho_{\mathtt{C}}(Y, M) = (X, C)$ (where $M, C \in \{0,1\}^{\le \tilde{n}}$, $|M| = |C|$). Let $\mathtt{Y}$ be a random variable uniform over $\{0,1\}^n \setminus \{Y\}$. For fixed $\mathtt{C} \in \{0,1\}^{\le \tilde{n}}$, let $\mathtt{X} = \rho_{\mathtt{C}_1}(\mathtt{Y}, \mathtt{padc}(\mathtt{msb}_{|\mathtt{C}|}(\mathtt{Y}) \oplus \mathtt{C}))$.*

Then, $\Pr_{\mathtt{Y}}[\mathtt{X} = X] \le 1/2^{n-2}$ holds for any fixed $\mathtt{C} \in \{0,1\}^{\le \tilde{n}}$.

Proof For $i \in [n]$, let $I_{\mathtt{msb}_i}$ be the $n \times n$ matrix such that $I_{\mathtt{msb}_i} \cdot Z = \mathtt{msb}_i(Z) \,\|\, 0^{n-i}$ for $Z \in \{0,1\}^n$. Let $|\mathtt{C}| = s$ and assume that the rank of $G_{\mathtt{C}} \oplus I_{\mathtt{msb}_s}$ is k. Let $\mathtt{Y}_i$ denote its ith bit. We have

$$\Pr[\mathtt{X} = X] = \Pr[G_{\mathtt{C}}(\mathtt{Y}) \oplus \mathtt{padc}(\mathtt{msb}_s(\mathtt{Y}) \oplus \mathtt{C}) = X]$$

$$= \Pr\left[G_{\mathtt{C}}(\mathtt{Y}) \oplus I_{\mathtt{msb}_s}(\mathtt{Y}) \oplus \left(\mathtt{C} \| 10^{n-s-1}\right) = X\right]$$

$$\le \max_{\delta \in \{0,1\}^n} \Pr[(G_{\mathtt{C}} \oplus I_{\mathtt{msb}_s})(\mathtt{Y}) = \delta].$$

The rank tells that the above probability is $\Pr\left[\mathtt{Y}_{i_1} = \delta'_1, \ldots, \mathtt{Y}_{i_k} = \delta'_k\right]$ for some $i_1, \ldots, i_k \in [n]$ and $\delta'_i \in \{0,1\}$, $i \in [k]$. Since $\mathtt{Y}$ has uniformity $1/(2^n - 1)$ (i.e. $\max_{y \in \{0,1\}^n} \Pr[\mathtt{Y} = y] \le 1/(2^n - 1)$), this probability is at most

$$\frac{2^{n-k}}{2^n - 1} \le \frac{2}{2^k}.$$

We confirmed that the rank of $G_{\mathtt{C}} \oplus I_{\mathtt{msb}_s}$ is n for all $s \in [n-1]$, and that is, $n - 1$ when $s = n$ as mentioned earlier, using a program. So, we let $k = n - 1$ and derive $2/2^{n-1} = 1/2^{n-2}$. This completes the proof.

[9] Formally, this is not a decryption transcript as it lacks the oracle response b.

Remark. The original proof [20] uses a similar bound on the collision probability of X and $\mathtt{X}$; however, because that bound is used when the underlying primitive is a random function rather than a random permutation (i.e. after PRP-PRF switching), $\mathtt{Y}$ has uniformity $1/2^n$, that is, completely random and independent of Y.

