Comprehensive Robustness Analysis of GCM, CCM, and OCB3

Akiko Inoue[1], Tetsu Iwata[2], and Kazuhiko Minematsu[1,3]

[1] NEC, Kawasaki, Japan, `a_inoue@nec.com`,`k-minematsu@nec.com`
[2] Nagoya University, Nagoya, Japan, `tetsu.iwata@nagoya-u.jp`
[3] Yokohama National University, Yokohama, Japan

Abstract. Clarifying the robustness of authenticated encryption (AE) schemes, such as security under nonce misuse or Release of Unverified Plaintext (RUP), is critically important due to the extensive use of AEs in real-world applications. We present a comprehensive analysis of the robustness of well-known standards, namely GCM, CCM, and OCB3. Despite many existing studies, we uncovered several robustness properties for them that were not known in the literature. In particular, we show that both GCM and CCM maintain authenticity under RUP. Moreover, CCM keeps this feature even if a nonce is misused. Together with existing analysis, our work gives a complete picture of the robustness of these standards for the first time. Our results also imply several new robust AE schemes based on GCM and CCM.

Keywords: Authenticated Encryption · Robustness · GCM · CCM · OCB3

1 Introduction

Authenticated encryption (AE) [BN00,Rog02][4] is a type of symmetric-key encryption that simultaneously ensures the confidentiality and authenticity of messages. AE is widely acknowledged as a fundamental tool in practical cryptography and is widely deployed in practice, such as TLS for the Internet and WPA for Wifi access. A wide class of AE is *nonce-based*; that is, it takes a nonce as input, a value that never repeats, in encryption. The most popular and widely accepted prerequisite for nonce-based AE is *nonce-respecting*; the assumption that a nonce is non-repeating is crucial as a repeat of the nonce implies an immediate break of IND-CPA, the standard cryptographic notion for privacy/confidentiality. Another common prerequisite for AE is that the decryption routine must return a single error message when verification fails so that any information on the “unverified plaintext” does not leak.

However, in practice, these two prerequisites are sometimes violated, *i.e.*, AE can be *misused*. Misuse can happen due to various reasons, say poor randomness for nonce generation, misconfiguration of protocol, or side-channel/fault attacks,

[4] AE with associated data (AEAD) is also a common name of our object of study.

and has a devastating impact on real-world applications, such as [BZD+16, VP18, PDM+18]. Studying the impact of violation of these prerequisites, *i.e.*, *robustness*, is thus quite essential and practically relevant. A well-known example is Joux's "forbidden" attacks against GCM [Jou06], which shows that even a single nonce repeat allows a universal forgery attack. Padding oracle attack [Vau02] is another famous example regarding the second prerequisite. After these examples, AE's robustness has been a central topic in the literature. Violation of the first prerequisite is called Nonce Misuse (NM), and that of the second is called Release of Unverified Plaintext (RUP) [ABL+14] (as a special case of [BDPS14]), and studying the robustness of a given scheme means studying security under NM or RUP or both. A number of formal security notions capturing robustness have been proposed and studied [RS06, ABL+14, ADL17]. The robustness of GCM and other popular schemes is a frequent question raised by implementors/users [cse21, cse18, cse19] and received attention in IETF (see *e.g.*, Bozhko [Boz24]). Robustness of modern AE schemes, such as the candidates to CAESAR competition [cae] and NIST Lightweight Cryptography (LWC) [nisb], has been extensively studied [ABL+14, VV18, STA+15, MDV15, IMGM15, nisa]. In particular, NIST IR 8454 [nisa] mentioned that the robustness of the LWC finalists was considered for the final selection, together with a very detailed literature survey on the finalists, including their robustness analysis. The LWC winner Ascon also has been deeply studied on its robustness [asc, BCP22].

Given this situation, it would be interesting to ask: do we fully understand the robustness of well-known standards, namely GCM [nis07a], CCM [nis07b], and OCB3 [KR11]? At first glance, it seems so since there are many existing studies (see Table 1 and Related Work), including the aforementioned forbidden attack by Joux. However, we reveal several robustness properties for them that are unknown (nor mentioned) in the literature. The purpose of this work is to report them in a comprehensive manner[5]. For the first time, we present the full picture of these standards' robustness together with existing analysis.

GCM and CCM are the two NIST AE standards (NIST SP800-38D [nis07a] and SP800-38C [nis07b]). They have been extensively used for TLS, IPSec, SSH, etc. CCM is the first specified AE mode for Wifi since WPA2 and is still mandated in the latest WPA3. It is also used for many resource-constrained networks, including LoRaWan, Bluetooth, and Zigbee, to name a few. See Rogaway's CRYPTREC report [Rog11] for more information on their real-world applications. OCB3 is the third (and the final) version of the seminal OCB mode family and is an Internet standard (RFC 7253) [RFC14].

For GCM, we show that it maintains authenticity even if it releases unverified plaintext, also known as INTegrity under RUP (INT-RUP) [ABL+14], irrespective of nonce length. Except for Ashur *et al.*'s result [ADL17] (ADL17) on nonce misuse resilience privacy (see Table 1), GCM is considered to lack the robustness

[5] We do not consider leakage-resistance [BGP+19, BBC+20, PSV15] as they require additional security assumptions on side-channel attacks for implementations of (specific) components.

of any known kind. Our result shows that this is not the case, and hence, we think this is something unexpected.

For CCM, we show an even stronger result: it maintains INT-RUP even when nonce may repeat in encryption, which we refer to as Nonce-Misuse-Resistant (NMR) INT-RUP. This notion gives the strongest authenticity property that we consider in this paper. In addition, we show that CCM maintains privacy in the sense of Nonce Misuse resiLience (NML), a relaxed notion from nonce misuse resistance introduced by ADL17. These robustness properties are realized by CCM's prefix-free encoding applied to the internal CBC-MAC. It was also the key of the existing nonce-respecting proofs [Jon03, VV18, FMVZ08], however, never used for proving robustness. These results indicate that CCM is much more robust than GCM (and OCB3, see Table 1). Despite its wide real-world adoption, CCM has received surprisingly less attention than GCM or OCB3 from a provable security perspective after Jonsson's initial proof [Jon03]. Our results could benefit protocols/applications adopting CCM to provide an in-depth defense.

For OCB3, the previous analysis covers most of the existing robustness notions. We present a study on nonce misuse resilience. Specifically, we show OCB3's privacy in the sense of nonce misuse resilience. Authenticity is broken in a general case, however, we point out that under a restriction on associated data, authenticity is also maintained. These results compensate for the original analysis of ADL17, which mainly focuses on the first version of OCB.

Table 1 shows the summary of our results together with existing results. For comparison, we also list the results for ChaCha20-Poly1305 [NL15], where all the robustness properties we consider are already known in the literature.

Benefits of Our Results. Our results have several implications on AE constructions. First, given that GCM and CCM are INT-RUP secure, we can convert them into a RUP-secure AE [ABL+14], a secure AE for both privacy and authenticity under RUP, in an efficient (near) black-box way, thanks to a method by Andreeva *et al.* [ABL+14]. An earlier RUP-secure AE based on GCM (GCM-RUP [ADL17]) needs to modify the algorithm. No CCM-based scheme is known. RUP-secure AE is relevant as a countermeasure against real-world attacks such as Efail [PDM+18]. Second, our security proofs reveal that one block cipher call in CCM can be omitted, maintaining all the security properties, including those we prove in this paper. Surprisingly, we found such an optimization after more than 15 years of being standardized by NIST. This improvement is particularly effective when messages are short, as shown by Adomnicăi *et al.* [AMS23]. This optimization could be practically relevant because of the wide adoption of CCM to Internet protocols and wireless low-power communication protocols.

Related Work. Provable security of GCM under the nonce-respecting scenario has been extensively studied [MV04, IOM12, NOMI15, BT16, LMP17, LP18, Nan18, HTT18]. Design issues such as security degradation for short tag or weak keys have been discussed [Fer05, HP08, PC14, ABBT15, MW16]. Dodis *et al.* studied key committing security of GCM [DGRW18].

Table 1: Summary of results. GCM is NML-Priv secure only if nonce is 96 bits and broken otherwise. OCB3 is NML-Auth secure only if AD is fixed. CCM2 is our optimized version of CCM (Sect. 8.2).

	RUP		NMR		NML		RUP+NMR
	Priv (PA1)	INT-RUP	Priv	Auth	Priv	Auth	Auth
GCM	✗ [ABL$^+$14]	✓ Sect. 4	✗ [Classical]	✗ [Jou06]	✓/ ✗ [ADL17]	✗ [ADL17]	✗ [Jou06]
CCM/CCM2	✗ [ABL$^+$14]	✓ Sect. 5	✗ [Classical]	✓ Sect. 5	✓ Sect. 6	✓ Sect. 5	✓ Sect. 5
OCB3	✗ [ABL$^+$14]	✗ [ABL$^+$14]	✗ [Classical]	✗ [VV18]	✓ Sect. 7	✓/ ✗ Sect. 7, [VV18]	✗ [VV18]
ChaChaPoly	✗ [ABL$^+$14]	✓ [IMI16, IMI18]	✗ [Classical]	✗ [KDD17]	✓ [ADL17]	✓ [ADL17]	✗ [KDD17]

Provable security of CCM under the nonce-respecting scenario was proved by Jonsson [Jon03]. Rogaway and Wagner [RW03] reviewed the design and pointed out several deficiencies. Fouque *et al.* [FMVZ08] presented a security bound for a variant of CCM and forgery attacks on (a general form of) CCM based on nonce repeat. Their attack against the original CCM has birthday complexity and hence does not contradict our result. Gjiriti *et al.* [GRV21] showed provable security of a variant of CCM with variable tag stretch. Menda *et al.* [MLGR23] showed key committing attack against CCM.

Provable security of OCB3 under the nonce-respecting scenario has been proved by Krovetz and Rogaway [KR11]. The bound was improved by Bhaumik and Nandi [BN17]. An authenticity attack under RUP was shown by [ABL$^+$14]. Liénardy and Lafitte [LL24] pointed out an issue of the current specification on the valid nonce length.

Vaudenay and Vizár [VV18] showed a nonce-misuse analysis on CAESAR candidates and GCM, CCM and OCB3. Rogaway and Shrimpton [RS06] introduced the notion of nonce-misuse resistance and proposed SIV, an offline AE with nonce-misuse resistance. Robust AE (RAE) [HKR15] is a class of (offline) AEs having full protection against nonce misuse and RUP. Online AE [FFL12] is a class of nonce-based AE that has partial privacy protection against nonce misuse while online processing. Hoang *et al.*. [HRRV15] discussed its practical relevance and limitation.

2 Preliminaries

2.1 Basic notations

For non-negative integers i and j with $i < j$, let $[i..j] \coloneqq \{i, i+1, i+2, \ldots, j\}$. For any list $X = (X[1], \ldots, X[x])$ and $i, j \in [1..x]$, $i < j$, we write $X[i..j]$ to mean $(X[i], \ldots, X[j])$. Let $\{0,1\}^*$ be the set of all bit strings, including the empty string ε, the single element in $\{0,1\}^0$. For $X \in \{0,1\}^*$, $|X|$ denotes its bit length and $|X|_n$ denotes $\lceil |X|/n \rceil$. We define the parsing of a string into n-bit blocks for a positive integer n by $(X[1], X[2], \ldots, X[m]) \xleftarrow{n} X$, where

$X[1] \,\|\, X[2] \,\|\, \ldots \,\|\, X[m] = X$, $|X[i]| = n$ for $1 \le i < m$ and $0 < |X[m]| \le n$ when $|X| > 0$. When $|X| = 0$ (*i.e.*, $X = \varepsilon$), we let $X[1] \xleftarrow{n} X$ with $X[1] = \varepsilon$. A concatenation of bit strings X and Y is denoted as $X \,\|\, Y$, or XY, in case no confusion is possible. Let 0^i be the string of i zero bits. Hence, we write 10^i for $1 \,\|\, 0^i$. For $X \in \{0,1\}^*$ with $|X| \ge i$, $\mathtt{msb}_i(X)$ is the first (left) i bits of X, and $\mathtt{lsb}_i(X)$ is the last (right) i bits of X. Let $\langle X \rangle_c$ be the c-bit standard representation of $X \in [0..2^c - 1]$. If X is uniformly chosen from the set $\mathcal{X}$, we write $X \xleftarrow{\$} \mathcal{X}$. For any $X \in \{0,1\}^*$ and a positive integer n, let $\mathsf{pad}_n(X)$ be $X \,\|\, 00\ldots0$ so that $|\mathsf{pad}_n(X)|$ be the minimum number of multiple of n. If $|X|$ is a positive multiple of n, $\mathsf{pad}_n(X) = X$, and $\mathsf{pad}_n(\varepsilon) = \varepsilon$. Note that pad_n is not injective.

Oracles and Advantage. Suppose $\mathcal{A}$ is an adversary in a game. $\mathcal{A}$ can query to s oracles, $\mathcal{O}_1, \ldots, \mathcal{O}_s$, in any order. In the case of a distinguishing game, $\mathcal{A}$ outputs a bit after the queries, which is a random variable whose probability space is defined under $\mathcal{A}$ and $\{\mathcal{O}_i\}_{i \in [1..s]}$. Let $[\mathcal{A}^{\mathcal{O}_1, \ldots, \mathcal{O}_s} = 1]$ denote the event that this bit is 1. We call $\mathcal{O}_i$ the i-th oracle in the game. By writing $\mathbf{Adv}^{\mathtt{xxx}}_{\Pi}(\mathcal{A})$, we mean *advantage* of the adversary $\mathcal{A}$ in the game $\mathtt{xxx}$ involving Π. We say Π is $\mathtt{xxx}$-secure if the corresponding advantage is negligible for all computationally bounded adversaries.

(Tweakable) Block cipher and random primitives. Any keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ with key space $\mathcal{K}$, we may write $F_K(x)$ to denote $F(K, x)$. Unless otherwise specified, we assume $K \xleftarrow{\$} \mathcal{K}$ in evaluation of $F_K(x)$. A block cipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is a keyed function such that for any $K \in \mathcal{K}$, $E(K, \cdot)$ is a permutation over the message space $\mathcal{M}$. We write $E_K^{-1}(\cdot)$ to denote the decryption function. A tweakable block cipher (TBC) [LRW02] $\widetilde{E} : \mathcal{K} \times \mathcal{TW} \times \mathcal{M} \to \mathcal{M}$ is a keyed function such that for any $K \in \mathcal{K}$ and *tweak* $W \in \mathcal{TW}$, $\widetilde{E}(K, W, \cdot)$ is a permutation over $\mathcal{M}$. Tweak is typically used as a public/chosen value in contrast to the secret key. Let $\mathrm{Perm}(n)$ be the set of all permutations of n bits, and $\mathrm{Func}(n, m)$ be the set of all functions: $\{0,1\}^n \to \{0,1\}^m$. A uniform random permutation (URP) $\mathsf{P} : \{0,1\}^n \to \{0,1\}^n$ is a random permutation uniformly chosen over $\mathrm{Perm}(n)$. A uniform random function (URF) $\mathsf{R} : \{0,1\}^n \to \{0,1\}^m$ is a random function uniformly chosen over $\mathrm{Func}(n, m)$. A tweakable uniform random permutation (TURP) $\widetilde{\mathsf{P}} : \mathcal{TW} \times \mathcal{M} \to \mathcal{M}$ consists of $|\mathcal{TW}|$ independent instances of P over $\mathcal{M}$ and the first argument (tweak) specifies the URP used.The security of TBC $\widetilde{E}$ is defined as the following distinguishing probability.

$$\mathbf{Adv}^{\mathsf{TPRP}}_{\widetilde{E}}(\mathcal{A}) := |\Pr[\mathcal{A}^{\widetilde{E}_K} = 1] - \Pr[\mathcal{A}^{\widetilde{\mathsf{P}}} = 1]|,$$

where $\widetilde{\mathsf{P}}$ has the same domain and range as $\widetilde{E}_K$. When $\mathcal{TW}$ is a singleton, the security of block cipher E_K is obtained by the above security, denoted by $\mathbf{Adv}^{\mathsf{PRP}}_{E}(\mathcal{A})$.

H-Coefficient. All our proofs use the standard H-Coefficient technique [Pat09, CS14]. See App. A for its basics.

2.2 Authenticated Encryption

A nonce-based AE scheme $\Pi = (\Pi.\mathcal{E}, \Pi.\mathcal{D})$ is defined over a key space $\mathcal{K}$, a nonce space $\mathcal{N}$, an associated data (AD) space $\mathcal{AD}$, a message space $\mathcal{M}$, and a tag space $\mathcal{T} = \{0,1\}^\tau$ for some fixed tag length τ. We use ν throughout the paper to denote the nonce length in bits, hence $\mathcal{N} = \{0,1\}^\nu$. An AD is information that is not to be kept confidential, but its integrity must be ensured. For example, network encryption will treat the protocol header as an AD. Formally, AE is a tuple of an encryption function $\Pi.\mathcal{E}\colon \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \to \mathcal{M} \times \mathcal{T}$, and a decryption function $\Pi.\mathcal{D} : \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \times \mathcal{T} \to \mathcal{M} \cup \{\perp\}$, where symbol $\perp$ indicates a verification failure. We require $\Pi.\mathcal{D}_K(N, A, C, T) = M$ if $\Pi.\mathcal{E}_K(N, A, M) = (C, T)$ for soundness. Moreover, we assume $|C| = |M|$; all our target schemes meet this condition. Basically, each nonce in encryption must be unique, which we call *nonce-respecting* (NR) model. Note that a nonce in decryption has no restrictions; it may repeat and it may collide with one used in encryption. A nonce-respecting adversary (NR adversary) may choose nonce arbitrarily in encryption, except that this condition must be respected [Rog04b]. Let $\Pi = (\Pi.\mathcal{E}, \Pi.\mathcal{D})$ be an AE scheme. Let \$ be the random-bit oracle that takes (N, A, M) and returns random $|M| + \tau$ bits. The standard security notions of Π against NR adversaries are Priv (confidentiality/privacy) and Auth (authenticity/integrity), defined below.

Definition 1 (Priv and Auth). *Let $\mathcal{A}$ be a* Priv *adversary against* Π *and let $\mathcal{B}$ be an* Auth *adversary against* Π.

$$\mathbf{Adv}_{\Pi}^{\mathtt{Priv}}(\mathcal{A}) := |\Pr[\mathcal{A}^{\Pi.\mathcal{E}_K} = 1] - \Pr[\mathcal{A}^{\$} = 1]|,$$
$$\mathbf{Adv}_{\Pi}^{\mathtt{Auth}}(\mathcal{B}) := \Pr[\mathcal{B}^{\Pi.\mathcal{E}_K, \Pi.\mathcal{D}_K} \text{ forges}],$$

where $\mathcal{A}$ and $\mathcal{B}$ are nonce-respecting. The event $[\mathcal{B}^{\Pi.\mathcal{E}_K, \Pi.\mathcal{D}_K} \text{ forges}]$ *means that $\mathcal{B}$ receives some $M' \neq \perp$ from $\Pi.\mathcal{D}_K$. $\mathcal{B}$ does not forward queries from $\Pi.\mathcal{E}_K$ to $\Pi.\mathcal{D}_K$, namely, $\mathcal{B}$ does not query (N, A, C, T) to $\Pi.\mathcal{D}_K$ after obtaining (N, A, M, C, T) as a result of query-response to $\Pi.\mathcal{E}_K$.*

It is also possible to consider a combined notion that captures Priv and Auth. While this is convenient, since our purpose is a fine-grained analysis, we always treat privacy and authenticity notions separately. This applies to the various robustness notions described in the next section.

3 Robustness Notions of Authenticated Encryption

3.1 Security notions under nonce misuse

Rogaway and Shrimpton [RS06] (RS06) introduced the concept of *Nonce-Misuse Resistance* (NMR), best-possible security notions under possibly repeating nonces in encryptions. NMR security notions are as follows.

Definition 2 (NMR-Priv and NMR-Auth [RS06]). *Let $\mathcal{A}$ be an NMR-Priv adversary against Π and let $\mathcal{B}$ be an NMR-Auth adversary against Π.*

$$\mathbf{Adv}_{\Pi}^{\texttt{NMR-Priv}}(\mathcal{A}) := |\Pr[\mathcal{A}^{\Pi.\mathcal{E}_K} = 1] - \Pr[\mathcal{A}^{\$} = 1]|,$$
$$\mathbf{Adv}_{\Pi}^{\texttt{NMR-Auth}}(\mathcal{B}) := \Pr[\mathcal{B}^{\Pi.\mathcal{E}_K, \Pi.\mathcal{D}_K} \text{ forges}],$$

where $\mathcal{A}$ and $\mathcal{B}$ may query to the first oracle with repeating nonces, but does not query a repeated tuple of (N, A, M). $\mathcal{B}$ does not forward queries from the first oracle to the second oracle.