Classification of Tweak Sequences. For each encryption or decryption query, $\mathsf{iGC}[\tilde{\mathsf{P}}]$ will generate a sequence of tweak values. If a query requires ℓ calls of $\tilde{\mathsf{P}}$, the tweaks sequence is in $\left(\mathcal{T}_w^{\mathsf{cofb}}\right)^{\ell}$ and is uniquely determined by the tuple (A, C) for encryption or $(\mathtt{A}, \mathtt{C})$ for decryption. Let $\mathsf{LI}: \{0,1\}^* \to \{e, c, p\}$ be a length-indicator function such that $\mathsf{LI}(X) = e$ (for empty) if $X = \varepsilon$, $\mathsf{LI}(X) = c$ (for complete) if $X \neq \varepsilon$ and $|X|$ is a multiple of n, and $\mathsf{LI}(X) = p$ (for partial) otherwise. For a tuple (N, A, M, C, T), we can define 9 classes depending on $\mathsf{LI}(A)$ and $\mathsf{LI}(C)$. Note that each class may have subcases, and the final tweak of any subcase is either $B \in \mathcal{H}$ or $B = (i, j) \in \mathcal{I} \times \mathcal{J}$ for some constant $j \in \{2, 3, 4\}$ specific to this class, because this j is a function of $(\mathsf{LI}(A), \mathsf{LI}(C))$.

The following lists the 9 classes of tweak sequences for an encryption query. We omit N as it is always contained. In the descriptions of subcases of a class, let $a = |A|_n$, $m = |C|_n$. The same classification also applies to a decryption query $Q_D = (\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$, using $\mathtt{A}$ and $\mathtt{C}$ instead of A and C, and using $a' = |\mathtt{A}|_n$ and $m' = |\mathtt{C}|_n$ instead of a and m.

Class 1: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (e, e)$
- **1-1** $(*_4)$

Class 2: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (e, c)$
- **2-1** $\mathrm{m} = 1$: $(*_2, (0, 3))$
- **2-2** $\mathrm{m} \ge 2$: $(*_2, (1, 2), \ldots, (m-1, 2), (m-1, 3))$

Class 3: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (e, p)$
- **3-1** $\mathrm{m} = 1$: $(*_2, (0, 4))$
- **3-2** $\mathrm{m} \ge 2$: $(*_2, (1, 2), \ldots, (m-1, 2), (m-1, 4))$

Class 4: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (c, e)$
- **4-1** $a = 1$: $(*_3)$
- **4-2** $a \ge 2$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 3))$

Class 5: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (c, c)$
- **5-1** $a = 1$, $\mathrm{m} = 1$: $(*_1, (0, 2))$
- **5-2** $a = 1$, $\mathrm{m} \ge 2$: $(*_1, (1, 1), \ldots, (m-1, 1), (m-1, 2))$
- **5-3** $a \ge 2$, $\mathrm{m} = 1$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 1), (a-1, 2))$
- **5-4** $a \ge 2$, $\mathrm{m} \ge 2$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 1), (a, 1), \ldots, (a+m-2, 1), (a+m-2, 2))$

Class 6: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (c, p)$
- **6-1** $a = 1$, $\mathrm{m} = 1$: $(*_1, (0, 3))$
- **6-2** $a = 1$, $\mathrm{m} \ge 2$: $(*_1, (1, 1), \ldots, (m-1, 1), (m-1, 3))$
- **6-3** $a \ge 2$, $\mathrm{m} = 1$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 1), (a-1, 3))$
- **6-4** $a \ge 2$, $\mathrm{m} \ge 2$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 1), (a, 1), \ldots, (a+m-2, 1), (a+m-2, 3))$

Class 7: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (p, e)$
- **7-1** $a = 1$: $(*_4)$
- **7-2** $a \ge 2$: $(*_0, (2, 0), \ldots, (a-1, 0), (a-1, 4))$

Class 8: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (p, c)$

8-1 $a = 1$, m = 1: ($*_2$, (0, 3))
8-2 $a = 1$, m $\geq$ 2: ($*_2$, (1, 2), …, ($m-1$, 2), ($m-1$, 3))
8-3 $a \geq 2$, m = 1: ($*_0$, (2, 0), …, ($a-1$, 0), ($a-1$, 2), ($a-1$, 3))
8-4 $a \geq 2$, m $\geq$ 2: ($*_0$, (2, 0), …, ($a-1$, 0), ($a-1$, 2), (a, 2), …, ($a+m-2$, 2), ($a+m-2$, 3))