We remark that NMR-Priv requires $\Pi.\mathcal{E}$ to be offline, *i.e.*, any ciphertext bit must reflect the whole encryption input. This limits applicability in particular for long messages. GCM and OCB3 are online schemes; it is inherently impossible to meet this notion. CCM is not online, but the encryption part is nevertheless a counter mode and fails to meet NMR-Priv [VV18].

Nonce-misuse resilience. Ashur, Dunkelman, and Luykx [ADL17] proposed the concept of *Nonce-Misuse resiLience* (NML), which is a relaxed form of NMR. Intuitively, NML security notions require that the attacker must win the game by making a query with a nonce that is not misused (repeated). Conversely, an AE scheme is NML-secure if a repeat of nonce N does not threaten the security of encryption/decryption with a different nonce from N. While weaker than NMR, NML notions can be fulfilled by online schemes. If nonce is determined by (*e.g.*) recipient ID or timestamp, NML is practically relevant.

Definition 3 (NML-Priv and NML-Auth [ADL17]). *Let $\mathcal{A}$ be an NML-Priv adversary against Π and let $\mathcal{B}$ be an NML-Auth adversary against Π.*

$$\mathbf{Adv}_{\Pi}^{\texttt{NML-Priv}}(\mathcal{A}) := |\Pr[\mathcal{A}^{\Pi.\mathcal{E}_K, \Pi.\mathcal{E}_K} = 1] - \Pr[\mathcal{A}^{\$, \Pi.\mathcal{E}_K} = 1]|,$$
$$\mathbf{Adv}_{\Pi}^{\texttt{NML-Auth}}(\mathcal{B}) := \Pr[\mathcal{B}^{\Pi.\mathcal{E}_K, \Pi.\mathcal{D}_K} \text{ forges}],$$

where $\mathcal{A}$ is nonce-respecting with respect to the first oracle, i.e., let $\mathcal{N}_1$ and $\mathcal{N}_2$ be the multisets of nonces used by the queries to the first (nonce-respecting) and the second (nonce-misusing) oracles; $\mathcal{N}_1 \cap \mathcal{N}_2 = \emptyset$ and each $N \in \mathcal{N}_1$ has a multiplicity one. $\mathcal{N}_2$ may contain nonces with multiplicity ≥ 2. Similarly for $\mathcal{B}$, we define $\mathcal{N}_1$ and $\mathcal{N}_2$. Both may contain nonces with multiplicity ≥ 2. However, any $N \in \mathcal{N}_1 \cap \mathcal{N}_2$ must have multiplicity one in $\mathcal{N}_1$. In addition, as with the standard Auth *notion, a trivial forgery is prohibited.*

3.2 Security notions under release of unverified plaintext

Release of Unverified Plaintext (RUP) was formalized by Andreeva *et al.* [ABL$^+$14]. RUP is the game environment that leaks the unverified plaintext to the adversary at decryption independent of the verification result. To formalize RUP security games, we require that $\Pi.\mathcal{D}$ is decomposed into the unverified decryption function, $\Pi.u\mathcal{D} : \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \times \mathcal{T} \to \mathcal{M}$ and the verification function, $\Pi.\mathcal{V} : \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \times \mathcal{T} \to \{\top, \bot\}$. The normal decryption combines them as $\Pi.\mathcal{D}_K(N, A, C, T) = M$ if $\Pi.u\mathcal{D}_K(N, A, C, T) = M$ and $\Pi.\mathcal{V}_K(N, A, C, T) = \top$, and $\Pi.\mathcal{D}_K(N, A, C, T) = \bot$ if $\Pi.\mathcal{D}_K(N, A, C, T) = \bot$. That is, when $\Pi.u\mathcal{D}_K(N, A, C, T) = M$, M denotes the correct decrypted plaintext if the input tuple is authentic, and otherwise M is something that would be discarded by the decryption oracle in the classical authenticity notions. Most existing AE schemes, including our targets, fulfill the aforementioned assumption. We will write $\Pi = (\Pi.\mathcal{E}, \Pi.u\mathcal{D}, \Pi.\mathcal{V})$ when we discuss about RUP security of Π. As described, $\Pi.\mathcal{D}$ is uniquely determined from $\Pi.u\mathcal{D}$ and $\Pi.\mathcal{V}$.

Privacy notion under RUP is Plaintext Awareness (PA), and PA is classified into a basic notion (PA1) and a stronger notion (PA2). As they are irrelevant to our analysis, we omit the definitions here. The authenticity notion under RUP is called INT-RUP (for INTegrity under RUP) [ABL+14].

Definition 4 (INT-RUP). *Let $\mathcal{A}$ be the INT-RUP adversary against $\Pi = (\Pi.\mathcal{E}, \Pi.u\mathcal{D}, \Pi.\mathcal{V})$.*

$$\mathbf{Adv}_{\Pi}^{\texttt{INT-RUP}}(\mathcal{A}) := \Pr[\mathcal{A}^{\Pi.\mathcal{E}_K, \Pi.u\mathcal{D}_K, \Pi.\mathcal{V}_K} \text{ forges}],$$

where $\mathcal{A}$ is nonce-respecting, i.e., never repeats nonce in queries to $\Pi.\mathcal{E}$. Moreover, $\mathcal{A}$ does not forward queries from $\Pi.\mathcal{E}$ to $\Pi.\mathcal{V}$. Queries to $\Pi.u\mathcal{D}$ have no restrictions.

We can combine INT-RUP with the nonce-misuse scenario, yielding a more robust authenticity notion.

Definition 5 (NMR-INT-RUP). *The nonce-misuse resistance INT-RUP (NMR-INT-RUP) advantage, $\mathbf{Adv}_{\Pi}^{\texttt{NMR-INT-RUP}}(\mathcal{A})$, is defined in the same manner as INT-RUP, except that $\mathcal{A}$ is allowed to repeat nonces in queries to the first oracle.*

By definition, we have the following implications: (1) NMR-Priv → NML-Priv → Priv, and (2) NMR-Auth → NML-Auth → Auth, and (3) NMR-INT-RUP → INT-RUP, and (4) NMR-INT-RUP → NMR-Auth.

4 Authenticity of GCM under RUP

We show that GCM is INT-RUP secure. As described in the introduction, we think this result is kind of unexpected since GCM is considered to lack robustness other than NML-Priv with a restriction to 96-bit nonce [ADL17].

4.1 Specification of GCM

We briefly present the specification of GCM. Let $n = 128$ and E be an n-bit block cipher. For $X \in \{0,1\}^{\ell}$ such that $\langle X \rangle_{\ell} = x_{\ell-1} \cdots x_1 x_0$, let $\mathsf{int}(X)$ be an integer $\sum_{i=0}^{\ell-1} x_i 2^i$. Let $\mathsf{inc}(X) = \mathtt{msb}_{n-32}(X) \,\|\, \langle \mathsf{int}(\mathtt{lsb}_{32}(X)) + 1 \mod 2^{32} \rangle_{32}$. For $i \geq 0$, $\mathsf{inc}^i(X)$ means that applying inc on X for i times. When $i = 0$, $\mathsf{inc}^i(X) = X$.

```
Algorithm $\mathsf{GCM}.\mathcal{E}[E_K](N, A, M)$

1. $C \leftarrow \mathsf{GCTR}[E_K](N, C)$
2. $T \leftarrow \mathsf{GMAC}.\mathcal{T}[E_K](N, A, C)$
3. return $(C, T)$

Algorithm $\mathsf{GCM}.u\mathcal{D}[E_K](N, A, C, T)$

1. $M \leftarrow \mathsf{GCTR}[E_K](N, C)$
2. return $M$

Algorithm $\mathsf{GCM}.\mathcal{D}[E_K](N, A, C, T)$

1. $b = \mathsf{GCM}.\mathcal{V}[E_K](N, A, C, T)$
2. if $b = \bot$ then return $\bot$
3. else $M \leftarrow \mathsf{GCM}.u\mathcal{D}[E_K](N, A, C, T)$
4. return $M$

Algorithm $\mathsf{GCM}.\mathcal{V}[E_K](N, A, C, T)$

1. $\widehat{T} \leftarrow \mathsf{GMAC}.\mathcal{T}[E_K](N, A, C)$
2. if $T = \widehat{T}$ then return $\top$
3. else return $\bot$
```

```
Algorithm $\mathsf{GCTR}[E_K](N, M)$

1. $L \leftarrow E_K(0^n)$
2. if $\nu = 96$ then $\mathsf{Ctr0} \leftarrow N \,\|\, 0^{31}1$
3. else then $\mathsf{Ctr0} \leftarrow \mathsf{GHASH}_L(\varepsilon, N)$
4. $(M[1], \ldots, M[m]) \xleftarrow{n} M$
5. for $i = 1$ to $m$ do
6.     $C[i] \leftarrow M[i] \oplus \mathtt{msb}_{|M[i]|}(E_K(\mathsf{inc}^i(\mathsf{Ctr0})))$
7. $C \leftarrow C[1] \,\|\, \cdots \,\|\, C[m-1] \,\|\, C[m]$
8. return $C$

Algorithm $\mathsf{GMAC}.\mathcal{T}[E_K](N, A, C)$

1. $L \leftarrow E_K(0^n)$
2. if $\nu = 96$ then $\mathsf{Ctr0} \leftarrow N \,\|\, 0^{31}1$
3. else then $\mathsf{Ctr0} \leftarrow \mathsf{GHASH}_L(\varepsilon, N)$
4. $\mathsf{Mask} \leftarrow \mathtt{msb}_\tau(E_K(\mathsf{Ctr0}))$
5. $T \leftarrow \mathsf{Mask} \oplus \mathtt{msb}_\tau(\mathsf{GHASH}_L(A, C))$
6. return $T$

Algorithm $\mathsf{GMAC}.\mathcal{V}[E_K](N, A, C, T)$

1. $\widehat{T} \leftarrow \mathsf{GMAC}.\mathcal{T}[E_K](N, A, C)$
2. if $T = \widehat{T}$ return $\top$
3. else return $\bot$

Algorithm $\mathsf{GHASH}_L(A, C)$

1. $X \leftarrow \mathsf{pad}_n(A) \,\|\, \mathsf{pad}_n(C) \,\|\, \langle |A| \rangle_{n/2} \,\|\, \langle |C| \rangle_{n/2}$
2. $(X[1], \ldots, X[x]) \xleftarrow{n} X$, $Y \leftarrow 0^n$
3. for $i = 1$ to $x$ do $Y \leftarrow L \cdot (Y \oplus X[i])$
4. return $Y$
```

Fig. 1: Algorithms of $\mathsf{GCM}[E_K]$. Note that $\nu := |N|$ and $\tau := |T|$ are fixed in advance. The operation "$\cdot$" in line 3 of GHASH denotes a multiplication over $\mathrm{GF}(2^n)$.

GCM is basically a composition of counter mode and a nonce-based MAC using a polynomial hashing over $\mathrm{GF}(2^n)$. Figure 1 shows the algorithms of GCM using E_K, denoted as $\mathsf{GCM}[E_K]$. In addition to the normal decryption, Fig. 1 shows the unverified decryption and verification routines together with GMAC MAC function inside GCM. They will be needed for our analysis. Here, $N, A, C \in \{0,1\}^*$ and $\tau := |T| \in [1..n]$ (NIST recommends $\tau \geq 64$). We also require $\nu := |N| \in [1..2^{n/2} - 1]$, $|A| \in [0..2^{n/2} - 1]$, and $|M| \in [0..n(2^{32} - 2)]$. The parameters ν and τ must be fixed in advance. The derivation of the first counter block input depends on whether $\nu = 96$ or not. Note that $|C| = |M|$ holds. Figure 2 depicts the encryption.

4.2 INT-RUP bounds of GCM

Let $\mathsf{GCM}[E] = (\mathsf{GCM}.\mathcal{E}[E], \mathsf{GCM}.u\mathcal{D}[E], \mathsf{GCM}.\mathcal{V}[E])$ employing a block cipher $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Let $\mathcal{A}$ be an INT-RUP adversary who makes q_e queries

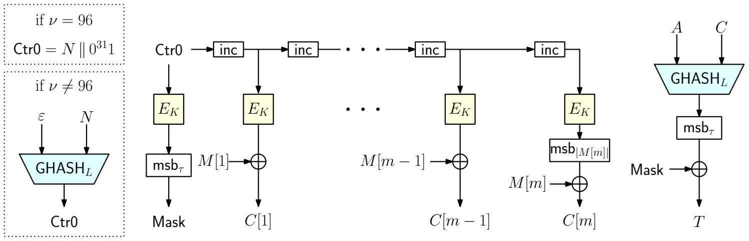

Fig. 2: Encryption of GCM.

to $\mathsf{GCM}.\mathcal{E}[E_K]$, q_d queries to $\mathsf{GCM}.u\mathcal{D}[E_K]$, and q_v queries to $\mathsf{GCM}.\mathcal{V}[E_K]$, with time complexity t (where $K \xleftarrow{\$} \mathcal{K}$). After all the queries, $\mathcal{A}$ obtains a transcript written as

- $\{(N_i^e, A_i^e, M_i^e, C_i^e, T_i^e)\}_{i=1,\ldots,q_e}$ from $\mathsf{GCM}.\mathcal{E}[E_K]$,
- $\{(N_i^d, A_i^d, M_i^d, C_i^d, T_i^d)\}_{i=1,\ldots,q_d}$ from $\mathsf{GCM}.u\mathcal{D}[E_K]$,
- $\{(N_i^v, A_i^v, C_i^v, T_i^v, b_i)\}_{i=1,\ldots,q_v}$ from $\mathsf{GCM}.\mathcal{V}[E_K]$, where $b_i \in \{\top, \bot\}$.

Let σ_e, σ_d, and σ_v be the total number of plaintext/ciphertext blocks queried to $\mathsf{GCM}.\mathcal{E}[E]$, $\mathsf{GCM}.u\mathcal{D}[E]$, and $\mathsf{GCM}.\mathcal{V}[E]$ oracles, *i.e.*, $\sigma_e = \sum_{i=1}^{q_e} |M_i^e|_n$, $\sigma_d = \sum_{i=1}^{q_d} |C_i^d|_n$, and $\sigma_v = \sum_{i=1}^{q_v} |C_i^v|_n$. Let $\sigma_{\text{all}} \coloneqq \sigma_e + \sigma_d + \sigma_v + q_e + q_v + 1$ to denote the maximum of the total number of E calls in the game, which we call the effective total queried blocks. Let $\ell_N \coloneqq \lceil \nu/n \rceil$ and ℓ_A be the maximum number of blocks of the input to GHASH in encryption and verification queries; thus, $|A_i^{\#}|_n + |C_i^{\#}|_n \le \ell_A$ for $\# \in \{e, v\}$, $i \in [1..q_{\#}]$.

The following theorem shows that GCM is INT-RUP secure up to the birthday bound irrespective of nonce length.

Theorem 1. *For the adversary $\mathcal{A}$ defined as above with time complexity t,*

$$\begin{aligned}
\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[E]}(\mathcal{A}) &\le \mathbf{Adv}^{\texttt{PRP}}_{E}(\widehat{\mathcal{A}}) + \frac{\sigma_{\text{all}}^2}{2^{n+1}} \\
&+ \frac{(q_e^2 + 2q_e q_v + 2q_e + 2q_v + 2\sigma_e + 2\sigma_d)(\ell_N + 1)}{2^n} \\
&+ \frac{64(2q_e + q_d + q_v - 1)(\sigma_e + \sigma_d + q_e + q_d)(\ell_N + 1)}{2^n} + \frac{2q_v(\ell_A + 2)}{2^\tau}
\end{aligned}$$

holds for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\text{all}})$. In particular, when $\nu = 96$, we have

$$\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[E]}(\mathcal{A}) \le \mathbf{Adv}^{\texttt{PRP}}_{E}(\widehat{\mathcal{A}}) + \frac{\sigma_{\text{all}}^2}{2^{n+1}} + \frac{2q_v(\ell_A + 2)}{2^\tau}$$

for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\text{all}})$.

4.3 Proof of Theorem 1

Overview. We take three steps to prove INT-RUP bound for $\mathsf{GCM}[E]$. First, we apply PRP/PRF switching lemma [BR06] and replace P with a URF $\mathsf{R} : \{0,1\}^n \rightarrow \{0,1\}^n$. Second, we define a variant of UF-CMA (unforgeability under chosen message attack) security of $\mathsf{GMAC}[\mathsf{R}]$, dubbed UF-CMA$^+$, and show that INT-RUP security of $\mathsf{GCM}[\mathsf{R}]$ reduces to UF-CMA$^+$ security of $\mathsf{GMAC}[\mathsf{R}]$. Third, we prove UF-CMA$^+$ security of $\mathsf{GMAC}[\mathsf{R}]$ using the H-coefficient technique.

Step 1. An application of the standard PRP/PRF switching lemma shows

$$\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\texttt{PRP}}_{E}(\widehat{\mathcal{A}}) + \frac{\sigma_{\mathrm{all}}^2}{2^{n+1}} + \mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[\mathsf{R}]}(\mathcal{A}') \qquad (1)$$

for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\mathrm{all}})$ and an INT-RUP adversary $\mathcal{A}'$ having the same computational cost as $\mathcal{A}$.

Step 2. We analyse $\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[\mathsf{R}]}(\mathcal{A}')$. Let $\mathsf{GMAC}[\mathsf{R}] = (\mathsf{GMAC}.\mathcal{T}[\mathsf{R}], \mathsf{GMAC}.\mathcal{V}[\mathsf{R}])$, where the algorithms of $\mathsf{GMAC}.\mathcal{T}$ and $\mathsf{GMAC}.\mathcal{V}$ are shown in Fig. 2. For simplicity, we write $\mathsf{GMAC}.\mathcal{T}$ and $\mathsf{GMAC}.\mathcal{V}$ to mean $\mathsf{GMAC}.\mathcal{T}[\mathsf{R}]$ and $\mathsf{GMAC}.\mathcal{V}[\mathsf{R}]$. Throughout this step, the same applies to other oracles, *e.g.*, $\mathsf{GCM}.u\mathcal{D}$ means $\mathsf{GCM}.u\mathcal{D}[\mathsf{R}]$. We also define a function to simulate $\mathsf{GCM}.u\mathcal{D}$ and the encryption part of $\mathsf{GCM}.\mathcal{E}$ in the INT-RUP game. Let $\mathcal{KS}_{\mathsf{G}} : \{0,1\}^\nu \times [1..2^{32}-2] \rightarrow \{0,1\}^n$ be a function that outputs a block of key stream $KS \in \{0,1\}^n$ for the tuple of $N \in \{0,1\}^\nu$ and block index $\mathsf{idx} \in [1..2^{32}-2]$ using R. Concretely, we define $\mathcal{KS}_{\mathsf{G}}(N, \mathsf{idx}) \coloneqq \mathsf{R}(\mathsf{inc}^{\mathsf{idx}}(\mathsf{Ctr0}))$, where

$$\mathsf{Ctr0} \coloneqq \begin{cases} N \,\|\, 0^{31}1 & \text{when} \quad \nu = 96 \\ \mathsf{GHASH}_L(\varepsilon, N) & \text{when} \quad \nu \neq 96, \end{cases}$$

and $L = \mathsf{R}(0^n)$. We define UF-CMA$^+$ game involving $\mathsf{GMAC}.\mathcal{T}$, $\mathcal{KS}_{\mathsf{G}}$, and $\mathsf{GMAC}.\mathcal{V}$. Its definition is UF-CMA game for $\mathsf{GMAC}[\mathsf{R}]$ with an additional oracle $\mathcal{KS}_{\mathsf{G}}$.

Definition 6 (UF-CMA$^+$ game). *Let $\mathcal{B}$ be an adversary querying to the three oracles, $\mathsf{GMAC}.\mathcal{T}$, $\mathcal{KS}_{\mathsf{G}}$, and $\mathsf{GMAC}.\mathcal{V}$. The adversary $\mathcal{B}$ does not forward queries from $\mathsf{GMAC}.\mathcal{T}$ to $\mathsf{GMAC}.\mathcal{V}$; $\mathcal{B}$ does not query (N, A, C, T) to $\mathsf{GMAC}.\mathcal{V}$ when $\mathcal{B}$ has already queried (N, A, C) to $\mathsf{GMAC}.\mathcal{T}$ and received T before. The UF-CMA$^+$ advantage of $\mathcal{B}$ is defined as*

$$\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B}) \coloneqq \Pr[\mathcal{B}^{\mathsf{GMAC}.\mathcal{T}, \mathcal{KS}_{\mathsf{G}}, \mathsf{GMAC}.\mathcal{V}} \text{ forges}],$$

*where the probability is defined over R and the random coins of $\mathcal{A}$. Here, "*forges*" means the event that $\mathsf{GMAC}.\mathcal{V}$ returns $\top$.*

In this section, we assume the adversary of UF-CMA$^+$ game $\mathcal{B}$ follows a nonce-respecting setting; thus, $\mathcal{B}$ does not repeat the same nonce in the queries to $\mathsf{GMAC}.\mathcal{T}$. We obtain the following lemma.

Lemma 1. *Let $\mathcal{A}'$ be an INT-RUP adversary against* $\mathsf{GCM}[\mathsf{R}]$ *using q_e encryption queries, q_d decryption queries, and q_v verification queries. Let σ_e and σ_d be as defined earlier. We have*

$$\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[\mathsf{R}]}(\mathcal{A}') \le \mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B})$$

for a UF-CMA$^+$ adversary $\mathcal{B}$ against $\mathsf{GMAC}[\mathsf{R}]$ *that makes q_e queries to* $\mathsf{GMAC}.\mathcal{T}$*, $(\sigma_e + \sigma_d)$ queries to $\mathcal{KS}_\mathsf{G}$, and q_v queries to* $\mathsf{GMAC}.\mathcal{V}$*.*

The proof of Lemma 1 is in App. B.

Step 3. We evaluate $\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B})$. We define the following indistinguishability notion to apply the H-coefficient technique.

$$\mathbf{Adv}^{\texttt{Ind+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B}) := |\Pr[\mathcal{B}^{\mathsf{GMAC}.\mathcal{T},\mathcal{KS}_\mathsf{G},\mathsf{GMAC}.\mathcal{V}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{R}_{ks},\perp} = 1]|,$$

where \$ (resp. R_{ks}) is a random oracle (resp. URF) whose input/output interface and lengths are the same as $\mathsf{GMAC}.\mathcal{T}$ (resp. $\mathcal{KS}_\mathsf{G}$). Note that R_{ks} is independent of R used by $\mathsf{GMAC}.\mathcal{T}$, $\mathcal{KS}_\mathsf{G}$, and $\mathsf{GMAC}.\mathcal{V}$. The $\perp$ oracle has the same input interface as $\mathsf{GMAC}.\mathcal{V}$ and returns $\perp$ for any input. We obtain the following inequality.

$$\begin{aligned}\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B}) &= |\Pr[\mathcal{B}^{\mathsf{GMAC}.\mathcal{T},\mathcal{KS}_\mathsf{G},\mathsf{GMAC}.\mathcal{V}} = 1] - \Pr[\mathcal{B}^{\mathsf{GMAC}.\mathcal{T},\mathcal{KS}_\mathsf{G},\perp} = 1] \\ &\quad + \Pr[\mathcal{B}^{\$,\mathsf{R}_{ks},\perp} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{R}_{ks},\perp} = 1]| \\ &\le 2\mathbf{Adv}^{\texttt{Ind+}}_{\mathsf{GMAC}[\mathsf{R}]}(\mathcal{B}). \end{aligned} \tag{2}$$

To bound the right-hand side of Eq. (2), we relax the game so that $\mathcal{B}$ obtains the GHASH key after all queries but before it determines an output bit. In the real world, $\mathcal{B}$ obtains a real key $L = \mathsf{R}(0^n)$, and in the ideal world, it obtains a dummy key $L \xleftarrow{\$} \{0,1\}^n$. Then, $\mathcal{B}$ can compute GHASH_L outputs for all queries. We define a transcript $\theta = (\theta_t, \theta_{ks}, \theta_v, L)$ of $\mathcal{B}$ such that

- $\theta_t = \{(N_i^t, A_i^t, C_i^t, T_i^t, \mathsf{Ctr0}_i^t, \mathsf{Mask}_i)\}_{i\in[1..q_t]}$,
- $\theta_{ks} = \{(N_i^{ks}, \mathsf{idx}_i, KS_i, \mathsf{Ctr0}_i^{ks})\}_{i\in[1..q_{ks}]}$,
- $\theta_v = \{(N_i^v, A_i^v, C_i^v, T_i^v, \mathsf{Ctr0}_i^v)\}_{i\in[1..q_v]}$,

where $\mathsf{Mask}_i = T_i^t \oplus \mathtt{msb}_\tau(\mathsf{GHASH}_L(A_i^t, C_i^t))$. Note that θ_v does not contain $b_i \in \{\top, \perp\}$ as any attainable transcript has $b_i = \perp$ for all $i \in [1..q_v]$ by definition. Let $\ell_N = \lceil \nu/n \rceil$ and ℓ_A be the maximum number of blocks of the input to GHASH in the game; thus, $|A_i^\#|_n + |C_i^\#|_n \le \ell_A$ for $\# \in \{t, v\}$, $i \in [1..q_\#]$. For a transcript θ, we define the following bad events.

Bad1 Collision of $\mathsf{Ctr0}^t$ in θ_t: there exists distinct $i, j \in [1..q_t]$ *s.t.* $\mathsf{Ctr0}_i^t = \mathsf{Ctr0}_j^t$.

Bad2 Collision of $\mathsf{Ctr0}^t$ in θ_t and $\mathsf{inc}^{\mathsf{idx}}(\mathsf{Ctr0}^{ks})$ in θ_{ks}: there exists $i \in [1..q_t]$, $j \in [1..q_{ks}]$ *s.t.* $\mathsf{Ctr0}_i^t = \mathsf{inc}^{\mathsf{idx}_j}(\mathsf{Ctr0}_j^{ks})$.

Bad3 Non-trivial collision of $\mathsf{Ctr0}^t$ in θ_t and $\mathsf{Ctr0}^v$ in θ_v: there exists $i \in [1..q_t]$, $j \in [1..q_v]$ *s.t.* $N_i^t \neq N_j^v$ and $\mathsf{Ctr0}_i^t = \mathsf{Ctr0}_j^v$.

Bad4 Non-trivial collision of $\mathsf{inc}^{\mathsf{idx}}(\mathsf{Ctr0}^{ks})$ in θ_{ks}: there exists $i, j \in [1..q_{ks}]$ *s.t.* $(N_i^{ks}, \mathsf{idx}_i) \neq (N_j^{ks}, \mathsf{idx}_j)$ and $\mathsf{inc}^{\mathsf{idx}_i}(\mathsf{Ctr0}_i^{ks}) = \mathsf{inc}^{\mathsf{idx}_j}(\mathsf{Ctr0}_j^{ks})$.

Bad5 Collision of $\mathsf{inc}^{\mathsf{idx}}(\mathsf{Ctr0}^{ks})$ in θ_{ks} and $\mathsf{Ctr0}^v$ in θ_v: there exists $i \in [1..q_v]$, $j \in [1..q_{ks}]$ *s.t.* $\mathsf{Ctr0}_i^v = \mathsf{inc}^{\mathsf{idx}_j}(\mathsf{Ctr0}_j^{ks})$.

Bad6 Collision of 0^n and any of $\mathsf{Ctr0}^t$, $\mathsf{inc}^{\mathsf{idx}}(\mathsf{Ctr0}^{ks})$, or $\mathsf{Ctr0}^v$ in θ: there exists $i \in [1..q_t]$, $j \in [1..q_{ks}]$, $k \in [1..q_v]$ *s.t.* $0^n = \mathsf{Ctr0}_i^t$ or $0^n = \mathsf{inc}^{\mathsf{idx}_j}(\mathsf{Ctr0}_j^{ks})$ or $0^n = \mathsf{Ctr0}_k^v$.

Bad7 Successful forgery: for $i \in [1..q_v]$, there exists $j \in [1..q_t]$ *s.t.* $N_i^v = N_j^t$ and $T_i^v = \mathsf{Mask}_j \oplus \mathtt{msb}_\tau(\mathsf{GHASH}_L(A_i^v, C_i^v))$.

We say (an attainable) θ is bad if any of the above bad events occur and define Θ_{bad} as the set of all bad transcripts. We define the good transcript set Θ_{good} following App. A. Let $\mathbf{Bad} \coloneqq \mathbf{Bad1} \cup \cdots \cup \mathbf{Bad7}$. We evaluate the upper bound of $\Pr[\mathsf{T}_{\mathsf{id}} \in \Theta_{\text{bad}}] =: \Pr[\mathbf{Bad}]$, where T_{id} is a random variable of the transcript in the ideal world.

Let us first focus on the general case of ν. We define q'_{ks} as the number of distinct queries of θ_{ks}. From the union bound for collisions among random elements and the fact that a polynomial of degree s has at most s solutions, we observe that **Bad1**, **Bad3**, **Bad6**, and **Bad7** are bounded as $\Pr[\mathbf{Bad1}] \leq \binom{q_t}{2}(\ell_N + 1)/2^n$, $\Pr[\mathbf{Bad3}] \leq q_t q_v(\ell_N + 1)/2^n$, $\Pr[\mathbf{Bad6}] \leq (q_t + q'_{ks} + q_v)(\ell_N + 1)/2^n$, and $\Pr[\mathbf{Bad7}] \leq q_v(\ell_A + 1)/2^\tau$. Note that the equations derived from these bad events are non-trivial equations of (random) L of degree at most $\ell_N + 1$ or $\ell_A + 1$ over $\mathrm{GF}(2^n)$. For the evaluation of **Bad2**, let $\mathsf{Coll}_L([a..b], N_1, N_2)$ be the event $\mathsf{GHASH}_L(\varepsilon, N_1) = \mathsf{inc}^r(\mathsf{GHASH}_L(\varepsilon, N_2))$ for some $r \in [a..b]$, where $0 \leq a \leq b \leq 2^{32} - 1$ and N_1 and N_2 are distinct nonces which are not 96 bits. The following lemma gives the upper bound of the event.

Lemma 2 (Lemmas 2 and 3 in [NOMI15]). *For $0 \leq m \leq 2^{32} - 1$ and two distinct nonces N_1 and N_2 which are not 96 bits, $\Pr[\mathsf{Coll}_L([0..m], N_1, N_2)] \leq 32(m + 1)(\ell_N + 1)/2^n$, where $|N_1|_n, |N_2|_n \leq \ell_N$ holds.*

To use Lemma 2, we define d as the number of distinct nonces in queries of θ_{ks}. For $i \in [1..d]$, let $\mathsf{idx}_i^{\mathsf{M}}$ be the maximum value of idx among queries for the i-th nonce N_i^{ks*}, using the arbitrary ordering of the nonces. Let $\rho = \sum_{i=1}^d \mathsf{idx}_i^{\mathsf{M}}$, and note that $q'_{ks} \leq \rho$. We then obtain the following evaluation.

$$\begin{aligned}\Pr[\mathbf{Bad2}] &\leq \sum_{i=1}^{q_t} \sum_{j=1}^{d} \Pr[\mathsf{Coll}_L([0..\mathsf{idx}_j^{\mathsf{M}}], N_i^t, N_j^{ks*})] \\ &\leq \sum_{i=1}^{q_t} \sum_{j=1}^{d} \frac{32(\mathsf{idx}_j^{\mathsf{M}} + 1)(\ell_N + 1)}{2^n} \leq \frac{32 q_t(\rho + d)(\ell_N + 1)}{2^n}.\end{aligned}$$

Note that $\Pr[\mathsf{Ctr0}_i^t = \mathsf{inc}^k(\mathsf{Ctr0}_j^{ks})] = 0$ when $N_i^t = N_j^{ks}$ since $k \geq 1$. We can evaluate $\Pr[\textbf{Bad4}]$ and $\Pr[\textbf{Bad5}]$ in the same manner as $\Pr[\textbf{Bad2}]$.

$$\Pr[\textbf{Bad5}] \leq \frac{32q_v(\rho + d)(\ell_N + 1)}{2^n},$$

$$\Pr[\textbf{Bad4}] \leq \sum_{i=1}^{d} \sum_{\substack{j \neq i \\ j=1}}^{d} \frac{32(\mathsf{idx}_j^{\mathsf{M}} + 1)(\ell_N + 1)}{2^n} \leq \sum_{i=1}^{d} \frac{32(\rho - \mathsf{idx}_i^{\mathsf{M}} + d - 1)(\ell_N + 1)}{2^n}$$

$$\leq \frac{32(d\rho - \rho + d^2 - d)(\ell_N + 1)}{2^n} \leq \frac{32(d-1)(\rho + d)(\ell_N + 1)}{2^n}.$$

Summing up all the bad event probabilities, we obtain the following upper bound.

$$\Pr[\textbf{Bad}] \leq \frac{(0.5q_t^2 + q_t q_v + q_t + q'_{ks} + q_v)(\ell_N + 1)}{2^n} + \frac{32(q_t + q_v + d - 1)(\rho + d)(\ell_N + 1)}{2^n} + \frac{q_v(\ell_A + 1)}{2^\tau}. \tag{3}$$

Eq. (3) holds for any ν. On the other hand, when we fix $\nu = 96$, we obtain $\Pr[\textbf{Bad1}] = \Pr[\textbf{Bad2}] = \cdots = \Pr[\textbf{Bad6}] = 0$, and

$$\Pr[\textbf{Bad}] = \Pr[\textbf{Bad7}] \leq \frac{q_v(\ell_A + 1)}{2^\tau}. \tag{4}$$

Next, we evaluate the lower bound of $\Pr[\mathsf{T}_{\mathsf{re}} = \theta] / \Pr[\mathsf{T}_{\mathsf{id}} = \theta]$ for $\theta \in \Theta_{\text{good}}$, where T_{re} is a random variable of the transcript in the real world. Let $\# \in \{\mathsf{re}, \mathsf{id}\}$. Let $\mathsf{T}_\#^t$, $\mathsf{T}_\#^{ks}$, $\mathsf{T}_\#^v$, $\mathsf{T}_\#^L$ denote the random variables of θ_t, θ_{ks}, θ_v, L in each world, respectively. For a good transcript $\theta \in \Theta_{\text{good}}$, we have

$$\begin{aligned}\Pr[\mathsf{T}_\# = \theta] = \Pr[\mathsf{T}_\#^L = L] &\cdot \Pr[\mathsf{T}_\#^{ks} = \theta_{ks} \mid \mathsf{T}_\#^L = L] \\ &\cdot \Pr[\mathsf{T}_\#^t = \theta_t \mid (\mathsf{T}_\#^L, \mathsf{T}_\#^{ks}) = (L, \theta_{ks})] \\ &\cdot \Pr[\mathsf{T}_\#^v = \theta_v \mid (\mathsf{T}_\#^t, \mathsf{T}_\#^L, \mathsf{T}_\#^{ks}) = (\theta_t, L, \theta_{ks})].\end{aligned}$$

In the ideal world, we obtain

$$\Pr[\mathsf{T}_{\mathsf{id}} = \theta] = \left(\frac{1}{2^n}\right) \cdot \left(\frac{1}{2^n}\right)^{q'_{ks}} \cdot \left(\frac{1}{2^\tau}\right)^{q_t}. \tag{5}$$

Note that $\Pr[\mathsf{T}_{\mathsf{id}}^v = \theta_v \mid (\mathsf{T}_{\mathsf{id}}^t, \mathsf{T}_{\mathsf{id}}^L, \mathsf{T}_{\mathsf{id}}^{ks}) = (\theta_t, L, \theta_{ks})] = 1$ holds since the adversary always obtains $\perp$ in the ideal world. In the real world, we also obtain

$$\Pr[\mathsf{T}_{\mathsf{re}}^L = L] = \frac{1}{2^n}, \tag{6}$$

$$\Pr[\mathsf{T}_{\mathsf{re}}^{ks} = \theta_{ks} \mid \mathsf{T}_{\mathsf{re}}^L = L] = \left(\frac{1}{2^n}\right)^{q'_{ks}}, \tag{7}$$

$$\Pr[\mathsf{T}_{\mathsf{re}}^t = \theta_t \mid (\mathsf{T}_{\mathsf{re}}^L, \mathsf{T}_{\mathsf{re}}^{ks}) = (L, \theta_{ks})] = \left(\frac{1}{2^\tau}\right)^{q_t}, \tag{8}$$

since θ is good. To be more precise, Eq. (7) holds since **Bad4** and **Bad6** do not happen, and Eq. (8) holds since **Bad1**, **Bad2**, and **Bad6** do not happen. All that remains is evaluating $\Pr[\mathsf{T}_{\mathsf{re}}^{v} = \theta_v \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})]$. For $i \in [1..q_v]$, let $\widehat{T}_i$ be a valid tag for the i-th verification query (N_i^v, A_i^v, C_i^v); thus, $\widehat{T}_i = \mathtt{msb}_\tau(\mathsf{R}(\mathsf{Ctr0}_i^v) \oplus \mathsf{GHASH}_L(A_i^v, C_i^v))$. We then obtain

$$\begin{aligned}
&\Pr[\mathsf{T}_{\mathsf{re}}^{v} = \theta_v \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] \\
&= \Pr[\{T_i^v \neq \widehat{T}_i\}_{i \in [1..q_v]} \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] \\
&\geq 1 - \sum_{i=1}^{q_v} \Pr[T_i^v = \widehat{T}_i \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] \geq 1 - \frac{q_v}{2^\tau}. \qquad (9)
\end{aligned}$$

Here, Eq. (9) holds because $\Pr[T_i^v = \widehat{T}_i \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] \leq 1/2^\tau$ holds; when there exists $j \in [1..q_t]$ *s.t.* $N_i^v = N_j^t$, we obtain $\Pr[T_i^v = \widehat{T}_i \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] = 0$ since **Bad7** does not happen. Otherwise, we obtain $\Pr[T_i^v = \widehat{T}_i \mid (\mathsf{T}_{\mathsf{re}}^{t}, \mathsf{T}_{\mathsf{re}}^{L}, \mathsf{T}_{\mathsf{re}}^{ks}) = (\theta_t, L, \theta_{ks})] \leq 1/2^\tau$ holds since **Bad3**, **Bad5**, and **Bad6** do not happen and $\mathsf{R}(\mathsf{Ctr0}_i^v)$ is uniformly random. From Eqs. (6), (7), (8), and (9), we obtain

$$\Pr[\mathsf{T}_{\mathsf{re}} = \theta] \geq \left(\frac{1}{2^n}\right) \cdot \left(\frac{1}{2^n}\right)^{q'_{ks}} \cdot \left(\frac{1}{2^\tau}\right)^{q_t} \cdot \left(1 - \frac{q_v}{2^\tau}\right). \qquad (10)$$

Eqs. (5) and (10) show

$$\frac{\Pr[\mathsf{T}_{\mathsf{re}} = \theta]}{\Pr[\mathsf{T}_{\mathsf{id}} = \theta]} \geq 1 - \frac{q_v}{2^\tau}. \qquad (11)$$

From Eqs. (3), (4), (11), and Lemma 7, we obtain the following lemma.

Lemma 3. *For any ν, we have*

$$\begin{aligned}
\mathbf{Adv}_{\mathsf{GMAC[R]}}^{\mathtt{Ind+}}(\mathcal{B}) \leq{} & \frac{(0.5q_t^2 + q_t q_v + q_t + q'_{ks} + q_v)(\ell_N + 1)}{2^n} \\
& + \frac{32(q_t + q_v + d - 1)(\rho + d)(\ell_N + 1)}{2^n} + \frac{q_v(\ell_A + 2)}{2^\tau}.
\end{aligned}$$

In particular, when $\nu = 96$,

$$\mathbf{Adv}_{\mathsf{GMAC[R]}}^{\mathtt{Ind+}}(\mathcal{B}) \leq \frac{q_v(\ell_A + 2)}{2^\tau}.$$

Applying Lemma 3 to Eq. (2) derives the upper bound of $\mathbf{Adv}_{\mathsf{GMAC[R]}}^{\mathtt{UF\text{-}CMA+}}(\mathcal{B})$.

From the simulation of the INT-RUP game by the UF-CMA$^+$ adversary $\mathcal{B}$, we can assume $d \leq q_e + q_d$ and $\rho \leq \sigma_e + \sigma_d$ hold. Thus, we have

$$\begin{aligned}
\mathbf{Adv}_{\mathsf{GCM[R]}}^{\mathtt{INT\text{-}RUP}}(\mathcal{A}) \leq{} & \frac{(q_e^2 + 2q_e q_v + 2q_e + 2q_v + 2\sigma_e + 2\sigma_d)(\ell_N + 1)}{2^n} \\
& + \frac{64(2q_e + q_d + q_v - 1)(\sigma_e + \sigma_d + q_e + q_d)(\ell_N + 1)}{2^n} + \frac{2q_v(\ell_A + 2)}{2^\tau},
\end{aligned}$$

and when $\nu = 96$,

$$\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM[R]}}(\mathcal{A}) \leq \frac{2q_v(\ell_A + 2)}{2^\tau}.$$

Combining Eq. (1) and the above bounds concludes the proof.

Remark: alternative bound. In addition to Lemma 2, [NOMI15] shows an alternative bound of $\Pr[\mathsf{Coll}_L([0..m], N_1, N_2)]$. It has a larger constant than Lemma 2 but can be a smaller overall bound depending on the balance of the parameters. We discuss the use of another bound in App. C.