Class 9: $(\mathsf{LI}(A), \mathsf{LI}(C)) = (p, p)$
9-1 $a = 1$, m = 1: ($*_2$, (0, 4))
9-2 $a = 1$, m $\geq$ 2: ($*_2$, (1, 2), …, ($m-1$, 2), ($m-1$, 4))
9-3 $a \geq 2$, m = 1: ($*_0$, (2, 0), …, ($a-1$, 0), ($a-1$, 2), ($a-1$, 4))
9-4 $a \geq 2$, m $\geq$ 2: ($*_0$, (2, 0), …, ($a-1$, 0), ($a-1$, 2), (a, 2), …, ($a+m-2$, 2), ($a+m-2$, 4))

We pick $Q_E = (N, A, M, C, T)$ and $Q_D = (\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T})$, where $\mathtt{N} = N$ but $(\mathtt{N}, \mathtt{A}, \mathtt{C}, \mathtt{T}) \neq (N, A, C, T)$, among these classes, and show a bound for pf. Let us write **Case** (i, j) to denote the case when Q_E is in **Class *i*** and Q_D is in **Class *j***, for $i, j \in [9]$. Let $\mathcal{S}_E^{\mathsf{tw}}$ $\left(\mathcal{S}_D^{\mathsf{tw}}\right)$ denote the tweak sequence of Q_E (Q_D). For example, if Q_E is in **Class 9** (**9-1**), $\mathcal{S}_E^{\mathsf{tw}} = (*_2, (0, 4))$. Recall that the actual tweak sequence is (N, $*_2$) and (N, (0, 4)).

Case (i, i) for $i \in [9]$. **Case** (1, 1) does not exist. For $i \in \{2, \ldots, 9\}$, the analysis is effectively the same; therefore, we take **Case** (8, 8) for example. For two non-empty bit sequences $X \neq \mathtt{X}$, where $|X|_n = |\mathtt{X}|_n$, let $\Delta(X, \mathtt{X}) \in \left[|X|_n\right]$ be the index of the first difference: when $i = \Delta(X, \mathtt{X})$, $X[i] \neq \mathtt{X}[i]$ and $X[j] = \mathtt{X}[j]$ for all $j \in [i-1]$, where $X[i]$ denotes the ith block. We use ℓ to denote the number of maximum $\tilde{\mathsf{P}}$ calls in a query. We further divide **Case** (8, 8) into the following subcases:

- **Subcase** (1): $a = a'$ and $m = m'$. We have $\mathcal{S}_E^{\mathsf{tw}} = \mathcal{S}_D^{\mathsf{tw}}$. We either have $A \neq \mathtt{A}$ or $A = \mathtt{A}$ and $C \neq \mathtt{C}$. In the first case, let $i = \Delta(A, \mathtt{A})$. Let ($X$, Y) be the input-output pair of the ith $\tilde{\mathsf{P}}$ call for Q_E. Define $(\mathtt{X}, \mathtt{Y})$ similarly for Q_D. By the definition of i and $\rho_{\mathtt{C}}$, $X \neq \mathtt{X}$ holds, and it means $\mathtt{Y} \xleftarrow{\$} \{0,1\}^n \setminus \{Y\}$ (as $\tilde{\mathsf{P}}$ takes an identical tweak). From Lemma 2, the collision probability between the next $\tilde{\mathsf{P}}$ block inputs is at most $1/2^{n-2}$. This means that Q_D will create a chain of random inputs to $\tilde{\mathsf{P}}$, and the encryption of the last chain value yields T^*. As we have ℓ $\tilde{\mathsf{P}}$ calls, taking the union bound, $\mathsf{pf} \leq \ell/2^{n-2}$ holds. For the second case ($A = \mathtt{A}$ and $C \neq \mathtt{C}$), the analysis is mostly identical; due to the definition of $\rho_{\mathtt{C}}$, the first ciphertext difference will create a difference in the $\tilde{\mathsf{P}}$ input, which will create a random chain with each collision probability $1/2^{n-2}$. Thus, $\mathsf{pf} \leq \ell/2^{n-2}$ holds too.
- **Subcase** (2): $a < a'$. When $a \geq 2$ (respectively, $a = 1$), (a, 0) (resp. ($*_0$)) appears only in $\mathcal{S}_D^{\mathsf{tw}}$, hence the corresponding $\tilde{\mathsf{P}}$ output is completely random. This will create a random chain for the successive $\tilde{\mathsf{P}}$ inputs and makes $\mathsf{pf} \leq \ell/2^{n-2}$.
- **Subcase** (3): $a > a'$. When $a' \geq 2$ (respectively, $a' = 1$), the tweak value ($a'-1$, 2) (resp. ($*_2$)) appears only in $\mathcal{S}_D^{\mathsf{tw}}$, hence $\mathsf{pf} \leq \ell/2^{n-2}$ holds in the same manner to the above case.
- **Subcase** (4): $a = a'$, $m \neq m'$. The last value of $\mathcal{S}_D^{\mathsf{tw}}$ is unique, hence $\mathsf{pf} \leq 1/2^n$ holds.