5 Authenticity of CCM under RUP and Nonce Misuse

We show that CCM is NMR-INT-RUP secure. This also means CCM's INT-RUP and NMR-Auth security from the implications shown in Sect. 3.

5.1 Specification of CCM

We describe CCM, partially adopting the notations of Gjiriti *et al.* [GRV21]. As in the case of GCM, we use $\nu := |N|$ and $\tau := |T|$ and assume they are fixed in advance. CCM fixes $n = 128$ and $\nu \in \{56, 64, 72, 80, 88, 96, 104\}$ and $\tau \in \{32, 48, 64, 80, 96, 112, 128\}$. All input and output variables of CCM are assumed to be byte strings. A valid AD A and a valid plaintext M must satisfy $0 \leq |A| < (2^{64}) \cdot 8$ and $0 \leq |M| < (2^{120-\nu}) \cdot 8$. CCM composes a counter mode (which we write as CCTR) and CBC-MAC in a way similar to MAC-then-Encryption, toghther with a certain input encoding applied to CBC-MAC.

Let $\mathsf{flags}(A)$ be a byte determined by AD A and ν and τ. As ν and τ are fixed, we do not write them as arguments. It is defined as $\mathsf{flags}(A) = (0 \,\|\, \mathsf{sign}(A = \varepsilon) \,\|\, \langle \tau/16 - 1\rangle_3 \,\|\, \langle 14 - \nu/8\rangle_3)$, where $\mathsf{sign}(\mathbf{S}) = 0$ if event $\mathbf{S}$ is true, $= 1$ otherwise. Let flags' be a byte $(0^5 \,\|\, \langle 14-\nu/8\rangle_3)$. Due to the range of τ, $\mathsf{flags}' \neq \mathsf{flags}(A)$ holds for any $A \in \{0,1\}^*$. Let $\mathsf{ecN}(N, i) = (\mathsf{flags}' \,\|\, N \,\|\, \langle i \rangle_{120-\nu})$ denote the i-th counter block. CBC-MAC takes an encoded sequence, $B = (B[0], B[1], \ldots, B[\ell])$, generated from (N, A, M). In particular, let $\mathsf{ecB}_0(N, A, M) := (\mathsf{flags}(A) \,\|\, N \,\|\, \langle |M|_8 \rangle_{120-\nu})$ which is used as $B[0]$. To determine the blocks after $B[0]$ in B, ecA encodes A as $\mathsf{ecA}(A) = \mathsf{pad}_n(\mathsf{lenA}(A) \,\|\, A)$. Here, $\mathsf{lenA}(A)$ denotes the length of A. Definitions of ecA and lenA are a bit complex and we omit the full details. See [Dwo07,RW03]. Our proof will only use the following facts: (1) $|\mathsf{ecA}(A)|$ is a multiple of n bits for any valid A, (2) $\mathsf{ecA}(A) \neq \mathsf{ecA}(A')$ for any valid and distinct A and A', and (3) $|\mathsf{ecA}(A)|_n \leq |A|_n + 1$ for any A. Finally, the rest of B blocks are determined by the message encoding function $\mathsf{ecM}(M) := \mathsf{pad}_n(M)$. CBC-MAC takes a full-block sequence of

$$\mathsf{ec}(N, A, M) := \mathsf{ecB}_0(N, A, M) \,\|\, \mathsf{ecA}(A) \,\|\, \mathsf{ecM}(M).$$

The τ-bit output of CBC-MAC taking $\mathsf{ec}(N, A, M)$ is masked by the most significant τ-bit of the first CCTR output with a counter block $\mathsf{ecN}(N, 0)$, which

Algorithm $\mathsf{CCM}.\mathcal{E}[E_K](N,A,M)$

```
$V \leftarrow \mathsf{CBC\text{-}MAC}.\mathcal{T}[E_K](N,A,M)$
$C \leftarrow \mathsf{CCTR}[E_K](N,M)$
$U \leftarrow E_K(\mathsf{ecN}(N,0))$
$T \leftarrow V \oplus \mathtt{msb}_\tau(U)$
return $(C,T)$
```

Algorithm $\mathsf{CCM}.u\mathcal{D}[E_K](N,A,C,T)$

```
$M \leftarrow \mathsf{CCTR}[E_K](N,C)$
return $M$
```

Algorithm $\mathsf{CCM}.\mathcal{D}[E_K](N,A,C,T)$

```
$b = \mathsf{CCM}.\mathcal{V}[E_K](N,A,C,T)$
if $b = \bot$ then return $\bot$
else $M \leftarrow \mathsf{CCM}.u\mathcal{D}[E_K](N,A,C,T)$
return $M$
```

Algorithm $\mathsf{CCM}.\mathcal{V}[E_K](N,A,C,T)$

```
$M \leftarrow \mathsf{CCM}.u\mathcal{D}[E_K](N,A,C,T)$
$V \leftarrow \mathsf{CBC\text{-}MAC}.\mathcal{T}[E_K](N,A,M)$
$U \leftarrow E_K(\mathsf{ecN}(N,0))$
$\widehat{T} \leftarrow V \oplus \mathtt{msb}_\tau(U)$
if $T = \widehat{T}$ then return $\top$
else return $\bot$
```

Algorithm $\mathsf{CBC\text{-}MAC}.\mathcal{T}[E_K](N,A,M)$
(assumes N, A and M are of valid length)

```
$V \leftarrow 0^n$
$B[0] \leftarrow \mathsf{ecB}_0(N,A,M)$
$(B[1],\ldots,B[\ell]) \xleftarrow{n} \mathsf{ecA}(A) \| \mathsf{ecM}(M)$
for $i = 0$ to $\ell$
    $V \leftarrow E_K(V \oplus B[i])$
$V \leftarrow \mathtt{msb}_\tau(V)$
return $V$
```

Algorithm $\mathsf{CBC\text{-}MAC}.\mathcal{V}[E_K](N,A,M,V)$
(assumes N, A and M are of valid length and $|V| = \tau$)

```
$\widehat{V} \leftarrow \mathsf{CBC\text{-}MAC}.\mathcal{T}[E_K](N,A,M)$
if $V = \widehat{V}$ return $\top$
else return $\bot$
```

Algorithm $\mathsf{CCTR}[E_K](N,M)$

```
$(M[1],\ldots,M[m]) \xleftarrow{n} M$
for $i = 1$ to $m-1$
    $C[i] \leftarrow E_K(\mathsf{ecN}(N,i)) \oplus M[i]$
$C[m] \leftarrow \mathtt{msb}_{|M[m]|}(E_K(\mathsf{ecN}(N,m))) \oplus M[m]$
$C \leftarrow C[1] \| \ldots \| C[m]$
return $C$
```

Fig. 3: Algorithms of CCM. $\nu := |N|$ and $\tau := |T|$ are fixed parameters.

becomes a tag. The plaintext M is encrypted by CCTR taking counter blocks $\mathsf{ecN}(N,i)$ for $i = 1,\ldots,|M|_n$. See Fig. 3 for the pseudocode and Fig. 4 for the illustration. As with Sect. 4, Fig. 3 contains the unverified and the verification routines for our analysis.

Definition 7 (Prefix-free encoding). *The encoding function* $\mathsf{ec}(\cdot,\cdot,\cdot)$ *is said to be prefix-free if, for any input* (N,A,M)*, there is no input* (N',A',M') *s.t.* $(N',A',M') \neq (N,A,M)$ *and* $\mathsf{ec}(N',A',M') = \mathtt{msb}_j(\mathsf{ec}(N,A,M))$*, where* $j = |\mathsf{ec}(N',A',M')|$ *and* $j \leq |\mathsf{ec}(N,A,M)|$*. We also say* $\{B = \mathsf{ec}(N,A,M)\}$ *is prefix-free for any input* (N,A,M) *if* $\mathsf{ec}(\cdot,\cdot,\cdot)$ *is prefix-free.*

An important observation is that ec in CCM is indeed prefix-free [Jon03]. This was used by several studies for both attack and proof sides [Jon03, FMVZ08]. It is known that $\mathsf{CBC\text{-}MAC}$ with a prefix-free input encoding realizes a PRF [PR00], however, CCTR and $\mathsf{CBC\text{-}MAC}$ in CCM share the key, and this shared-key structure does not allow to reuse this known result in a black-box way.

5.2 NMR-INT-RUP bound of CCM

Let $\mathsf{CCM}[E_K] = (\mathsf{CCM}.\mathcal{E}[E_K], \mathsf{CCM}.u\mathcal{D}[E_K], \mathsf{CCM}.\mathcal{V}[E_K])$ for the underlying block cipher $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. We suppose the adversary $\mathcal{A}$ makes

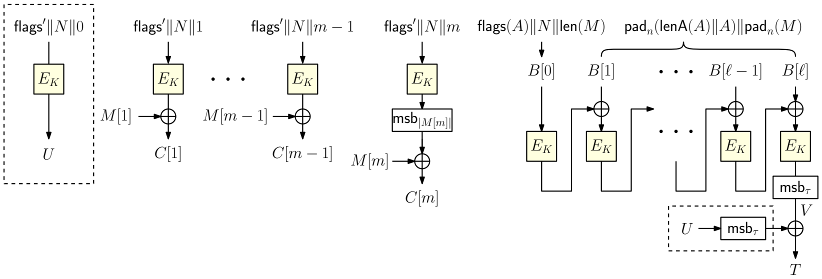

Fig. 4: Encryption of CCM. Our optimization (CCM2, Sect. 8.2) omits the boxes with dashed lines.

q_e queries to CCM.$\mathcal{E}$, q_d queries to CCM.$u\mathcal{D}$, and q_v queries to CCM.$\mathcal{V}$. The adversary $\mathcal{A}$ obtains a transcript such that

- $\{(N_i^e, A_i^e, M_i^e, C_i^e, T_i^e)\}_{i=1,\ldots,q_e}$ from CCM.$\mathcal{E}$,
- $\{(N_i^d, A_i^d, M_i^d, C_i^d, T_i^d)\}_{i=1,\ldots,q_d}$ from CCM.$u\mathcal{D}$,
- $\{(N_i^v, A_i^v, C_i^v, T_i^v, b_i)\}_{i=1,\ldots,q_v}$ from CCM.$\mathcal{V}$, where $b_i \in \{\top, \bot\}$.

Let σ_e, σ_d, and σ_v denote the total number of plaintext/ciphertext blocks queried in CCM.$\mathcal{E}$, CCM$u\mathcal{D}$, and CCM.$\mathcal{V}$, respectively; thus, $\sigma_e = \sum_{i=1}^{q_e} |M_i^e|_n$, $\sigma_d = \sum_{i=1}^{q_d} |C_i^d|_n$, and $\sigma_v = \sum_{i=1}^{q_v} |C_i^v|_n$. Let σ'_e and σ'_v be the total number of input blocks to CBC-MAC.$\mathcal{T}$ in CCM.$\mathcal{E}$ and CCM.$\mathcal{V}$, respectively; thus, $\sigma'_e = \sum_{i=1}^{q_e} |\mathsf{ec}(N_i^e, A_i^e, M_i^e)|_n$ and $\sigma'_v = \sum_{i=1}^{q_v} |\mathsf{ec}(N_i^v, A_i^v, M_i^v)|_n$, where $M_i^v = \mathsf{CCTR}(N_i^v, C_i^v)$. We define $\sigma_{\mathrm{all}} \coloneqq \sigma_e + \sigma_d + \sigma_v + \sigma'_e + \sigma'_v + q_e + q_v$ to denote the total number of block cipher calls in the game.

We present a NMR-INT-RUP bound of CCM. The bound shows up-to-birthday-bound security, hence quantitatively equivalent to the normal Auth bound [Jon03].

Theorem 2. *Let $\mathcal{A}$ be the NMR-INT-RUP adversary against* CCM$[E]$ *defined as above with time complexity t. We have*

$$\mathbf{Adv}_{\mathsf{CCM}[E]}^{\texttt{NMR-INT-RUP}}(\mathcal{A}) \leq \mathbf{Adv}_{E}^{\texttt{PRP}}(\widehat{\mathcal{A}}) + \frac{\sigma_{\mathrm{all}}^2}{2^{n+1}} + \frac{(\sigma'_e + \sigma'_v)(\sigma'_e + \sigma'_v + 2(q_e + q_v + \sigma_e + \sigma_d + \sigma_v))}{2^n} + \frac{4q_v}{2^\tau}$$

for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\mathrm{all}})$.

5.3 Proof of Theorem 2

Overview. We evaluate $\mathbf{Adv}_{\mathsf{CCM}[E]}^{\texttt{NMR-INT-RUP}}(\mathcal{A})$ in the same manner as INT-RUP security proof of GCM. We first apply PRP/PRF switching lemma, show the reduction from NMR-INT-RUP game of CCM to UF-CMA$^+$ of CBC-MAC, and then prove $\mathbf{Adv}_{\mathsf{CBC\text{-}MAC[R]}}^{\texttt{UF-CMA+}}(\mathcal{B})$, where R is an n-bit URF. Note that the tag of CBC-MAC is the unmasked value, V, not the tag of CCM, T.

Step 1. We start with PRP/PRF switching applied to n-bit URP P and URF R. We have

$$\mathbf{Adv}^{\texttt{NMR-INT-RUP}}_{\mathsf{CCM[P]}}(\mathcal{A}) \le \mathbf{Adv}^{\texttt{PRP}}_{E}(\widehat{\mathcal{A}}) + \frac{\sigma_{\text{all}}^2}{2^{n+1}} + \mathbf{Adv}^{\texttt{NMR-INT-RUP}}_{\mathsf{CCM[R]}}(\mathcal{A}') \tag{12}$$

for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\text{all}})$, and an NMR-INT-RUP adversary $\mathcal{A}'$ having the same computational cost as $\mathcal{A}$.

Step 2. We evaluate $\mathbf{Adv}^{\texttt{NMR-INT-RUP}}_{\mathsf{CCM[R]}}(\mathcal{A}')$. Let $\mathsf{CBC\text{-}MAC[R]} = (\mathsf{CBC\text{-}MAC}.\mathcal{T}[\mathsf{R}], \mathsf{CBC\text{-}MAC}.\mathcal{V}[\mathsf{R}])$. See Fig. 3 for the algorithms; note that $\mathsf{CBC\text{-}MAC[R]}$ is not a plain CBC-MAC but includes ec encoding function as a pre-processing of input tuple (N, A, M). The output of $\mathsf{CBC\text{-}MAC}.\mathcal{T}[\mathsf{R}]$ is τ-bit string V. As in the proof in Sect. 4.3, we hereafter may omit "[R]" for denoting the oracles/functions that invoke R, say we write $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ to mean $\mathsf{CBC\text{-}MAC}.\mathcal{T}[\mathsf{R}]$. We define a function to simulate $\mathsf{CCM}.u\mathcal{D}$, the encryption part of $\mathsf{CCM}.\mathcal{E}$ (including the derivation of U), and the decryption part of $\mathsf{CCM}.\mathcal{V}$ in the NMR-INT-RUP game. Let $\mathcal{KS}_{\mathsf{C}}$ be a function invoking R which takes (an encoded form of) a nonce $N \in \{0,1\}^{\nu}$ and an index $\mathsf{idx} \in [0..2^{120-\nu} - 1]$ and outputs a block of key stream $KS \in \{0,1\}^n$. Specifically,

$$\mathcal{KS}_{\mathsf{C}}(N, \mathsf{idx}) := \mathsf{R}(\mathsf{ecN}(N, \mathsf{idx})) = \mathsf{R}(\mathsf{flags}' \,\|\, N \,\|\, \langle \mathsf{idx} \rangle_{120-\nu}).$$

We show that the NMR-INT-RUP game against CCM is simulatable with the UF-CMA$^+$ game against $\mathsf{CBC\text{-}MAC}$ defined in Sect. 4.3.

Lemma 4. *Let $\mathcal{A}$ be an NMR-INT-RUP adversary making q_e, q_d, and q_v queries to $\mathsf{CCM}.\mathcal{E}$, $\mathsf{CCM}.u\mathcal{D}$, and $\mathsf{CCM}.\mathcal{V}$ respectively, and let σ_e, σ_d, σ_v, σ'_e, σ'_v be as defined earlier. We have*

$$\mathbf{Adv}^{\texttt{NMR-INT-RUP}}_{\mathsf{CCM[R]}}(\mathcal{A}) \le \mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$$

for a UF-CMA$^+$ adversary $\mathcal{B}$ against $\mathsf{CCM[R]}$ *making q_e, $q_e + q_v + \sigma_e + \sigma_d + \sigma_v$, and q_v queries to* $\mathsf{CBC\text{-}MAC}.\mathcal{T}$, $\mathcal{KS}_{\mathsf{C}}$, $\mathsf{CBC\text{-}MAC}.\mathcal{V}$, *respectively. Here, $\mathcal{B}$ may repeat nonces for the first oracle.*

The proof of Lemma 4 is in App. D.

Step 3. To evaluate $\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$, we define the following indistinguishability notion as in Sect. 4.3.

$$\mathbf{Adv}^{\texttt{Ind+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B}) := |\Pr[\mathcal{B}^{\mathsf{CBC\text{-}MAC}.\mathcal{T}, \mathcal{KS}_{\mathsf{C}}, \mathsf{CBC\text{-}MAC}.\mathcal{V}} = 1] - \Pr[\mathcal{B}^{\$, \mathsf{R}_{ks}, \perp} = 1]|,$$

where $\$$ (resp. R_{ks}) is a random oracle (resp. URF) whose input/output interface and lengths are the same as $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ (resp. $\mathcal{KS}_{\mathsf{C}}$). Note that R_{ks} is independent of the underlying random function R. Also, $\perp$ oracle has the same input interface as $\mathsf{CBC\text{-}MAC}.\mathcal{V}$ and always returns $\perp$. As in Eq. (2), we obtain

$$\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B}) \le 2\mathbf{Adv}^{\texttt{Ind+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B}). \tag{13}$$

We evaluate $\mathbf{Adv}^{\mathtt{Ind+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$ using the H-coefficient technique. We suppose that $\mathcal{B}$ makes q_t tagging queries, q_{ks} key stream queries, and q_v verification queries. Let $(N^t_i, A^t_i, M^t_i, V^t_i)$, $(N^{ks}_j, \mathsf{idx}_j, KS_j)$, and $(N^v_k, A^v_k, M^v_k, V^v_k)$ be transcripts obtained from i-th tagging query for $i \in [1..q_t]$, j-th key stream query for $j \in [1..q_{ks}]$, and k-th verification query for $k \in [1..q_v]$, respectively. For $\# \in \{t, v\}$ and $i \in [1..q_\#]$, let $\mathsf{ec}(N^\#_i, A^\#_i, M^\#_i) = B^\#_i = (B^\#_i[0], \ldots, B^\#_i[\ell^\#_i])$, and $|B^\#_i|_n = \ell^\#_i + 1$. Let σ'_t and σ'_v be the total number of input blocks to $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ and $\mathsf{CBC\text{-}MAC}.\mathcal{V}$; thus, for $\# \in \{t, v\}$, $\sigma'_\# := \sum_{i=1}^{q_\#}(\ell^\#_i + 1)$.

Simplification of the analysis. To simplify the analysis of $\mathbf{Adv}^{\mathtt{Ind+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$, we give $\mathcal{B}$ all the inputs to R in tagging and verification queries after all queries are made but before it determines an output bit. In the real world, this is straightforward. In the ideal world, we give dummy values, which are basically sampled from $\{0, 1\}^n$ uniformly at random. One important point is that samplings must be *consistent* with queries. This part shows how to do that.

For $i \in [1..q_t]$ and $j \in [0..\ell^t_i]$, let $X^t_i[j]$ be $j+1$-th URF input of $\mathsf{CBC\text{-}MAC}$ in i-th tagging query, and for $i \in [1..q_v]$ and $j \in [0..\ell^v_i]$, let $X^v_i[j]$ be $j+1$-th URF input of $\mathsf{CBC\text{-}MAC}$ in i-th verification query. In the real world, for $\# \in \{t, v\}$, $i \in [1..q_\#]$, and $j \in [1..\ell^\#_i]$, we have

$$X^\#_i[0] = B^\#_i[0],$$
$$X^\#_i[j] = \mathsf{R}(X^\#_i[j-1]) \oplus B^\#_i[j].$$

Here, we list tagging and verification queries as $(N^t_1, A^t_1, M^t_1, V^t_1)$, …, $(N^t_{q_t}, A^t_{q_t}, M^t_{q_t}, V^t_{q_t})$, $(N^v_1, A^v_1, M^v_1, V^v_1)$, …, $(N^v_{q_v}, A^v_{q_v}, M^v_{q_v}, V^v_{q_v})$. Thus, a *previous* query of i-th tagging query $(N^t_i, A^t_i, M^t_i, V^t_i)$ refers to j-th tagging query $(N^t_j, A^t_j, M^t_j, V^t_j)$ for $j < i$. Also, a *previous* query of i-th verification query $(N^v_i, A^v_i, M^v_i, V^v_i)$ refers to j-th verification query $(N^v_j, A^v_j, M^v_j, V^v_j)$ or k-th tagging query $(N^t_k, A^t_k, M^t_k, V^t_k)$ for $j < i$ and $k \in [1..q_t]$.

For $\# \in \{t, v\}$, $i \in [1..q_\#]$, and $j \in [0..\ell^\#_i]$, we classify $X^\#_i[j]$ into the following three cases according to the value of $B^\#_i[0..j]$.

Case1 $X^\#_i[j]$ fulfills either of the following conditions:

(a) For $j = 0$, there are no previous queries *s.t.* $B^\#_i[0] = B^{\#'}_{i'}[0]$ for $\#' \in \{t, v\}$, $i' \in [1..q^\#]$.

(b) For $j \neq 0$, there are no previous queries *s.t.* $B^\#_i[0..j-1] = B^{\#'}_{i'}[0..j-1]$ for $\#' \in \{t, v\}$, $i' \in [1..q^\#]$.

Case2 There is a previous query *s.t.* $B^\#_i[0..j] = B^{\#'}_{i'}[0..j]$, and $X^{\#'}_{i'}[j]$ is classified as **Case1** for $\#' \in \{t, v\}$, $i' \in [1..q^\#]$.

Case3 For $j \neq 0$, $X^\#_i[j]$ fulfills both of the following conditions:

(a) $X^\#_i[j]$ is not classified as **Case2**.

(b) There is a previous query *s.t.* $|B^{\#'}_{i'}|_n \geq j+1$, $B^\#_i[0..j-1] = B^{\#'}_{i'}[0..j-1]$, $B^\#_i[j] \neq B^{\#'}_{i'}[j]$, and $X^{\#'}_{i'}[j]$ is classified as **Case1** for $\#' \in \{t, v\}$, $i' \in [1..q^\#]$.

Let $\mathcal{X}_\$$, $\mathcal{X}_=$, $\mathcal{X}_\oplus$ be a set of $X_i^{\#}[j]$ classified as **Case1**, **Case2**, and **Case3**, respectively. Technically, as each $X_i^{\#}[j]$ is a variable, each set is interpreted as a set of $(i, j, \#)$. Intuitively, $\mathcal{X}_\$$ denotes the set of (the indexes of) $X_i^{\#}[j]$ values that are to be sampled uniformly in the ideal world when $j \neq 0$, $\mathcal{X}_=$ denotes those are equal to a variable $X \in \mathcal{X}_\$$, and $\mathcal{X}_\oplus$ denotes those are determined by a sum of an element $X \in \mathcal{X}_\$$ and blocks in B. We obtain the following lemma.

Lemma 5. *Assume that $\{B_i^{\#}\}_{\# \in \{t,v\}, i \in [1..q_\#]}$ is prefix-free. Let $\mathcal{X}_{all}$ denote the set $\{X_i^{\#}[j]\}_{\# \in \{t,v\}, i \in [1..q_\#], j \in [0..\ell_i^{\#}]}$. Then the set of three sets, $\mathcal{X}_\$$, $\mathcal{X}_=$, and $\mathcal{X}_\oplus$, is a partition of $\mathcal{X}_{all}$. That is, $\mathcal{X}_\$ \cap \mathcal{X}_= = \mathcal{X}_= \cap \mathcal{X}_\oplus = \mathcal{X}_\$ \cap \mathcal{X}_\oplus = \emptyset$ holds and every $X_i^{\#}[j]$ is in any one of $\mathcal{X}_\$$, $\mathcal{X}_=$, $\mathcal{X}_\oplus$.*

The proof is a direct consequence of prefix-free encoding, hence we omit it. We note that, in order for Lemma 5 to hold, the prefix-freeness is necessary. For example, suppose that B_1^t is a prefix of B_2^t; say, suppose that $|B_2^t|_n = 3$ and there is a previous query *s.t.* $|B_1^t|_n = 2$ and $B_2^t[0..1] = B_1^t[0..1] = B_1^t$. In this case, $X_2^t[2]$ cannot be classified as any of the above three cases.

In this paper, we say $X_i^{\#}[j]$ is *a representative node*, when $X_i^{\#}[j] \in \mathcal{X}_\$ \sqcup \mathcal{X}_\oplus$. In the ideal world, when $j = 0$, the adversary can compute $X_i^{\#}[0]$ by itself. For $j \in [1..\ell_i^{\#}]$, the dummy value of $X_i^{\#}[j]$ is determined as follows.

1. When $X_i^{\#}[j] \in \mathcal{X}_\$$, $X_i^{\#}[j]$ is chosen from $\{0,1\}^n$ uniformly at random.
2. When $X_i^{\#}[j] \in \mathcal{X}_=$, $X_i^{\#}[j]$ is determined as $X_i^{\#}[j] = X_{i'}^{\#'}[j]$ using $X_{i'}^{\#'}[j]$ in a previous query, where $B_i^{\#}[0..j] = B_{i'}^{\#'}[0..j]$, and $X_{i'}^{\#'}[j] \in \mathcal{X}_\$$ for $\#' \in \{t, v\}$, $i' \in [1..q^{\#}]$.
3. When $X_i^{\#}[j] \in \mathcal{X}_\oplus$, $X_i^{\#}[j]$ is determined as $X_i^{\#}[j] = X_{i'}^{\#'}[j] \oplus B_{i'}^{\#'}[j] \oplus B_i^{\#}[j]$ using $X_{i'}^{\#'}[j]$ in a previous query, where $|B_{i'}^{\#'}|_n \geq j + 1$, $B_i^{\#}[0..j-1] = B_{i'}^{\#'}[0..j-1]$, $B_i^{\#}[j] \neq B_{i'}^{\#'}[j]$, and $X_{i'}^{\#'}[j] \in \mathcal{X}_\$$ for $\#' \in \{t, v\}$, $i' \in [1..q^{\#}]$.

Definitions of a transcript and bad events. Including all the determined $X_i^{\#}[j]$, we define a transcript $\theta = (\theta_t, \theta_{ks}, \theta_v, \theta_x)$ of the adversary $\mathcal{B}$ such that

– $\theta_t = \{(N_i^t, A_i^t, M_i^t, V_i^t)\}_{i \in [1..q_t]}$,
– $\theta_{ks} = \{(N_i^{ks}, \mathsf{idx}_i, KS_i)\}_{i \in [1..q_{ks}]}$,
– $\theta_v = \{(N_i^v, A_i^v, M_i^v, V_i^v)\}_{i \in [1..q_v]}$,
– $\theta_x = \{X_i^{\#}[j]\}_{\# \in \{t,v\}, i \in [1..q_\#], j \in [0..\ell_i^{\#}]}$.

Note that we exclude $b_i \in \{\top, \bot\}$ in the verification queries from the above definition because an attainable transcript always has $b_i = \bot$.

A transcript θ is bad if any of the following bad events occur, and let Θ_{bad} be the set of bad transcripts. Let Θ_{good} denote the good transcript set following Appendix A.

Bad1 Collision of $X[\cdot]$ corresponding to representative nodes in θ_x: there exists $\#_1, \#_2 \in \{t, v\}$, $i_1 \in [1..q_{\#_1}]$, $i_2 \in [1..q_{\#_2}]$, $j_1 \in [0..\ell_{i_1}^{\#_1}]$, $j_2 \in [0..\ell_{i_2}^{\#_2}]$ *s.t.* $X_{i_1}^{\#_1}[j_1], X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_\$ \sqcup \mathcal{X}_\oplus$ and $X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]$.

Bad2 Collision of $X[\cdot]$ corresponding to a representative node in θ_x and $\mathsf{ecN}(N^{ks}, \mathsf{idx})$ for some $(N^{ks}, \mathsf{idx}, KS) \in \theta_{ks}$: there exists $\# \in \{t, v\}$, $i \in [1..q_{\#}]$, $j \in [0..\ell_i^{\#}]$, $k \in [1..q_{ks}]$ *s.t.* $X_i^{\#}[j] \in \mathcal{X}_{\$} \sqcup \mathcal{X}_{\oplus}$ and $X_i^{\#}[j] = \mathsf{ecN}(N_k^{ks}, \mathsf{idx}_k)$.

Bad3 Successful forgery: there exists $i \in [1..q_v]$ *s.t.* $(N_i^v, A_i^v, M_i^v) = (N_j^t, A_j^t, M_j^t)$ and $V_i^v = V_j^t$ for $j \in [1..q_t]$.

Let **Bad** denote $\mathbf{Bad1} \cup \mathbf{Bad2} \cup \mathbf{Bad3}$. We evaluate $\Pr[\mathsf{T}_{\mathsf{id}} \in \Theta_{\mathrm{bad}}] =: \Pr[\mathbf{Bad}]$.

Bad1 evaluation. We fix $\#_1, \#_2 \in \{t, v\}$, $i_1 \in [1..q_{\#_1}]$, $i_2 \in [1..q_{\#_2}]$, $j_1 \in [0..\ell_{i_1}^{\#_1}]$, $j_2 \in [0..\ell_{i_2}^{\#_2}]$, $(\#_1, i_1, j_1) \neq (\#_2, i_2, j_2)$, *s.t.* both $X_{i_1}^{\#_1}[j_1]$ and $X_{i_2}^{\#_2}[j_2]$ are representative nodes.

First, we consider the case when $j_1 = 0$ or $j_2 = 0$. Without loss of generality, we can assume $j_1 = 0$. When $j_2 = 0$, we obtain $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = 0$ since they are representative nodes. When $j_2 \neq 0$ and $X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_{\$}$, we obtain $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = 1/2^n$ since $X_{i_2}^{\#_2}[j_2]$ is randomly chosen. When $j_2 \neq 0$ and $X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_{\oplus}$, we have $X_{i_2}^{\#_2}[j_2] = X_k^{\#'}[j_2] \oplus B_k^{\#'}[j_2] \oplus B_{i_2}^{\#_2}[j_2]$ for $\#' \in \{t, v\}$, $k \in [q_{\#'}]$, where $X_k^{\#'}[j_2] \in \mathcal{X}_{\$}$ from the definition of $\mathcal{X}_{\oplus}$. Thus, we obtain $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = \Pr[X_{i_1}^{\#_1}[j_1] = X_k^{\#'}[j_2] \oplus B_k^{\#'}[j_2] \oplus B_{i_2}^{\#_2}[j_2]] = 1/2^n$ since $X_k^{\#'}[j_2]$ is randomly chosen.

Second, we assume $j_1 \neq 0$ and $j_2 \neq 0$. We then consider the case when $X_{i_1}^{\#_1}[j_1] \in \mathcal{X}_{\oplus}$ or $X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_{\oplus}$. We can assume $X_{i_1}^{\#_1}[j_1] \in \mathcal{X}_{\oplus}$ *w.l.o.g.* and let $X_{i_1}^{\#_1}[j_1] = X_k^{\#'}[j_1] \oplus B_k^{\#'}[j_1] \oplus B_{i_1}^{\#_1}[j_1]$ for $\#' \in \{t, v\}$, $k \in [q_{\#'}]$, where $X_k^{\#'}[j_1] \in \mathcal{X}_{\$}$. Since $X_k^{\#'}[j_1]$ is randomly chosen, we obtain $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = \Pr[X_k^{\#'}[j_1] \oplus B_k^{\#'}[j_1] \oplus B_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] \leq 1/2^n$. Note that $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = 0$ holds when $\#' = \#_2$, $k = i_2$, $j_1 = j_2$ since $B_{i_2}^{\#_2}[j_1] \oplus B_{i_1}^{\#_1}[j_1] \neq 0$ holds from the definition of $\mathcal{X}_{\oplus}$.

Third, we assume $j_1 \neq 0$ and $j_2 \neq 0$. When both $X_{i_1}^{\#_1}[j_1]$, $X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_{\$}$, $\Pr[X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]] = 1/2^n$ holds since they are randomly chosen.

Summing up all the cases of $(\#_1, i_1, j_1)$, $(\#_2, i_2, j_2)$, we obtain $\Pr[\mathbf{Bad1}] \leq (\sigma'_t + \sigma'_v)^2/2^{n+1}$.

Other bad events. We can evaluate **Bad2** in the same way as **Bad1**; $\Pr[\mathbf{Bad2}] \leq (\sigma'_t + \sigma'_v)q_{ks}/2^n$. Note that $\Pr[X_i^{\#}[0] = \mathsf{ecN}(N_k^{ks}, \mathsf{idx}_k)] = 0$ always holds due to the domain separation in the definition; *i.e.*, $\mathsf{flags}(A_i^{\#}) \neq \mathsf{flags}'$. Regarding **Bad3**, we obtain $\Pr[\mathbf{Bad3}] \leq q_v/2^\tau$ since V_j^t is randomly chosen from $\{0,1\}^\tau$.

Summing up all the bad event probabilities, we obtain

$$\Pr[\mathbf{Bad}] \leq \frac{(\sigma'_t + \sigma'_v)(0.5\sigma'_t + 0.5\sigma'_v + q_{ks})}{2^n} + \frac{q_v}{2^\tau}. \tag{14}$$

Good transcript ratio. We derive a lower bound of $\Pr[\mathsf{T}_{\mathsf{re}} = \theta] / \Pr[\mathsf{T}_{\mathsf{id}} = \theta]$ for $\theta \in \Theta_{\mathrm{good}}$. Let $\# \in \{\mathsf{re}, \mathsf{id}\}$. Let $\mathsf{T}_{\#}^t$, $\mathsf{T}_{\#}^{ks}$, $\mathsf{T}_{\#}^v$, $\mathsf{T}_{\#}^x$ denote the random variables of θ_t, θ_{ks}, θ_v, θ_x in each world, respectively. For a good transcript $\theta \in \Theta_{\mathrm{good}}$,

$$\begin{aligned}\Pr[\mathsf{T}_{\#} = \theta] = \Pr[\mathsf{T}_{\#}^{ks} = \theta_{ks}] \cdot \Pr[\mathsf{T}_{\#}^{x} = \theta_x \mid \mathsf{T}_{\#}^{ks} = \theta_{ks}]\\ \cdot \Pr[\mathsf{T}_{\#}^{t} = \theta_t \mid (\mathsf{T}_{\#}^{ks}, \mathsf{T}_{\#}^{x}) = (\theta_{ks}, \theta_x)]\\ \cdot \Pr[\mathsf{T}_{\#}^{v} = \theta_v \mid (\mathsf{T}_{\#}^{t}, \mathsf{T}_{\#}^{ks}, \mathsf{T}_{\#}^{x}) = (\theta_t, \theta_{ks}, \theta_x)],\end{aligned}$$

holds. In the ideal world, we obtain

$$\Pr[\mathsf{T}_{\mathsf{id}} = \theta] = \left(\frac{1}{2^n}\right)^{q'_{ks}} \cdot \left(\frac{1}{2^n}\right)^{q_x} \cdot \left(\frac{1}{2^\tau}\right)^{q_t}, \tag{15}$$

where q'_{ks} is the number of distinct queries of θ_{ks}, and q_x is the number of $X_i^{\#}[j] \in \mathcal{X}_{\$}$ for $j \neq 0$. Note that $\Pr[\mathsf{T}_{\#}^{v} = \theta_v \mid (\mathsf{T}_{\#}^{t}, \mathsf{T}_{\#}^{ks}, \mathsf{T}_{\#}^{x}) = (\theta_t, \theta_{ks}, \theta_x)] = 1$ holds since the adversary always obtains $\perp$ in the ideal world.

In the real world, we first obtain

$$\Pr[\mathsf{T}_{\mathsf{re}}^{ks} = \theta_{ks}] = \left(\frac{1}{2^n}\right)^{q'_{ks}} \tag{16}$$

since there are q'_{ks} distinct queries in θ_{ks}. Second,

$$\Pr[\mathsf{T}_{\mathsf{re}}^{x} = \theta_x \mid \mathsf{T}_{\mathsf{re}}^{ks} = \theta_{ks}] = \left(\frac{1}{2^n}\right)^{q_x} \tag{17}$$

holds. The reasons are as follows. When $j \neq 0$ and $X_i^{\#}[j] \in \mathcal{X}_{\$}$, we necessarily obtain $X_i^{\#}[j] = \mathsf{R}(X_i^{\#}[j-1]) \oplus B_i^{\#}[j]$, where $X_i^{\#}[j-1]$ is a representative node. Due to $\overline{\textbf{Bad1}}$, there are no collisions between representative nodes in θ_x. Also, due to $\overline{\textbf{Bad2}}$, there are no collisions between representative nodes in θ_x and inputs of R in θ_{ks}. Thus, each $X_i^{\#}[j] \in \mathcal{X}_{\$}$ is fixed with probability $1/2^n$. Once all $X_i^{\#}[j] \in \mathcal{X}_{\$}$ for $j \neq 0$ are fixed, all other $X_{i'}^{\#'}[j']$ in θ_x are determined with probability 1 because when $X_{i'}^{\#'}[j'] \in \mathcal{X}_{=} \sqcup \mathcal{X}_{\oplus}$, $X_{i'}^{\#'}[j']$ can be determined as $X_i^{\#}[j']$ or $X_i^{\#}[j'] \oplus B_i^{\#}[j'] \oplus B_{i'}^{\#'}[j']$, where $X_i^{\#}[j'] \in \mathcal{X}_{\$}$. Therefore, Eq. (17) holds. Third, we obtain

$$\Pr[\mathsf{T}_{\mathsf{re}}^{t} = \theta_t \mid (\mathsf{T}_{\mathsf{re}}^{ks}, \mathsf{T}_{\mathsf{re}}^{x}) = (\theta_{ks}, \theta_x)] = \left(\frac{1}{2^\tau}\right)^{q_t}. \tag{18}$$

The reasons are as follows. Since all tagging queries (N_i^t, A_i^t, M_i^t) for $i \in [1..q_t]$ are distinct and $\{B_i^t\}_{i \in [1..q_t]}$ is prefix-free, all inputs of R deriving V_i^t, *i.e.* $X_i^t[\ell_i^t]$, are all representative nodes. Under the condition $(\mathsf{T}_{\mathsf{re}}^{ks}, \mathsf{T}_{\mathsf{re}}^{x}) = (\theta_{ks}, \theta_x)$, all $\mathsf{R}(X_i^t[\ell_i^t])$ are not fixed because **Bad1** and **Bad2** do not happen, and the prefix-freeness of $\{B_i^{\#}\}_{\# \in \{t,v\}, i \in [1..q_{\#}]}$ ensures that $\mathsf{R}(X_i^t[\ell_i^t])$ is not fixed by the element of θ_x. Also, $\overline{\textbf{Bad1}}$ ensures that all $X_i^t[\ell_i^t]$ are distinct. Thus, we obtain Eq. (18).

Last, we evaluate $\Pr[\mathsf{T}^v_{\mathsf{re}} = \theta_v \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)]$. Let $\widehat{V}_i$ be the valid tag for the i-th verification query (N^v_i, A^v_i, M^v_i). We then obtain

$$\begin{aligned}
&\Pr[\mathsf{T}^v_{\mathsf{re}} = \theta_v \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \\
&= \Pr[\{V^v_i \neq \widehat{V}_i\}_{i\in[1..q_v]} \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \\
&\geq 1 - \sum_{i=1}^{q_v} \Pr[V^v_i = \widehat{V}_i \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \geq 1 - \frac{q_v}{2^\tau}. \qquad (19)
\end{aligned}$$

Here, Eq. (19) holds because $\Pr[V^v_i = \widehat{V}_i \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \leq 1/2^\tau$ holds; when there exists $j \in [1..q_t]$ *s.t.* $(N^v_i, A^v_i, M^v_i) = (N^t_j, A^t_j, M^t_j)$, we obtain $\Pr[V^v_i = \widehat{V}_i \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] = 0$ since $\widehat{V}_i = V^t_j$ holds and **Bad3** does not happen. Suppose that there are no tagging queries *s.t.* $(N^v_i, A^v_i, M^v_i) = (N^t_j, A^t_j, M^t_j)$ for $j \in [1..q_t]$, and we focus on $X^v_i[\ell^v_i]$, which is the input of R deriving $\widehat{V}_i$. When $X^v_i[\ell^v_i]$ is a representative node, similar to the analysis of Eq. (18), $\mathsf{R}(X^v_i[\ell^v_i])$ is not fixed even under the condition $(\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)$ since **Bad1** and **Bad2** do not happen, and $\{B^\#_i\}_{\#\in\{t,v\}, i\in[1..q_\#]}$ is prefix-free. Thus, we obtain $\Pr[V^v_i = \widehat{V}_i \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \leq 1/2^\tau$. When $X^v_i[\ell^v_i]$ is not a representative node, there exists a unique $i' \in [1..q_v]$ *s.t.* $(N^v_i, A^v_i, M^v_i) = (N^v_{i'}, A^v_{i'}, M^v_{i'})$ and thus $X^v_i[\ell^v_i] = X^v_{i'}[\ell^v_{i'}]$, where $X^v_{i'}[\ell^v_{i'}] \in \mathcal{X}_\$$ because the prefix-freeness ensures that there is previous query *s.t.* $(N^v_i, A^v_i, M^v_i) = (N^\#_j, A^\#_j, M^\#_j)$ for $\# \in \{t, v\}$ and $j \in [1..q_\#]$, and we here assume that there are no tagging queries *s.t.* $(N^v_i, A^v_i, M^v_i) = (N^t_j, A^t_j, M^t_j)$ for $j \in [1..q_t]$. Similar to the above case, we obtain $\Pr[V^v_i = \widehat{V}_i \mid (\mathsf{T}^t_{\mathsf{re}}, \mathsf{T}^{ks}_{\mathsf{re}}, \mathsf{T}^x_{\mathsf{re}}) = (\theta_t, \theta_{ks}, \theta_x)] \leq 1/2^\tau$ by using the randomness of $\mathsf{R}(X^v_{i'}[\ell^v_{i'}])$.