Hence, $\mathsf{pf} \leq \ell/2^{n-2}$ holds for **Case**(8, 8). As mentioned earlier, other **Case**(i, i) for all $i \neq 8$ are similarly proved with the same bound.

Case (i, j) for $i \neq j$. For most of the cases, the analysis is simple as there is a unique value that appears only in $\mathcal{S}_D^{\mathsf{tw}}$. From the same analysis as above, it makes $\mathsf{pf} \leq \ell/2^{n-2}$.

Still, there are two categories of **Case** (i, j) that need a different analysis. The first category consists of **Case** (1, 7), **Case** (7, 1), **Case** (2, 8), **Case** (8, 2), **Case** (3, 9), and **Case** (9, 3). The second category consists of **Case** (6, 4), **Case** (8, 4), and **Case** (9, 7).

The first category allows $\mathcal{S}_D^{\mathsf{tw}} = \mathcal{S}_E^{\mathsf{tw}}$. But all the cases included in this category have either A is empty and $\mathtt{A}$ is partial (or vice versa), while the first tweak value may or may not be identical. Thanks to the property of $\mathtt{padc}$, this means that the first (tweak, block) input tuples to $\tilde{\mathsf{P}}$ are always different, and its output in Q_D will create a random chain to the last $\tilde{\mathsf{P}}$ input, from the same reason as in **Case** (i, i), irrespective of the lengths of queries. So $\mathsf{pf} \leq \ell/2^{n-2}$ holds for this category.

The second category is somewhat special because $\mathcal{S}_D^{\mathsf{tw}}$ can be a subset of $\mathcal{S}_E^{\mathsf{tw}}$. We take **Case** (6, 4), for example, when $a \geq 2$, m = 1 (**Class6 − 3**) and $a' \geq 2$ and $\mathtt{C}$ is empty (**Class4 − 2**). If $a \neq a'$, the last value in $\mathcal{S}_D^{\mathsf{tw}}$, namely ($a'-1$, 3), is new, so $\mathcal{S}_D^{\mathsf{tw}} \not\subseteq \mathcal{S}_E^{\mathsf{tw}}$ and $\mathsf{pf} \leq 1/2^n$. However, when $a = a'$, $\mathcal{S}_D^{\mathsf{tw}} \subset \mathcal{S}_E^{\mathsf{tw}}$ holds as $\mathcal{S}_D^{\mathsf{tw}} = \mathcal{S}_E^{\mathsf{tw}} \setminus \{(a-1, 1)\}$. Let ($X_0$, Y_0), (X_1, Y_1), and (X_2, $Y_2 = T$) be the I/O pairs of the last three $\tilde{\mathsf{P}}$ for Q_E. Similarly, let $(\mathtt{X}_0, \mathtt{Y}_0)$, $(\mathtt{X}_1, \mathtt{Y}_1 = T^*)$ be the last two I/O pairs of $\tilde{\mathsf{P}}$ for Q_D. If $\mathtt{X}_1 = X_2$ holds, it leads to a forgery. Q_E reveals Y_1, X_2, and T. However, X_1 is completely random, given Q_E, as the corresponding tweak ($a-1$, 1) in $\mathcal{S}_E^{\mathsf{tw}}$ are used only once in $\mathcal{Q}_E$ (together with N). As Y_0 is a permutation of X_1 given A [a], this makes Y_0 random too. If $a = a'$ and $\Delta(A, \mathtt{A}) = a$ or just $A = \mathtt{A}$, we have $Y_0 = \mathtt{Y}_0$, and the randomness of Y_0 ensures