From Eqs. (16), (17), (18), (19), we obtain

$$\Pr[\mathsf{T}_{\mathsf{re}} = \theta] \geq \left(\frac{1}{2^n}\right)^{q'_{ks}} \cdot \left(\frac{1}{2^n}\right)^{q_x} \cdot \left(\frac{1}{2^\tau}\right)^{q_t} \cdot \left(1 - \frac{q_v}{2^\tau}\right). \qquad (20)$$

From Eqs. (15), (20), we obtain

$$\frac{\Pr[\mathsf{T}_{\mathsf{re}} = \theta]}{\Pr[\mathsf{T}_{\mathsf{id}} = \theta]} \geq 1 - \frac{q_v}{2^\tau}. \qquad (21)$$

From Eqs. (14), (21), and Lemma 7, we obtain the following lemma.

Lemma 6.

$$\mathbf{Adv}^{\mathtt{Ind+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B}) \leq \frac{(\sigma'_t + \sigma'_v)(0.5\sigma'_t + 0.5\sigma'_v + q_{ks})}{2^n} + \frac{2q_v}{2^\tau}$$

Lemma 6 and Eq. (13) give the bound of $\mathbf{Adv}^{\mathtt{UF\text{-}CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$.

From the simulation of the NMR-INT-RUP game by the UF-CMA$^+$ adversary $\mathcal{B}$, we obtain the following bound.

$$\mathbf{Adv}^{\mathtt{NMR\text{-}INT\text{-}RUP}}_{\mathsf{CCM[R]}}(\mathcal{A}) \leq \frac{(\sigma'_e + \sigma'_v)(\sigma'_e + \sigma'_v + 2(q_e + q_v + \sigma_e + \sigma_d + \sigma_v))}{2^n} + \frac{4q_v}{2^\tau}.$$

By combining Eq. (12) and the above, we conclude the proof of Theorem 2.

6 Privacy of CCM under Nonce Misuse

As Table 1 shows, CCM does not fulfill NMR-Priv. However, CCM still fulfills the weaker NML-Priv. The following theorem shows our bound for CCM.

Theorem 3. *Let q_r and q_m be the number of nonce-respecting and nonce-misusing queries of an adversary $\mathcal{A}$, and σ_{er} and σ_{em} be the total number of plaintext blocks queried to the nonce-respecting and nonce-misusing oracles. Let σ'_r and σ'_m be the total number of input blocks to underlying* $\mathsf{CBC\text{-}MAC}$ *in nonce-respecting and nonce-misusing queries. Let $\sigma_{\mathrm{all}} \coloneqq \sigma'_r + \sigma'_m + \sigma_{er} + \sigma_{em} + q_r + q_m$ and t be the time complexity of $\mathcal{A}$. We obtain*

$$\mathbf{Adv}^{\texttt{NML-Priv}}_{\mathsf{CCM}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\texttt{PRP}}_{E}(\widehat{\mathcal{A}}) + \frac{\sigma_{\mathrm{all}}^2}{2^{n+1}} + \frac{(\sigma'_r + \sigma'_m)(\sigma'_r + \sigma'_m + 2(\sigma_{er} + \sigma_{em} + q_r + q_m))}{2^n}$$

for a PRP adversary $\widehat{\mathcal{A}}$ with σ_{all} queries and time complexity $t + O(\sigma_{\mathrm{all}})$.

The proof is similar to the NMR-INT-RUP proof of CCM described in Sect. 5.3. Specifically, by replacing $\mathsf{CBC\text{-}MAC}$ of the nonce-misusing oracle in the ideal world with a random oracle, we conduct almost the same evaluations of the bad events and the good transcript ratio as in the NMR-INT-RUP proof. See App. E for the full proof.

7 Nonce Misuse Resilience of OCB3

As shown by Table 1, $\mathsf{OCB3}$ has no security with respect to RUP and NMR for both privacy and authenticity. What about NML security? ADL17 provided NML security analysis of OCB. Concretely, they showed NML-Priv and NML-Auth attacks against *the first version of* OCB, also known as $\mathsf{OCB1}$ [RBBK01]. These attacks exploit the incomplete domain separation of $\mathsf{OCB1}$ between the encryption of plaintext blocks and the encryption of checksum and recover $E_K(0^n)$ via repeating nonces. ADL17 stated, "We focus on OCB version 1 [65], however, our results extend to all versions of OCB" [ADL17, Appendix A.1]. While there is no concrete interpretation of this claim, we do show that $\mathsf{OCB3}$ is *not* completely broken regarding NML security.

Theorem 4. $\mathsf{OCB3}$ *has NML-Priv security.*

Theorem 5. $\mathsf{OCB3}$ *does not have NML-Auth security, however, if AD is fixed to any value throughout the game, it maintains NML-Auth security.*

The proofs of Theorems 4 and 5 are straightforward. To prove NML-Priv, we observe that $\mathsf{OCB3}$ can be interpreted as a mode of TBC built on a block cipher, called $\mathsf{\Theta CB3}$ shown in Fig. 5 (App. F). It uses a TBC $\widetilde{E}$ based on XEX and XE modes by Rogaway [Rog04a] but with a more complex tweak space and mask derivation than the original (refer to [KR11] for the specification of $\widetilde{E}$). Thanks to the explicit domain separation via tweaks in $\Theta\mathsf{CB3}$, any output block in an encryption query with nonce N is of the form $\widetilde{E}_K^{(N,\mathtt{x})}(\alpha) \oplus \beta$ for some $\mathtt{x}$ (a tuple of size one or two) and some $\alpha, \beta \in \{0,1\}^n$ that do not involve computation of $\widetilde{E}_K^{(N,\mathtt{y})}$ for any possible $\mathtt{y}$. Suppose $\widetilde{E}_K$ is ideal (*i.e.*, a TURP $\widetilde{\mathsf{P}}$) and consider the real world in the NML-Priv game. The above observation implies that the responses from the first (nonce-respecting) oracle are completely random and independent of the responses from the second (nonce-misusing) oracles since the sets of used nonce values do not intersect. Therefore, $\Theta\mathsf{CB3}$ using $\widetilde{\mathsf{P}}$ is perfectly secure regarding NML-Priv. Thus, we obtain

$$\mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{OCB3[P]}}(\mathcal{A}) = \mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\Theta\mathsf{CB3}[\widetilde{E}[\mathsf{P}]]}(\mathcal{A}) \le \mathbf{Adv}^{\mathtt{TPRP}}_{\widetilde{E}[\mathsf{P}]}(\widehat{\mathcal{A}}) + \mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\Theta\mathsf{CB3}[\widetilde{\mathsf{P}}]}(\mathcal{A}) \le \frac{6\sigma^2}{2^n}$$

for any NML-Priv adversary $\mathcal{A}$ with σ total queried blocks, for a TPRP adversary $\widehat{\mathcal{A}}$ with σ queries. Here, $\widetilde{E}[\mathsf{P}]$ is a TBC built on n-bit URP P, and the last inequality follows from [KR11, Lemma 3][6].

For NML-Auth, if no restriction on AD is imposed, Vaudenay and Vizár [VV18] showed an attack, which exploits the fact that AD processing of $\Theta\mathsf{CB3}/\mathsf{OCB3}$ does not involve nonce. In contrast, the attack generally does not work if A is fixed to any value. In $\Theta\mathsf{CB3}$, AD processing function, Hash, (see Fig. 5) uses distinct tweak values for the internal $\widetilde{\mathsf{P}}$ that are never used in the "core" encryption routine, G, because those used for Hash do not contain nonce while those for G always contain nonce. This fact implies that, if A is fixed to any value throughout the game, the encryption queries with repeating nonces do not contribute, hence can be ignored. Eventually, we can reuse the existing (nonce-respecting) Auth proof of $\Theta\mathsf{CB3}$ [KR11] including the bound. The final bound for $\mathsf{OCB3}$ will be obtained by adding the TBC's security bound [KR11, Lemma 3]. A proof is straightforward and hence omitted.

Some ways to achieve NML-Auth security exist. A simple option is to change Hash of $\Theta\mathsf{CB3}$ so that it takes nonce as a part of the tweak for each AD block process. This also allows the reuse of existing Auth proof even if AD is not fixed, making the modified $\mathsf{OCB3}$ NML secure for both privacy and authenticity. This comes at the cost of losing the property of efficient processing for static AD (*i.e.*, caching Hash(A)). Another option is to add Hash(A) to the checksum instead of the tag, *i.e.*, the tag is an encryption of the sum of checksum and Hash(A). This enables caching static AD, although the proof needs some revisions (future work).

[6] The TBC $\widetilde{E}$ reduces to (variants of) XEX and XE depending on the tweak used, and $\widetilde{E}$ is designed so that it is indistinguishable from TURP as long as the adversary performs CCA against XEX and performs only CPA against XE. This security property is needed for authenticity. We remark that $\mathsf{OCB2}$ [Rog04a] used a similar, but wrong, combination, which leads to an attack [IIMP19]. However, the case of $\mathsf{OCB3}$ is different and safe.

Table 2: Comparison of RUP-secure AEs based on GCM. F and G are PRFs; $F : \mathcal{K}' \times \{0,1\}^* \rightarrow \{0,1\}^\nu$ and $G : \mathcal{K}' \times \{0,1\}^\nu \rightarrow \{0,1\}^\nu$ for some key space $\mathcal{K}'$.

Scheme	Black-box	Additional cost	Online (Dec)	Output expansion∗
PRF-to-IV + GCM	✓	$F_K(N \,\|\, A \,\|\, M)$	✓	ν
GCM-RUP [ADL17]	✗	1 E_K + 1 GF(2^n) Mul †	✗	$n - \nu$
Nonce decoy + GCM	✓	$G_K(N)$	✓	ν

∗ Additional output expansion in bits from the original GCM

† This can be none when the length of the last message block is in $[1..n - \tau]$.

8 Implications of Our Results

Proving robustness property is generally relevant as it gives defense in depth. Still, it is also natural to ask if there are real benefits. We show that this is indeed the case: our results enable 1) an efficient GCM-based RUP-secure AE and 2) an optimized version of CCM without losing security.

8.1 RUP-secure AE

An AE scheme equipped with PA1/2 and INT-RUP security properties is often called *RUP-secure* AE. It has been studied extensively [ABL$^+$14, AFL$^+$16, ADL17, CDD$^+$19]. ABL+14 shows *nonce decoy*, a generic method to turn an AE scheme $\Pi = (\Pi.\mathcal{E}, \Pi.\mathcal{D})$ into a PA1-secure one if Π is PA1 secure under a random nonce setting. It takes an independently-keyed PRF, $G : \mathcal{K}' \times \{0,1\}^\nu \rightarrow \{0,1\}^\nu$, to encrypt the nonce N, and $G_{K'}(N)$ is given to $\Pi.\mathcal{E}$ as an input nonce. Nonce decoy preserves INT-RUP security of the baseline scheme if it has [ABL$^+$14, Proposition 10]. ABL+14 also introduces another conversion scheme, called PRF-to-IV, from an AE scheme Π into a PA1 and INT-RUP secure one if Π is PA1 secure under a random nonce setting. While Π does not need to be INT-RUP secure, it also needs a variable-input-length PRF to take the whole input tuple of (N, A, M), imposing a significant computational overhead. ABL+14 shows that CTR is PA1 secure under a random nonce setting and that PA1 security of GCM and CCM can be reduced to that of CTR. Combining this result of ABL+14 and our INT-RUP results of GCM and CCM, nonce decoy with GCM or CCM implements RUP-secure AE *without modifying the algorithms of* GCM/CCM and *at a small computation overhead*. ADL17 introduces a RUP-secure variant of GCM, GCM-RUP, but this modifies the original algorithm, although the change is not extensive. Compared with GCM-RUP, nonce decoy works as a black-box conversion, enabling an easier adoption from the implementation point of view. Moreover, while the decryption of GCM-RUP cannot be online because of its MAC-then-Decrypt construction, the combination of nonce decoy and GCM preserves its online property. On the downside, as a nature of nonce decoy, the output must be expanded by ν bits from GCM. See the comparison in Table 2.

Table 3: Number of block cipher calls for encryption of a 128-bit block of message without AD. $(2+1)$ means the first two calls are in parallel followed by one call.

Scheme	GCM	CCM	OCB3	COFB	CCM2
Calls	$3*$ (3)	4 (2+2)	4 (2+2)	3 (1+1+1)	3 (2+1)

* GCM needs additional GF(2^{128}) multiplications (2 when $\nu = 96$ and 4 when $\nu \in [1..128] \setminus \{96\}$)

8.2 Optimizing CCM

Our NMR-INT-RUP and NML-Priv proofs imply that the first CCTR output block used to mask CBC-MAC output does not contribute to any security. That is, if that block is omitted, we maintain all the security properties of CCM shown in Table 1. We call such optimized version CCM2. See Fig. 4. The proofs are mainly verbatim to those of NMR-INT-RUP and NML-Priv for CCM. CCM2 reduces the number of block cipher calls by one for any input. The gain seems minor. However, we do not know any example among the popular standards that allow such optimization after their standardization. Adomnicăi *et al.* [AMS23] showed that CCM needs at least four block cipher calls (overhead) for any non-empty message. As far as known in the literature, three is the minimum number of overhead achievable by a general-purpose (*i.e.*, taking variable-length inputs) AE mode, namely COFB [CIMN17, BCI$^+$22]. See Table 3. Overhead is a critical measure to determine the performance for (very) short inputs. Consequently, CCM2 is yet another mode that achieves the overhead of three calls, implying excellent performance for (very) short inputs, notably on microcontrollers [AMS23].

9 Concluding Remarks

We have presented multiple new robustness properties for GCM, CCM, and OCB3. Our results provide a complete answer to the robustness of these standards and serve as a reference point for future research. Notably, CCM's strong robustness is somewhat surprising. This feature was probably not intended by the designers. We understand the design issues around CCM as pointed out by [RW03, Rog11]. Still, our results will give some positive views on this classical mode.

Studying the tightness of our bounds would be an interesting future topic. Extending the targets to the modern schemes, including Sponge AE schemes, would also be interesting. Finally, designing a strongly robust AE mode with minimal overhead (an early attempt is CLOC [IMGM15]), not limited to be based on CCM, is also worth investigating.

References

ABBT15. Mohamed Ahmed Abdelraheem, Peter Beelen, Andrey Bogdanov, and Elmar Tischhauser. Twisted polynomials and forgery attacks on GCM. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 762–786. Springer, Heidelberg, April 2015.

ABL$^+$14. Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. How to securely release unverified plaintext in authenticated encryption. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 105–125. Springer, Heidelberg, December 2014.

ADL17. Tomer Ashur, Orr Dunkelman, and Atul Luykx. Boosting authenticated encryption robustness with minimal modifications. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 3–33. Springer, Heidelberg, August 2017.

AFL$^+$16. Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. RIV for robust authenticated encryption. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 23–42. Springer, Heidelberg, March 2016.

AMS23. Alexandre Adomnicai, Kazuhiko Minematsu, and Junji Shikata. Authenticated encryption for very short inputs. In *CT-RSA 2023*, LNCS, pages 553–572. Springer, Heidelberg, February 2023.

asc. Ascon. https://ascon.iaik.tugraz.at/publications.html.

BBC$^+$20. Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 369–400. Springer, Heidelberg, August 2020.

BCI$^+$22. Subhadeep Banik, Avik Chakraborti, Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT-COFB. Submission to the NIST Lightweight Cryptography project (final round updates), 2022.

BCP22. Jules Baudrin, Anne Canteaut, and Léo Perrin. Practical cube attack against nonce-misused Ascon. *IACR Trans. Symm. Cryptol.*, 2022(4):120–144, 2022.

BDPS14. Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson, and Martijn Stam. On symmetric encryption with distinguishable decryption failures. In Shiho Moriai, editor, *FSE 2013*, volume 8424 of *LNCS*, pages 367–390. Springer, Heidelberg, March 2014.

BGP$^+$19. Francesco Berti, Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. TEDT: a leakage-resistant AEAD mode. *IACR TCHES*, 2020(1):256–320, 2019. https://tches.iacr.org/index.php/TCHES/article/view/8400.

BN00. Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545. Springer, Heidelberg, December 2000.

BN17. Ritam Bhaumik and Mridul Nandi. Improved security for OCB3. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 638–666. Springer, Heidelberg, December 2017.

Boz24. Andrey Bozhko. Properties of AEAD Algorithms. Internet-Draft draft-irtf-cfrg-aead-properties-07, Internet Engineering Task Force, June 2024. Work in Progress.

BR06. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.

BT16. Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 247–276. Springer, Heidelberg, August 2016.

BZD$^+$16. Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, and Philipp Jovanovic. Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. In *WOOT*. USENIX Association, 2016.

cae. Competition for authenticated encryption: Security, applicability, and robustness. https://competitions.cr.yp.to/caesar.html.

CDD$^+$19. Donghoon Chang, Nilanjan Datta, Avijit Dutta, Bart Mennink, Mridul Nandi, Somitra Sanadhya, and Ferdinand Sibleyras. Release of unverified plaintext: Tight unified model and application to ANYDAE. *IACR Trans. Symm. Cryptol.*, 2019(4):119–146, 2019.

CIMN17. Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi. Blockcipher-based authenticated encryption: How small can we go? In Wieland Fischer and Naofumi Homma, editors, *CHES 2017*, volume 10529 of *LNCS*, pages 277–298. Springer, Heidelberg, September 2017.

CS14. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, Heidelberg, May 2014.

cse18. Why is release of unverified plaintext so Bad? StackExchange, 2018. https://crypto.stackexchange.com/questions/59973/why-is-release-of-unverified-plaintext-so-bad.

cse19. How bad it is using the same IV twice with AES/GCM? StackExchange, 2019. https://crypto.stackexchange.com/questions/26790/how-bad-it-is-using-the-same-iv-twice-with-aes-gcm.

cse21. AES GCM : is it acceptable to return the wrong plaintext if the tag is incorrect? StackExchange, 2021. https://crypto.stackexchange.com/questions/89365/aes-gcm-is-it-acceptable-to-return-the-wrong-plaintext-if-the-tag-is-incorrect.

DGRW18. Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage. Fast message franking: From invisible salamanders to encryptment. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 155–186. Springer, Heidelberg, August 2018.

Dwo07. Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality.* NIST-SP 800-38C, 2007.

Fer05. Niels Ferguson. Authentication Weaknesses in GCM. Public Comments to NIST, 2005. http://csrc.nist.gov/groups/ST/toolkit/BCM/comments.html.

FFL12. Ewan Fleischmann, Christian Forler, and Stefan Lucks. McOE: A family of almost foolproof on-line authenticated encryption schemes. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 196–215. Springer, Heidelberg, March 2012.

FMVZ08. Pierre-Alain Fouque, Gwenaëlle Martinet, Frédéric Valette, and Sébastien Zimmer. On the security of the CCM encryption mode and of a slight variant. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *ACNS 08*, volume 5037 of *LNCS*, pages 411–428. Springer, Heidelberg, June 2008.

GRV21. Emiljano Gjiriti, Reza Reyhanitabar, and Damian Vizár. Power yoga: Variable-stretch security of CCM for energy-efficient lightweight IoT. *IACR Trans. Symm. Cryptol.*, 2021(2):446–468, 2021.

HKR15. Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 15–44. Springer, Heidelberg, April 2015.

HP08. Helena Handschuh and Bart Preneel. Key-recovery attacks on universal hash function based MAC algorithms. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 144–161. Springer, Heidelberg, August 2008.

HRRV15. Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway, and Damian Vizár. Online authenticated-encryption and its nonce-reuse misuse-resistance. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 493–517. Springer, Heidelberg, August 2015.

HTT18. Viet Tung Hoang, Stefano Tessaro, and Aishwarya Thiruvengadam. The multi-user security of GCM, revisited: Tight bounds for nonce randomization. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 1429–1440. ACM Press, October 2018.

IIMP19. Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering. Cryptanalysis of OCB2: Attacks on authenticity and confidentiality. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 3–31. Springer, Heidelberg, August 2019.

IMGM15. Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka. CLOC: Authenticated encryption for short input. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 149–167. Springer, Heidelberg, March 2015.

IMI16. Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata. Integrity analysis of authenticated encryption based on stream ciphers. In Liqun Chen and Jinguang Han, editors, *ProvSec 2016*, volume 10005 of *LNCS*, pages 257–276. Springer, Heidelberg, November 2016.

IMI18. Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata. Integrity analysis of authenticated encryption based on stream ciphers. *Int. J. Inf. Sec.*, 17(5):493–511, 2018.

IOM12. Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu. Breaking and repairing GCM security proofs. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 31–49. Springer, Heidelberg, August 2012.

Jon03. Jakob Jonsson. On the security of CTR + CBC-MAC. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 76–93. Springer, Heidelberg, August 2003.

Jou06. Antoine Joux. Authentication Failures in NIST version of GCM. Public Comments to NIST, 2006. http://csrc.nist.gov/groups/ST/toolkit/BCM/comments.html.

KDD17. KDDI Research, Inc. Security Analysis of ChaCha20-Poly1305 AEAD. CRYPTREC-EX-2601-2016, 2017.

KR11. Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Antoine Joux, editor, *FSE 2011*, volume 6733 of *LNCS*, pages 306–327. Springer, Heidelberg, February 2011.

LL24. Jean Liénardy and Frédéric Lafitte. A weakness in OCB3 used with short nonces allowing for a break of authenticity and confidentiality. *Inf. Process. Lett.*, 183:106404, 2024.

LMP17. Atul Luykx, Bart Mennink, and Kenneth G. Paterson. Analyzing multi-key security degradation. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 575–605. Springer, Heidelberg, December 2017.

LP18. Atul Luykx and Bart Preneel. Optimal forgeries against polynomial-based MACs and GCM. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 445–467. Springer, Heidelberg, April / May 2018.

LRW02. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, Heidelberg, August 2002.

MDV15. Aleksandra Mileva, Vesna Dimitrova, and Vesselin Velichkov. Analysis of the Authenticated Cipher MORUS (v1). In *BalkanCryptSec*, volume 9540 of *Lecture Notes in Computer Science*, pages 45–59. Springer, 2015.

MLGR23. Sanketh Menda, Julia Len, Paul Grubbs, and Thomas Ristenpart. Context discovery and commitment attacks - how to break CCM, EAX, SIV, and more. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part IV*, volume 14007 of *LNCS*, pages 379–407. Springer, Heidelberg, April 2023.

MV04. David A. McGrew and John Viega. The security and performance of the Galois/counter mode (GCM) of operation. In Anne Canteaut and Kapalee Viswanathan, editors, *INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 343–355. Springer, Heidelberg, December 2004.

MW16. John Mattsson and Magnus Westerlund. Authentication key recovery on galois/counter mode (GCM). In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT 16*, volume 9646 of *LNCS*, pages 127–143. Springer, Heidelberg, April 2016.

Nan18. Mridul Nandi. Bernstein bound on WCS is tight - repairing luykx-preneel optimal forgeries. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 213–238. Springer, Heidelberg, August 2018.

nisa. Nist internal report 8454: Status report on the final round of the nist lightweight cryptography standardization process. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8454.pdf.

nisb. Nist lightweight cryptography. https://csrc.nist.gov/projects/lightweight-cryptography.

nis07a. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007. National Institute of Standards and Technology.

nis07b. Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality. NIST Special Publication 800-38C, 2007. National Institute of Standards and Technology.

NL15. Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF protocols. IRTF RFC 7539, May 2015. https://tools.ietf.org/html/rfc7539.

NOMI15. Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, and Tetsu Iwata. GCM security bounds reconsidered. In Gregor Leander, editor, *FSE 2015*, volume 9054 of *LNCS*, pages 385–407. Springer, Heidelberg, March 2015.

Pat09. Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, Heidelberg, August 2009.

PC14. Gordon Procter and Carlos Cid. On weak keys and forgery attacks against polynomial-based MAC schemes. In Shiho Moriai, editor, *FSE 2013*, volume 8424 of *LNCS*, pages 287–304. Springer, Heidelberg, March 2014.

PDM$^+$18. Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky, and Jörg Schwenk. Efail: Breaking S/MIME and OpenPGP email encryption using exfiltration channels. In William Enck and Adrienne Porter Felt, editors, *USENIX Security 2018*, pages 549–566. USENIX Association, August 2018.

PR00. Erez Petrank and Charles Rackoff. CBC MAC for real-time data sources. *Journal of Cryptology*, 13(3):315–338, June 2000.

PSV15. Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek. Leakage-resilient authentication and encryption from symmetric cryptographic primitives. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *ACM CCS 2015*, pages 96–108. ACM Press, October 2015.

RBBK01. Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *ACM CCS 2001*, pages 196–205. ACM Press, November 2001.

RFC14. The OCB Authenticated-Encryption Algorithm. IRTF RFC 7253, 2014.

Rog02. Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, *ACM CCS 2002*, pages 98–107. ACM Press, November 2002.

Rog04a. Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, Heidelberg, December 2004.

Rog04b. Phillip Rogaway. Nonce-based symmetric encryption. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 348–359. Springer, Heidelberg, February 2004.

Rog11. Phillip Rogaway. Evaluation of Some Blockcipher Modes of Operation. Investigation Reports on Cryptographic Techniques in FY 2010, 2011. http://www.cryptrec.go.jp/english/.

RS06. Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, Heidelberg, May / June 2006.

RW03. P. Rogaway and D. Wagner. A critique of CCM. Cryptology ePrint Archive, Report 2003/070, 2003. https://eprint.iacr.org/2003/070.

STA$^+$15. Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher v1.1. Submission to the CAESAR competition, 2015.

Vau02. Serge Vaudenay. Security flaws induced by CBC padding - applications to SSL, IPSEC, WTLS... In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 534–546. Springer, Heidelberg, April / May 2002.

VP18. Mathy Vanhoef and Frank Piessens. Release the kraken: New KRACKs in the 802.11 standard. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 299–314. ACM Press, October 2018.

VV18. Serge Vaudenay and Damian Vizár. Can caesar beat galois? - Robustness of CAESAR candidates against nonce reusing and high data complexity attacks. In Bart Preneel and Frederik Vercauteren, editors, *ACNS 18*, volume 10892 of *LNCS*, pages 476–494. Springer, Heidelberg, July 2018.

Supplementary Material

A H-coefficient technique

We assume that an adversary $\mathcal{A}$ queries the two worlds, real and ideal, denoted by $\mathcal{O}_{\mathsf{re}}$ and $\mathcal{O}_{\mathsf{id}}$, and tries to distinguish them. The H-coefficient [Pat09, CS14] is a general technique to evaluate the distinguishing probability of $\mathcal{A}$. We define a *transcript* as a set of input/output values that $\mathcal{A}$ obtains during the interaction with the world. Let T_{re} (*resp.* T_{id}) denote the probability distribution of the transcript induced by the real world (*resp.* the ideal world). By extension, we also use the same notation to refer to a random variable distributed according to each distribution. We say that a transcript θ is *attainable* if $\Pr[\mathsf{T}_{\mathsf{id}} = \theta] > 0$ holds with respect to $\mathcal{A}$. Let Θ denote the set of attainable transcripts. The following is the fundamental lemma of the H-coefficient technique. See *e.g.* [CS14] for the proof.

Lemma 7. *Let $\Theta = \Theta_{\text{good}} \sqcup \Theta_{\text{bad}}$ be a partition of the set of attainable transcripts. Assume that there exists $\varepsilon_1 \geq 0$ such that for any $\theta \in \Theta_{\text{good}}$, one has*

$$\frac{\Pr[\mathsf{T}_{\mathsf{re}} = \theta]}{\Pr[\mathsf{T}_{\mathsf{id}} = \theta]} \geq 1 - \varepsilon_1,$$

and that there exists $\varepsilon_2 \geq 0$ such that $\Pr[\mathsf{T}_{\mathsf{id}} \in \Theta_{\text{bad}}] \leq \varepsilon_2$. Then $|\Pr[\mathcal{A}^{\mathcal{O}_{\mathsf{re}}} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_{\mathsf{id}}} = 1]| \leq \varepsilon_1 + \varepsilon_2$.

B Proof of Lemma 1

We show the INT-RUP game of $\mathcal{A}$ can be simulated by $\mathcal{B}$ in the UF-CMA$^+$ game.

Encryption oracle: $\mathsf{GCM}.\mathcal{E}$ can be simulated using $\mathsf{GMAC}.\mathcal{T}$ and $\mathcal{KS}_{\mathsf{G}}$. Suppose that $\mathcal{A}$ queries (N^e, A^e, M^e) to $\mathsf{GCM}.\mathcal{E}$. To simulate the output of $\mathsf{GCM}.\mathcal{E}$, $\mathcal{B}$ queries $(N^e, 1), \ldots, (N^e, m^e)$ to $\mathcal{KS}_{\mathsf{G}}$, where $m^e = |M^e|_n$, and obtains their outputs $KS_1, \ldots, KS_{m^e}$. Then, $\mathcal{B}$ computes the ciphertext $C^e = M^e \oplus \mathtt{msb}_{|M^e|}(KS_1 \,\|\, \cdots \,\|\, KS_{m^e})$. The tag derivation can also be simulated by querying (N^e, A^e, C^e) to $\mathsf{GMAC}.\mathcal{T}$ and obtaining $T^e = \mathsf{GMAC}.\mathcal{T}(N^e, A^e, C^e)$. Thus, $\mathcal{B}$ can output (C^e, T^e) $(= \mathsf{GCM}.\mathcal{E}(N^e, A^e, M^e))$ with m^e queries to $\mathcal{KS}_{\mathsf{G}}$ and one query to $\mathsf{GMAC}.\mathcal{T}$. The total cost for q_e encryption queries to $\mathsf{GCM}.\mathcal{E}$ is σ_e queries to $\mathcal{KS}_{\mathsf{G}}$ and q_e queries to $\mathsf{GMAC}.\mathcal{T}$. Note that the above simulation maintains the nonce-respecting condition for UF-CMA$^+$ game as long as $\mathcal{A}$ is also nonce-respecting.

Unverified decryption oracle: $\mathsf{GCM}.u\mathcal{D}$ can be simulated using $\mathcal{KS}_{\mathsf{G}}$. Suppose that $\mathcal{A}$ queries (N^d, A^d, C^d, T^d) to $\mathsf{GCM}.u\mathcal{D}$. The adversary $\mathcal{B}$ queries $(N^d, 1)$, …, (N^d, m^d) to $\mathcal{KS}_{\mathsf{G}}$, where $m^d = |C^d|_n$, obtains their outputs $KS_1, \ldots, KS_{m^d}$, and outputs the unverified plaintext $M^d = C^d \oplus \mathtt{msb}_{|C^d|}(KS_1 \,\| \cdots \|\, KS_{m^d})$. The total cost for q_d encryption queries to $\mathsf{GCM}.u\mathcal{D}$ is at most σ_d queries to $\mathcal{KS}_{\mathsf{G}}$.

Verification oracle: $\mathsf{GCM}.\mathcal{V}$ can be simulated by simply forwarding its query to $\mathsf{GMAC}.\mathcal{V}$ since their algorithms are identical. This simulation does not invoke $\mathcal{B}$'s forwarding query from $\mathsf{GMAC}.\mathcal{T}$ to $\mathsf{GMAC}.\mathcal{V}$ since the forwarding queries from $\mathsf{GCM}.\mathcal{E}$ to $\mathsf{GCM}.\mathcal{V}$ are not allowed in INT-RUP game.

Therefore, the queries in INT-RUP game can be simulated by $\mathcal{B}$, and when $\mathcal{A}$ obtains $\top$ from $\mathsf{GCM}.\mathcal{V}$, $\mathcal{B}$ also obtains $\top$ from $\mathsf{GMAC}.\mathcal{V}$. This concludes the proof of Lemma 1.

C Alternative bound for Theorem 1

In addition to Lemma 2, the authors of [NOMI15] show an alternative bound for the probability of $\mathsf{Coll}_L([0..m], N_1, N_2)$ useful for the case $\nu \neq 96$.

Lemma 8 (Lemmas 4 and 5 in [NOMI15]). *For $0 \leq m \leq 2^{32}-1$ and two distinct nonces N_1 and N_2 which are not 96 bits, it holds that $\Pr[\mathsf{Coll}_L([0..m], N_1, N_2)] \leq 2^{32}(\ell_N + 1)/2^n$, where $|N_1|_n, |N_2|_n \leq \ell_N$.*

Lemma 8 could be used to derive another bound for $\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM[P]}}(\mathcal{A})$. While the above bound has a larger constant than that of Lemma 2, it is independent of m. Which lemma we should choose for bad event evaluations depends on the parameters. Specifically, when $(\sigma_e + \sigma_d)/(q_e + q_d) > 2^{27} - 1$, the following bound, based on Lemma 8, is smaller than that of Theorem 1. See [NOMI15, Sect. 6.5] for more details on the comparison.

Theorem 6. *For the same adversary $\mathcal{A}$ as in Theorem 1, we have*

$$\begin{aligned}\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\texttt{PRP}}_{E}(\mathcal{B}) + \frac{\sigma_{\mathrm{all}}^2}{2^{n+1}} \\ + \frac{(q_e^2 + 2q_e q_v + 2q_e + 2q_v + 2\sigma_e + 2\sigma_d)(\ell_N + 1)}{2^n} \\ + \frac{2^{33}(2q_e + q_d + q_v - 1)(q_e + q_d)(\ell_N + 1)}{2^n} + \frac{2q_v(\ell_A + 2)}{2^\tau}\end{aligned}$$

for a PRP adversary $\mathcal{B}$ with σ_{all} queries and time complexity $t + O(\sigma_{\mathrm{all}})$.

Proof. The proof of Theorem 6 mostly follows the proof of Theorem 1 and [NOMI15]. From Lemma 8, we can reevaluate probabilities of **Bad2**, **Bad4**, and **Bad5** as follows.

$$\Pr[\mathbf{Bad2}] \leq \sum_{i=1}^{q_t} \sum_{j=1}^{d} \Pr[\mathsf{Coll}_L([0..\mathsf{idx}_j^{\mathsf{M}}], N_i^t, N_j^{ks*})] \leq q_t d \frac{2^{32}(\ell_N + 1)}{2^n},$$

$$\Pr[\mathbf{Bad4}] \leq \sum_{i=1}^{d} \sum_{\substack{j \neq i \\ j=1}}^{d} \Pr[\mathsf{Coll}_L([0..\mathsf{idx}_j^{\mathsf{M}}], N_i^{ks*}, N_j^{ks*})] \leq d(d-1) \frac{2^{32}(\ell_N + 1)}{2^n},$$

$$\Pr[\mathbf{Bad5}] \leq \sum_{i=1}^{q_v} \sum_{j=1}^{d} \Pr[\mathsf{Coll}_L([0..\mathsf{idx}_j^{\mathsf{M}}], N_i^v, N_j^{ks*})] \leq q_v d \frac{2^{32}(\ell_N + 1)}{2^n}.$$

We then obtain the following evaluations in the same manner as the previous proof.

$$
\begin{aligned}
\Pr[\mathbf{Bad}] &\le \frac{(0.5q_t^2 + q_t q_v + q_t + q'_{ks} + q_v)(\ell_N + 1)}{2^n} \\
&\quad + \frac{2^{32} d(q_t + q_v + d - 1)(\ell_N + 1)}{2^n} + \frac{q_v(\ell_A + 1)}{2^\tau}, \\
\mathbf{Adv}^{\texttt{Ind+}}_{\mathsf{GMAC[R]}}(\mathcal{B}) &\le \frac{(0.5q_t^2 + q_t q_v + q_t + q'_{ks} + q_v)(\ell_N + 1)}{2^n}, \\
&\quad + \frac{2^{32} d(q_t + q_v + d - 1)(\ell_N + 1)}{2^n} + \frac{q_v(\ell_A + 2)}{2^\tau} \\
\mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{GMAC[R]}}(\mathcal{B}) &\le \frac{(q_t^2 + 2q_t q_v + 2q_t + 2q'_{ks} + 2q_v)(\ell_N + 1)}{2^n}, \\
&\quad + \frac{2^{33} d(q_t + q_v + d - 1)(\ell_N + 1)}{2^n} + \frac{2q_v(\ell_A + 2)}{2^\tau}, \\
\mathbf{Adv}^{\texttt{INT-RUP}}_{\mathsf{GCM[R]}}(\mathcal{A}) &\le \frac{(q_e^2 + 2q_e q_v + 2q_e + 2q_v + 2\sigma_e + 2\sigma_d)(\ell_N + 1)}{2^n}, \\
&\quad + \frac{2^{33}(q_e + q_d)(2q_e + q_d + q_v - 1)(\ell_N + 1)}{2^n} + \frac{2q_v(\ell_A + 2)}{2^\tau}.
\end{aligned}
$$

Note that $q_t = q_e$, $q'_{ks} \le q_{ks} = \sigma_e + \sigma_d$, and $d \le q_e + q_d$.

D Proof of Lemma 4

We define a new game, Game-1, against CCM. For Game-1 and an adversary $\mathcal{A}_1$ following Game-1, we relax the NMR-INT-RUP game against $\mathsf{CCM[R]}$ by changing the outputs of $\mathsf{CCM}.\mathcal{E}$ and $\mathsf{CCM}.\mathcal{V}$. When the adversary $\mathcal{A}_1$ queries (N^e, A^e, M^e) and (N^v, A^v, C^v, T^v) to them, suppose it obtains (C^e, U^e, T^e) and (U^v, b), respectively, where $U^\# = \mathsf{R}(\mathsf{ecN}(N^\#, 0))$ for $\# \in \{e, v\}$. We trivially obtain $\mathbf{Adv}^{\texttt{NMR-INT-RUP}}_{\mathsf{CCM[R]}}(\mathcal{A}) \le \mathbf{Adv}^{\texttt{Game-1}}_{\mathsf{CCM[R]}}(\mathcal{A}_1)$ since Game-1 is the same as NMR-INT-RUP game except that Game-1 additionally reveals $U^\#$. Here, the computational resource of $\mathcal{A}_1$ is the same as that of $\mathcal{A}$.

We then prove $\mathbf{Adv}^{\texttt{Game-1}}_{\mathsf{CCM[R]}}(\mathcal{A}_1) \le \mathbf{Adv}^{\texttt{UF-CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$. For a simulation of $\mathsf{CCM}.\mathcal{E}$ in Game-1, $\mathcal{B}$ can forward the query of $\mathcal{A}_1$, (N^e, A^e, M^e), to $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ and obtain V. Then $\mathcal{B}$ queries $(N^e, 0)$, $(N^e, 1)$, …, (N^e, m^e) to $\mathcal{KS}_\mathsf{C}$ and obtains U^e, KS_1, …, KS_{m^e}, where $m^e = |M^e|_n$. As a value of $\mathsf{CCM}.\mathcal{E}(N^e, A^e, M^e)$, $\mathcal{B}$ can return $(C^e, U^e, T^e) = (M^e \oplus \mathtt{msb}_{|M^e|}(KS_1 \,\|\, \cdots \,\|\, KS_{m^e}), U^e, V \oplus \mathtt{msb}_\tau(U^e))$ to $\mathcal{A}_1$. Thus, q_e queries to $\mathsf{CCM}.\mathcal{E}$ of $\mathcal{A}_1$ costs q_e queries to $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ and $\sigma_e + q_e$ queries to $\mathcal{KS}_\mathsf{C}$ of $\mathcal{B}$. Note that the total number of input blocks to $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ equals σ'_e.

Let (N^d, A^d, C^d, T^d) be the unverified decryption query of $\mathcal{A}_1$. For a simulation of $\mathsf{CCM}.u\mathcal{D}$ in Game-1, $\mathcal{B}$ queries $(N^d, 1)$, …, (N^d, m^d) to $\mathcal{KS}_\mathsf{C}$ and obtains KS_1, …, KS_{m^d}, where $m^d = |C^d|_n$, and it returns $M^d = C^d \oplus \mathtt{msb}_{|C^d|}(KS_1 \,\|\, \cdots \,\|\, KS_{m^d})$. Thus, q_d queries to $\mathsf{CCM}.u\mathcal{D}$ of $\mathcal{A}_1$ costs σ_d queries to $\mathcal{KS}_\mathsf{C}$ of $\mathcal{B}$.