$$\Pr[\mathtt{X}_1 = X_2] = \Pr[G_{\mathtt{C}}(\mathtt{Y}_0) \oplus \mathtt{A}[a] = X_2] \leq \frac{1}{2^n}$$

irrespective of the choice of $\mathtt{A}[a]$. Unless $\mathtt{X}_1 = X_2$, T^* is random, which means $\mathsf{pf} \leq 2/2^n$. If $a = a'$ and $\Delta(A, \mathtt{A}) < a$, there is a pair of distinct inputs to $\tilde{\mathsf{P}}$ taking the same tweak, which creates a random chain. As before, we have $\mathsf{pf} \leq \ell/2^{n-2}$. Other cases in the second category follow similarly. Summarising the entire case analysis, $\mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}(\mathsf{A}) \leq \ell/2^{n-2}$ when $q_d = 1$. The bound for general $q_d \geq 1$ is obtained by multiplying q_d:

$$\mathbf{Adv}^{\mathsf{nmrl-auth}}_{\mathsf{iGC}[\tilde{\mathsf{P}}]}(\mathsf{A}) \leq \frac{q_d \ell}{2^{n-2}} \tag{8}$$

for adversary A using q_d decryption queries and maximum input block length (for both encryption and decryption) ℓ. From Def. 8 and Figure 4, $\ell \leq \ell_{\max}$ holds for any query. From this and Equations (7) and (8), we conclude the proof.

7 | CONCLUSION

We have shown that the two finalists of NIST Lightweight Cryptography project, Romulus-N and GIFT-COFB, have nonce-misuse resilience privacy and authenticity, while originally defined as nonce-based AE schemes. We also show that they do not have stronger, misuse resistant security. Hence, our results are qualitatively tight with respect to the security guarantee under nonce misuse. Such security features would provide an additional defense for these schemes in practical use cases. For GIFT-COFB, an open question is to find matching attacks resolving the tightness of nonce-misuse resilience bounds. In addition, studying nonce-misuse resilience/resistance of other finalists, both from the attack and provable security perspectives, would be an interesting topic for future work.

AUTHOR CONTRIBUTIONS

Akiko Inoue: Formal analysis; Investigation; Writing – Original draft preparation. **Chun Guo**: Formal analysis; Investigation; Writing – Original draft preparation. **Kazuhiko Minematsu**: Conceptualisation; Investigation; Writing – Original draft preparation.

ACKNOWLEDGEMENTS

We thank Mustafa Khairallah, Shoichi Hirose, Akinori Hosoyamada, Ryoma Ito, Tetsu Iwata, Thomas Peyrin, Ferdinand Sibleyras, and Yosuke Todo for (initial) discussions. We would like to thank the anonymous reviewers for many helpful comments. Chun Guo was partly supported by the National Natural Science Foundation of China (Grant No. 62002202) and the Shandong Nature Science Foundation of China (Grant No. ZR2020MF053).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Akiko Inoue https://orcid.org/0000-0002-0173-7245
Chun Guo https://orcid.org/0000-0002-8520-6301
Kazuhiko Minematsu https://orcid.org/0000-0002-3427-6772