For a simulation of $\mathsf{CCM}.\mathcal{V}$ in Game-1, let (N^v, A^v, C^v, T^v) be the query of $\mathcal{A}_1$. Similar to above, $\mathcal{B}$ queries $(N^v, 0)$, $(N^v, 1)$, …, (N^v, m^v) to $\mathcal{KS}_{\mathsf{C}}$ and obtains U^v, $KS_1, \ldots, KS_{m^v}$, where $m^v = |C^v|_n$. Then $\mathcal{B}$ queries (N^v, A^v, M^v, V) to $\mathsf{CBC\text{-}MAC}.\mathcal{V}$, where $M^v = C^v \oplus \mathtt{msb}_{|C^v|}(KS_1 \,\|\, \cdots \,\|\, KS_{m^v})$ and $V = T^v \oplus \mathtt{msb}_\tau(U^v)$ and obtains b, and it can return (U^v, b) to $\mathcal{A}_1$. Thus, q_v queries to $\mathsf{CCM}.\mathcal{V}$ of $\mathcal{A}_1$ costs q_v queries to $\mathsf{CBC\text{-}MAC}.\mathcal{V}$ and $\sigma_v + q_v$ queries to $\mathcal{KS}_{\mathsf{C}}$ of $\mathcal{B}$. Note that the total number of blocks to execute $\mathsf{CBC\text{-}MAC}.\mathcal{V}$ equals σ'_v. This simulation does not invoke $\mathcal{B}$'s forwarding query from $\mathsf{CBC\text{-}MAC}.\mathcal{T}$ to $\mathsf{CBC\text{-}MAC}.\mathcal{V}$ since Game-1 prohibits the forwarding query from $\mathsf{CCM}.\mathcal{E}$ to $\mathsf{CCM}.\mathcal{V}$.

Therefore, the queries in Game-1 can be simulated by $\mathcal{B}$, and when $\mathcal{A}_1$ obtains $\top$ from $\mathsf{CCM}.\mathcal{V}$, $\mathcal{B}$ also obtains $\top$ from $\mathsf{CBC\text{-}MAC}.\mathcal{V}$. Thus, we obtain $\mathbf{Adv}^{\mathtt{Game\text{-}1}}_{\mathsf{CCM[R]}}(\mathcal{A}_1) \le \mathbf{Adv}^{\mathtt{UF\text{-}CMA+}}_{\mathsf{CBC\text{-}MAC[R]}}(\mathcal{B})$, and this concludes the proof of Lemma 4.

E Proof of Theorem 6

We first apply PRP/PRF switching lemma.

$$\mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{CCM}[E]}(\mathcal{A}) \le \mathbf{Adv}^{\mathtt{PRP}}_{E}(\hat{\mathcal{A}}) + \frac{\sigma_{\mathrm{all}}^2}{2^{n+1}} + \mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{CCM[R]}}(\mathcal{A}'), \tag{22}$$

where $\widehat{\mathcal{A}}$ makes σ_{all} queries, and the computational cost of $\mathcal{A}'$ is the same as $\mathcal{A}$. We then define a function $\mathsf{CCM+}.\mathcal{E}[\mathsf{R}]$ by revising the output of $\mathsf{CCM}.\mathcal{E}[\mathsf{R}]$; it takes (N, A, M) as input and outputs (C, U, V), where $U = \mathsf{R}(\mathsf{ecN}(N, 0))$ and $V = T \oplus \mathtt{msb}_\tau(U)$. Since $\mathsf{CCM+}$ just additionally outputs U compared to CCM, we obtain

$$\mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{CCM[R]}}(\mathcal{A}') \le \mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{CCM+[R]}}(\mathcal{B}), \tag{23}$$

where the computational cost of $\mathcal{B}$ is the same as $\mathcal{A}'$.

Let $\mathsf{CCM+\$}.\mathcal{E}[\mathsf{R}]$ be a function obtained by replacing $\mathsf{CBC\text{-}MAC}$ of $\mathsf{CCM+}.\mathcal{E}[\mathsf{R}]$ with a random oracle \$. Thus, $\mathsf{CCM+\$}.\mathcal{E}[\mathsf{R}]$ takes (N, A, M) as input and outputs (C, U, V), where C and U are determined in the same manner as $\mathsf{CCM+}.\mathcal{E}$, but V is chosen from $\{0,1\}^\tau$ at random. We then obtain the following inequations.

$$\begin{aligned}
\mathbf{Adv}^{\mathtt{NML\text{-}Priv}}_{\mathsf{CCM+[R]}}(\mathcal{B}) &= |\Pr[\mathcal{B}^{\mathsf{CCM+}.\mathcal{E},\mathsf{CCM+}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+}.\mathcal{E}} = 1]| \\
&= |\Pr[\mathcal{B}^{\mathsf{CCM+}.\mathcal{E},\mathsf{CCM+}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+}.\mathcal{E}} = 1] \\
&\quad + \Pr[\mathcal{B}^{\$,\mathsf{CCM+\$}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+\$}.\mathcal{E}} = 1]| \\
&\le |\Pr[\mathcal{B}^{\mathsf{CCM+}.\mathcal{E},\mathsf{CCM+}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+\$}.\mathcal{E}} = 1]| \\
&\quad + |\Pr[\mathcal{B}^{\$,\mathsf{CCM+}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+\$}.\mathcal{E}} = 1])| \\
&\le 2|\Pr[\mathcal{B}^{\mathsf{CCM+}.\mathcal{E},\mathsf{CCM+}.\mathcal{E}} = 1] - \Pr[\mathcal{B}^{\$,\mathsf{CCM+\$}.\mathcal{E}} = 1]| \\
&=: 2\mathbf{Adv}^{\mathtt{NML\text{-}Priv\$}}_{\mathsf{CCM+[R]}}(\mathcal{B}).
\end{aligned} \tag{24}$$

We evaluate $\mathbf{Adv}^{\mathtt{NML\text{-}Priv\$}}_{\mathsf{CCM+[R]}}(\mathcal{B})$ using H-coefficient technique. Let $(N^r_i, A^r_i, M^r_i, C^r_i, U^r_i, V^r_i)$ and $(N^m_j, A^m_j, M^m_j, C^m_j, U^m_j, V^m_j)$ be i-th nonce-respecting query for $i \in [1..q_r]$ and j-th nonce-misusing query for $j \in [1..q_m]$, respectively. For $\# \in \{r, m\}$ and $i \in [1..q_\#]$, let $m_i^\# = |M_i^\#|_n$; thus, $\sigma_{er} = \sum_{i=1}^{q_r} m_i^r$ and $\sigma_{em} = \sum_{i=1}^{q_m} m_i^m$. Let $\mathsf{ec}(N_i^\#, A_i^\#, M_i^\#) = B_i^\# = (B_i^\#[0], \ldots, B_i^\#[\ell_i^\#])$, and $|B_i^\#|_n = \ell_i^\# + 1$; thus, $\sigma'_\# = \sum_{i=1}^{q_\#}(\ell_i^\# + 1)$.

Similarly to the NMR-INT-RUP proof of CCM, we suppose that $\mathcal{B}$ obtains all the block cipher inputs in nonce-respecting and nonce-misusing queries after all queries but before determining an output bit. For $\# \in \{r, m\}$, $i \in [q_\#]$ and $j \in [0..\ell_i^\#]$, let $X_i^\#[j]$ be $j+1$-th block cipher input of CBC-MAC in i-th nonce-respecting/nonce-misusing query. Here, we list all queries as $(N_1^r, A_1^r, M_1^r, C_1^r, U_1^r, V_1^r)$, …, $(N_{q_r}^r, A_{q_r}^r, M_{q_r}^r, C_{q_r}^r, U_{q_r}^r, V_{q_r}^r)$, $(N_1^m, A_1^m, M_1^m, C_1^m, U_1^m, V_1^m)$, …, $(N_{q_m}^m, A_{q_m}^m, M_{q_m}^m, C_{q_m}^m, U_{q_m}^m, V_{q_m}^m)$. In the real world, $\mathcal{B}$ obtains the real values of $X_i^\#[j]$. In the ideal world, $\mathcal{B}$ obtains the dummy values of $X_i^\#[j]$, which are determined in the same way as in the NMR-INT-RUP proof of CCM.

Including all the revealed $X_i^\#[j]$, we define a transcript $\theta = (\theta_r, \theta_m, \theta_x)$ of $\mathcal{B}$ such that

- $\theta_r = \{(N_i^r, A_i^r, M_i^r, C_i^r, U_i^r, V_i^r)\}_{i \in [1..q_r]}$,
- $\theta_m = \{(N_i^m, A_i^m, M_i^m, C_i^r, U_i^r, V_i^m)\}_{i \in [1..q_m]}$,
- $\theta_x = \{X_i^\#[j]\}_{\# \in \{r,m\}, i \in [1..q_\#], j \in [0..\ell_i^\#]}$.

Bad event evaluation. We define $\theta \in \Theta_{\text{bad}}$ if at least one of the following events happens in θ.

Bad1 Collision of $X[\cdot]$ corresponding to representative nodes in θ_x: there exists $\#_1, \#_2 \in \{r, m\}$, $i_1 \in [1..q_{\#_1}]$, $i_2 \in [1..q_{\#_2}]$, $j_1 \in [0..\ell_{i_1}^{\#_1}]$, $j_2 \in [0..\ell_{i_2}^{\#_2}]$ *s.t.* $X_{i_1}^{\#_1}[j_1], X_{i_2}^{\#_2}[j_2] \in \mathcal{X}_\$ \sqcup \mathcal{X}_\oplus$ and $X_{i_1}^{\#_1}[j_1] = X_{i_2}^{\#_2}[j_2]$.

Bad2 Collision of $X[\cdot]$ corresponding to representative nodes in θ_x and $\mathsf{ecN}(N^r, \cdot)/\mathsf{ecN}(N^m, \cdot)$ in θ_r/θ_m: there exists $\#_1, \#_2 \in \{r, m\}$, $i_1 \in [1..q_{\#_1}]$, $j_1 \in [0..\ell_{i_1}^{\#_1}]$, $i_2 \in [1..q_{\#_2}]$, $j_2 \in [0..m_{i_2}^{\#_2}]$ *s.t.* $X_{i_1}^{\#_1}[j_1] \in \mathcal{X}_\$ \sqcup \mathcal{X}_\oplus$ and $X_{i_1}^{\#_1}[j_1] = \mathsf{ecN}(N_{i_2}^{\#_2}, j_2)$.

We can evaluate the upper bound of $\Pr[\mathsf{T}_{\mathsf{id}} \in \Theta_{\text{bad}}] \coloneqq \Pr[\mathbf{Bad1} \cup \mathbf{Bad2}]$ in the same manner as that in the NMR-INT-RUP proof of CCM; thus, we obtain

$$\begin{aligned}\Pr[\mathsf{T}_{\mathsf{id}} \in \Theta_{\text{bad}}] &\le \frac{(\sigma'_r + \sigma'_m)^2}{2^{n+1}} + \frac{(\sigma'_r + \sigma'_m)(\sigma_{er} + \sigma_{em} + q_r + q_m)}{2^n} \\ &= \frac{(\sigma'_r + \sigma'_m)(0.5\sigma'_r + 0.5\sigma'_m + \sigma_{er} + \sigma_{em} + q_r + q_m)}{2^n}. \qquad (25)\end{aligned}$$

Good transcript ratio. For $i \in [1..q_m]$, we split transcript $\theta_m = \{(N_i^m, A_i^m, M_i^m, C_i^r, U_i^r, V_i^m)\}$ into $\theta_{m1} = \{(N_i^m, A_i^m, M_i^m, C_i^r, U_i^r)\}$ and $\theta_{m2} = \{V_i^m\}$. For $\# \in \{\mathsf{re}, \mathsf{id}\}$, let $\mathsf{T}_\#^r$, $\mathsf{T}_\#^{m1}$, $\mathsf{T}_\#^{m2}$, $\mathsf{T}_\#^x$ denote the random variables of θ_r, θ_{m1}, θ_{m2}, θ_x in each world, respectively. For a good transcript $\theta \in \Theta_{\text{good}}$, we have

$$\begin{aligned}\Pr[\mathsf{T}_\# = \theta] = \Pr[\mathsf{T}_\#^{m1} = \theta_{m1}] &\cdot \Pr[\mathsf{T}_\#^x = \theta_x \mid \mathsf{T}_\#^{m1} = \theta_{m1}] \\ &\cdot \Pr[\mathsf{T}_\#^r = \theta_r \mid (\mathsf{T}_\#^{m1}, \mathsf{T}_\#^x) = (\theta_{m1}, \theta_x)] \\ &\cdot \Pr[\mathsf{T}_\#^{m2} = \theta_{m2} \mid (\mathsf{T}_\#^r, \mathsf{T}_\#^{m1}, \mathsf{T}_\#^x) = (\theta_r, \theta_{m1}, \theta_x)].\end{aligned}$$

We first obtain $\Pr[\mathsf{T}^{m1}_{\mathsf{re}} = \theta_{m1}] = \Pr[\mathsf{T}^{m1}_{\mathsf{id}} = \theta_{m1}]$ because we define $\mathsf{CCM+\$}.\mathcal{E}$ to output (C, U) in the same distribution as $\mathsf{CCM+}.\mathcal{E}$. In both worlds, we obtain

$$\Pr[\mathsf{T}^{x}_{\#} = \theta_x \mid \mathsf{T}^{m1}_{\#} = \theta_{m1}] = \left(\frac{1}{2^n}\right)^{q_x}, \tag{26}$$

$$\Pr[\mathsf{T}^{r}_{\#} = \theta_r \mid (\mathsf{T}^{m1}_{\#}, \mathsf{T}^{x}_{\#}) = (\theta_{m1}, \theta_x)] = \left(\frac{1}{2}\right)^{\sum_{i=1}^{q_r}|M_i^r|} \left(\frac{1}{2^n}\right)^{q_r} \left(\frac{1}{2^\tau}\right)^{q_r}, \tag{27}$$

$$\Pr[\mathsf{T}^{m2}_{\#} = \theta_{m2} \mid (\mathsf{T}^{r}_{\#}, \mathsf{T}^{m1}_{\#}, \mathsf{T}^{x}_{\#}) = (\theta_r, \theta_{m1}, \theta_x)] = \left(\frac{1}{2^\tau}\right)^{q_m}, \tag{28}$$

where q_x is the number of $X_i^{\#}[j] \in \mathcal{X}_\$$ for $j \neq 0$. In the ideal world, Eq. (26) holds since all $X_i^{\#}[j] \in \mathcal{X}_\$$ for $j \neq 0$ are randomly chosen, and Eqs.(27) and (28) hold since (C_i^r, U_i^r, V_i^r) and V_j^m for $i \in [1..q_r]$, $j \in [1..q_m]$ are output from the random oracles.

In the real world, Eq. (26) holds in the same manner as Eq. (17). All $X_i^{\#}[j] \in \mathcal{X}_\$$, where $j \neq 0$ can be derived using representative node $X_i^{\#}[j-1]$; *i.e.*, $X_i^{\#}[j] = \mathsf{R}(X_i^{\#}[j-1]) \oplus B_i^{\#}[j]$. $\overline{\mathbf{Bad1}}$ and $\overline{\mathbf{Bad2}}$ enables us to fix all $X_i^{\#}[j] \in \mathcal{X}_\$$, where $j \neq 0$, with the probability $(1/2^n)^{q_x}$. Moreover, once all $X_i^{\#}[j] \in \mathcal{X}_\$$ for $j \neq 0$ are fixed, all other $X_i^{\#}[j]$ is fixed with probability 1. Regarding Eq. (27), $\overline{\mathbf{Bad2}}$ and $\mathcal{N}_1 \cap \mathcal{N}_2 = \emptyset$ enables us to fix C_i^r and U_i^r with probability $(1/2)^{\sum_{i=1}^{q_r}|M_i^r|}$ and $(1/2^n)^{q_r}$, respectively. Also, V_i^r can be fixed in the same manner as Eq. (18); distinctness of queries and prefix-freeness ensure all $X_i^r[\ell_i^r]$, which are the input of R deriving V_i^r, are representative nodes. $\overline{\mathbf{Bad1}}$ ensures that all $X_i^r[\ell_i^r]$ are distinct, and $\mathsf{R}(X_i^r[\ell_i^r])$ is not fixed due to $\overline{\mathbf{Bad1}}$, $\overline{\mathbf{Bad2}}$, and prefix-freeness. Similarly, we obtain Eq. (28).

From Eqs. (26), (27), (28), and $\Pr[\mathsf{T}^{m1}_{\mathsf{re}} = \theta_{m1}] = \Pr[\mathsf{T}^{m1}_{\mathsf{id}} = \theta_{m1}]$, we obtain

$$\frac{\Pr[\mathsf{T}_{\mathsf{re}} = \theta]}{\Pr[\mathsf{T}_{\mathsf{id}} = \theta]} = 1 \tag{29}$$

for $\theta \in \Theta_{\mathrm{good}}$. From Eqs. (25) and (29), we obtain the following bound.

$$\mathbf{Adv}^{\texttt{NML-Priv\$}}_{\mathsf{CCM+[R]}}(\mathcal{B}) \leq \frac{(\sigma_r' + \sigma_m')(0.5\sigma_r' + 0.5\sigma_m' + \sigma_{er} + \sigma_{em} + q_r + q_m)}{2^n}. \tag{30}$$

Combining Eqs. (22), (23), (24), (30) concludes the proof.

F Algorithms of ΘCB3

Figure 5 shows the algorithms of ΘCB3.

```
**Algorithm** $\Theta\mathsf{CB3}.\mathcal{E}[\widetilde{E}_K](N, A, M)$

$\Sigma \leftarrow 0^n$
$(M[1], \ldots, M[m-1]) \xleftarrow{n} M$
**for** $i = 1$ **to** $m - 1$ **do**
    $C[i] \leftarrow \widetilde{E}_K^{(N,i)}(M[i])$
    $\Sigma \leftarrow \Sigma \oplus M[i]$
**if** $|M[m]| = n$ **then**
    $C[m] \leftarrow \widetilde{E}_K^{(N,m)}(M[m])$
    $\Sigma \leftarrow \Sigma \oplus M[m]$
    $V \leftarrow \widetilde{E}_K^{(N,m,\$)}(\Sigma)$
**else**
    $C[m] = \mathtt{msb}_{|M[m]|}(\widetilde{E}_K^{(N,m,*)}(0^n) \oplus M[m])$
    $\Sigma \leftarrow \Sigma \oplus (M[m] \,\|\, 10^*)$
    $V \leftarrow \widetilde{E}_K^{(N,m,*\$)}(\Sigma)$
$T \leftarrow \mathtt{msb}_\tau(V \oplus \mathrm{Hash}[\widetilde{E}_K](A))$
$C \leftarrow C[1] \,\|\, \cdots \,\|\, C[m-1] \,\|\, C[m]$
**return** $(C, T)$
```

```
**Algorithm** $\mathrm{Hash}[\widetilde{E}_K](N, A, M)$

$\Gamma \leftarrow 0^n$
$(A[1], \ldots, A[a-1]) \xleftarrow{n} A$
**for** $i = 1$ **to** $a - 1$ **do**
    $\Gamma \leftarrow \Gamma \oplus \widetilde{E}_K^{(i)}(A[i])$
**if** $|A[a]| = n$ **then**
    $\Gamma \leftarrow \Gamma \oplus \widetilde{E}_K^{(m)}(A[m])$
**else**
    $\Gamma \leftarrow \Gamma \oplus \widetilde{E}_K^{(m,*)}(A[m] \,\|\, 10^*)$
**return** $\Gamma$
```

```
**Algorithm** $\Theta\mathsf{CB3}.\mathcal{D}[\widetilde{E}_K](N, A, C, T)$

$\Sigma \leftarrow 0^n$
$(C[1], \ldots, C[m-1]) \xleftarrow{n} C$
**for** $i = 1$ **to** $m - 1$ **do**
    $M[i] \leftarrow \widetilde{D}_K^{(N,i)}(C[i])$
    $\Sigma \leftarrow \Sigma \oplus M[m]$
**if** $|C[m]| = n$ **then**
    $M[m] \leftarrow \widetilde{D}_K^{(N,m)}(C[m])$
    $\Sigma \leftarrow \Sigma \oplus M[m]$
    $V \leftarrow \widetilde{E}_K^{(N,m,\$)}(\Sigma)$
**else**
    $M[m] = \mathtt{msb}_{|C[m]|}(\widetilde{D}_K^{(N,m,*)}(0^n) \oplus C[m])$
    $\Sigma \leftarrow \Sigma \oplus (M[m] \,\|\, 10^*)$
    $V \leftarrow \widetilde{E}_K^{(N,m,*\$)}(\Sigma)$
$\widehat{T} \leftarrow \mathtt{msb}_\tau(V \oplus \mathrm{Hash}[\widetilde{E}_K](A))$
**if** $T \neq \widehat{T}$ **then return** $\perp$
**else**
    $M \leftarrow M[1] \,\|\, \cdots \,\|\, M[m-1] \,\|\, M[m]$
    **return** $M$
```

Fig. 5: Algorithms of $\Theta\mathsf{CB3}[\widetilde{E}_K]$.