REFERENCES

1. McGrew, D.A., Viega, J.: The security and performance of the Galois/counter mode (GCM) of operation. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 343–355. Springer (2004)
2. Rogaway, P., et al.: OCB: a block-cipher mode of operation for efficient authenticated encryption. In: Reiter, M.K., Samarati, P. (eds.) ACM CCS 2001, pp. 196–205. ACM Press (2001). https://doi.org/10.1145/501983.502011
3. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer (2004). https://doi.org/10.1007/978-3-540-30539-2_2
4. Krovetz, T., Rogaway, P.: The software performance of authenticated-encryption modes. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 306–327. Springer (2011). https://doi.org/10.1007/978-3-642-21702-9_18
5. Böck, H., et al.: Nonce-disrespecting adversaries: practical forgery attacks on GCM in TLS. In: WOOT. USENIX Association (2016)
6. Shakevsky, A., Ronen, E., Wool, A.: Trust dies in darkness: shedding light on samsung's trustzone keymaster design. IACR Cryptol. ePrint Arch. (To appear at USENIX 2022). 208 (2022)
7. Joux, A.: Authentication Failures in NIST Version of GCM. Comments on the Draft GCM Specification (2006). https://csrc.nist.gov/CSRC/media/Projects/Block-Cipher-Techniques/docum%20ents/BCM/Comments/800-38-series-drafts/GCM/Joux_comments.pdf/
8. Handschuh, H., Preneel, B.: Key-recovery attacks on universal hash function based MAC algorithms. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 144–161. Springer (2008). https://doi.org/10.1007/978-3-540-85174-5_9
9. Peyrin, T., et al.: Cryptanalysis of JAMBU. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 264–281. Springer (2015). https://doi.org/10.1007/978-3-662-48116-5_13
10. Sasaki, Y., Wang, L.: Message extension attack against authenticated encryptions: application to PANDA. In: Gritzalis, D., Kiayias, A., Askoxylakis, I.G. (eds.) CANS 14. LNCS, vol. 8813, pp. 82–97. Springer (2014). https://doi.org/10.1007/978-3-319-12280-9_6
11. Ashur, T., Dunkelman, O., Luykx, A.: Boosting authenticated encryption robustness with minimal modifications. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 3–33. Springer (2017). https://doi.org/10.1007/978-3-319-63697-9_1
12. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 373–390. Springer (2006). https://doi.org/10.1007/11761679_23
13. Guo, C., et al.: Romulus v1.3. Submission to the NIST Lightweight Cryptography Project (2021)
14. Iwata, T., et al.: Duel of the titans: the Romulus and Remus families of lightweight AEAD algorithms. IACR Trans. Symm. Cryptol.(1), 43–120 (2020). https://doi.org/10.13154/tosc.v2020.i1.43-120
15. Andreeva, E., Bhati, A.S., Vizár, D.: Nonce-misuse security of the SAEF authenticated encryption mode. In: SAC. Lecture Notes in Computer Science, vol. 12804, pp. 512–534. Springer (2020)
16. Banik, S., et al.: GIFT-COFB v1.1. Submission to the NIST Lightweight Cryptography Project (2021)
17. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce reuse in WPA2. In: Thuraisingham, B.M., et al. (eds.) ACM CCS 2017, pp. 1313–1328. ACM Press (2017). https://doi.org/10.1145/3133956.3134027
18. Turan, M.S., et al.: Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process (2021). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932630
19. Chakraborti, A., et al.: Blockcipher-based authenticated encryption: how small can we go? In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 277–298. Springer (2017). https://doi.org/10.1007/978-3-319-66787-4_14
20. Banik, S., et al., GIFT-COFB.: IACR Cryptol. ePrint Arch. (2020). https://eprint.iacr.org/2020/738.738
21. Dobraunig, C., et al.: Ascon v1.2. Submission to the NIST Lightweight Cryptography Project (2021)
22. Dobraunig, C., et al.: ISAP v2.0. Submission to the NIST Lightweight Cryptography Project (2021)
23. Guo, C., et al.: Towards lightweight side-channel security and the leakage-resilience of the duplex sponge. IACR Cryptol. ePrint Arch., 193 (2019). https://eprint.iacr.org/2019/193
24. Bellizia, D., et al.: Mode-level vs. implementation-level physical security in symmetric cryptography - a practical guide through the leakage-resistance jungle. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part I. LNCS, vol. 12170, pp. 369–400. Springer (2020). https://doi.org/10.1007/978-3-030-56784-2_13
25. Bellizia, D., et al.: Spook: sponge-based leakage-resistant authenticated encryption with a masked tweakable block cipher. IACR Trans. Symm.

Cryptol. 2020(S1), 295–349 (2020). https://doi.org/10.13154/tosc.v2020.iS1.295-349
26. Beyne, T., et al.: Elephant v2.0. Submission to the NIST Lightweight Cryptography Project (2021)
27. Beyne, T., et al.: Multi-user security of the elephant v2 authenticated encryption mode. In: SAC. Lecture Notes in Computer Science, vol. 13203, pp. 155–178. Springer (2021)
28. Bellare, M., Namprempre, C.: Authenticated encryption: relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer (2000). https://doi.org/10.1007/3-540-44448-3_41
29. Dutta, A., Nandi, M., Talnikar, S.: Beyond birthday bound secure MAC in faulty nonce model. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 437–466. Springer (2019). https://doi.org/10.1007/978-3-030-17653-2_15
30. Beierle, C., et al.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 123–153. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5
31. Banik, S., et al.: GIFT: a small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer (2017). https://doi.org/10.1007/978-3-319-66787-4_16
32. Dodis, Y., et al.: Provable Security of Substitution-Permutation Networks. Cryptology ePrint Archive, Report 2017/016 (2017), https://eprint.iacr.org/2017/016
33. Minematsu, K., Matsushima, T.: Generalization and extension of xex* mode. IEICE Trans. Fund. Electron. Commun. Comput. Sci. 92-A(2), 517–524 (2009). https://doi.org/10.1587/transfun.E92.A.517
34. Patarin, J.: The 'coefficients H' technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer (2009). https://doi.org/10.1007/978-3-642-04159-4_21
35. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer (2014). https://doi.org/10.1007/978-3-642-55220-5_19
36. Inoue, A., Iwata, T., Minematsu, K.: Analyzing the provable security bounds of GIFT-COFB and photon-beetle. IACR Cryptol, 1 (2022). ePrint Arch https://eprint.iacr.org/2022/001

How to cite this article: Inoue, A., Guo, C., Minematsu, K.: Nonce-misuse resilience of Romulus-N and GIFT-COFB. IET Inf. Secur. 1–17 (2023). https://doi.org/10.1049/ise2.12110

APPENDIX

The H-coefficient technique

We use Patarin's H-coefficient technique [34] to prove security for the involved new TBCs. We provide a quick overview of its main ingredients here. Our presentation borrows heavily from that of [35]. Fix a distinguisher D that makes at most q queries to its oracles. As in the security definition presented above, D's aim is to distinguish between two worlds: a 'real world' and an 'ideal world'. Assume wlog that D is deterministic. The execution of D defines a *transcript* that includes the sequence of queries and answers received from its oracles; D's output is a deterministic function of its transcript. Thus, if $T_{\mathsf{re}}, T_{\mathsf{id}}$ denote the probability distributions on transcripts induced by the real and ideal worlds, respectively, then D's distinguishing advantage is upper bounded by the statistical distance

$$\Delta(T_{\mathsf{re}}, T_{\mathsf{id}}) := \frac{1}{2}\sum_{\tau} \left|\Pr[T_{\mathsf{re}} = \tau] - \Pr[T_{\mathsf{id}} = \tau]\right|,$$

where the sum is taken over all possible transcripts τ.

Let Θ denote the set of *attainable transcripts*, that is, transcripts that can be generated by D in the ideal world with non-zero probability. We look for a partition of Θ into two sets Θ_{good} and Θ_{bad} of 'good' and 'bad' transcripts, respectively, along with a constant $\epsilon_1 \in [0, 1)$ such that

$$\tau \in \mathcal{T}_1 \Rightarrow \frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} \geq 1 - \epsilon_1. \tag{9}$$

It is then possible to show (see [35] for details) that

$$\Delta(T_{\mathsf{re}}, T_{\mathsf{id}}) \leq \epsilon_1 + \Pr[T_{\mathsf{id}} \in \Theta_{\mathrm{bad}}]$$

is an upper bound on the distinguisher's advantage. One should think of ϵ_1 and $\Pr[T_{\mathsf{id}} \in \Theta_{\mathrm{bad}}]$ as 'small', so 'good' transcripts have nearly the same probability of appearing in the real world and the ideal world, whereas 'bad' transcripts have a low probability of occurring in the ideal world.