Understanding RUP Integrity of COLM

Nilanjan Datta[1], Atul Luykx[2,3], Bart Mennink[4,5] and Mridul Nandi[6]

[1] Indian Institute of Technology, Kharagpur, India
nilanjan_isi_jrf@yahoo.com
[2] imec-COSIC, KU Leuven, Belgium
atul.luykx@esat.kuleuven.be
[3] Department of Computer Science, University of California, Davis
One Shields Ave, Davis, California 95616 USA
[4] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl
[5] CWI, Amsterdam, The Netherlands
[6] Indian Statistical Institute, Kolkata, India
mridul.nandi@gmail.com

Abstract. The authenticated encryption scheme COLM is a third-round candidate in the CAESAR competition. Much like its antecedents COPA, ELmE, and ELmD, COLM consists of two parallelizable encryption layers connected by a linear mixing function. While COPA uses plain XOR mixing, ELmE, ELmD, and COLM use a more involved invertible mixing function. In this work, we investigate the integrity of the COLM structure when unverified plaintext is released, and demonstrate that its security highly depends on the choice of mixing function. Our results are threefold. First, we discuss the practical nonce-respecting forgery by Andreeva et al. (ASIACRYPT 2014) against COPA's XOR mixing. Then we present a nonce-misusing forgery against arbitrary mixing functions with practical time complexity. Finally, by using significantly larger queries, we can extend the previous forgery to be nonce-respecting.

Keywords: Integrity · Release of unverified plaintext · COLM · COPA · ELmD · ELmE

1 Introduction

Authenticated encryption schemes, which target both data confidentiality and integrity simultaneously, have received considerable attention over the last years. The increased interest is in part due to the ongoing CAESAR competition [CAE14], which aims to deliver a portfolio of state-of-the-art authenticated encryption schemes covering a spectrum of security and efficiency trade-offs.

Whereas the security of conventional authenticated encryption schemes, such as OCB1-3 [RBBK01, Rog04, KR11] and GCM [MV04], breaks down if a nonce is used twice, new schemes offer varying degrees of robustness when nonces are reused [FFL12, ABL+13, RS06, HRRV15]. Albeit different levels of confidentiality in the nonce misuse setting may be required depending on the application, the CAESAR competition explicitly mentions that data integrity should never be sacrificed [Ber16].

Schemes implemented in particularly vulnerable environments might demand even stronger security requirements, as described by one of the CAESAR competition's use cases [Ber16], which lists security under release of unverified plaintext (RUP) [ABL+14] as being highly desirable. A RUP-secure authenticated encryption scheme does not leak meaningful information even if its decryption algorithm outputs decrypted ciphertext

Table 1: Summary of our RUP attacks against the COLM type structure. All attacks succeed with overwhelming probability

Mixing	Nonce	Complexity (ignoring constants)			Reference
		Encrypt	Decrypt	Length (blocks)	
XOR	respecting	1	2	$2n$	[ABL+14], Section 4
any	misusing	$4n$	$4n$	$3n$	Section 5
any	respecting	1	$2n$	$(n+1)n$	Section 6

regardless of whether the authentication tag is verified. Such security is particularly desirable in settings where one has not enough memory to store the entire (unverified) plaintext [FJMV03] or for stream-wise authenticated encryption [TSS09]. Related ideas that imply RUP security are schemes that are secure even when multiple distinguishable decryption failures are allowed [BDPS13], or any scheme satisfying robust authenticated encryption [HKR15] (see Barwell et al. [BPS15] for an overview).

Various popular schemes have been shown to be vulnerable in the RUP setting. Andreeva et al. [ABL+14] showed that OCB does not achieve RUP integrity, and Chakraborti et al. [CDN16] presented a RUP integrity attack on any authenticated encryption scheme that makes one block cipher query per message block. For some recent authenticated encryption schemes, such as AEGIS [WP13], ALE [BMR+13], FIDES [BMR+13], and OCB [KR13], the designers explicitly note that unverified plaintexts should not be released. For many authenticated encryption schemes, however, the situation is unknown.

1.1 Our Contribution

Central to this work is the CAESAR submission COLM by Andreeva et al. [ABD+15], a merge of the CAESAR submissions COPA [ABL+15, ABL+13] and ELmD [DN15, DN14]. COLM is a block cipher based design that consists of two layers of parallelizable encryption, connected by a linear mixing functionality. The general structure of COLM is given in Figure 1. Here, E is an n-bit block cipher, K denotes the key, N the nonce, A associated data, M the message, C the ciphertext, and T the tag. The linear mixing layer is a sequential evaluation of linear functions $\rho : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$. In this work, we focus on a generalized linear function of the form

$$\rho(X, W) = (Y, W') = (a \cdot X \oplus b \cdot W\,,\ c \cdot X \oplus d \cdot W)\,,$$

for some $a, b, c, d \neq 0$. A detailed description of the generic COLM type structure is given in Section 3. CAESAR submission COLM [ABD+15] uses the instantiation $(a, b, c, d) = (1, 3, 1, 2)$ (see Section 3.1 for further minor differences). Likewise, COPA is covered by setting $(a, b, c, d) = (1, 1, 1, 1)$, which corresponds to XOR mixing, and ELmE and ELmD by $(a, b, c, d) = (1, 3, 1, 2)$ (disregarding details which are irrelevant for this paper, cf., Section 3.2 and Section 3.3).

COLM and its antecedents are proved to be online authenticated encryption schemes resistant against nonce-misuse adversaries. In this work, we investigate the RUP integrity of the COLM type structure. Although the COLM designers did not claim any RUP security [ABD+15], Bossuet et al. [BDMN16] suggested that ELmD may be RUP secure. It turns out that COLM's RUP integrity strongly depends on the choice of ρ, and we analyze it for various classes of functions. The results are summarized in Table 1. We remark that the attacks below only affect the COLM type structure without intermediate tags and refer to Remark 1 for further discussion on COLM with intermediate tags.

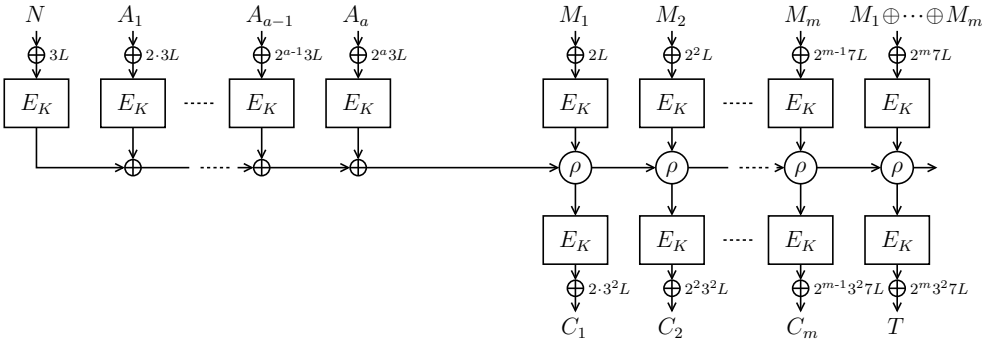


Figure 1: COLM[ρ] type structure for integral data. Here, $L = E_K(0)$.

Nonce-Respecting Attack for XOR Mixing. In Section 4 we consider the case of XOR mixing, i.e.,

$$\rho(X, W) = (X \oplus W, X \oplus W)\,,$$

and present a nonce-respecting forgery that makes 1 encryption query and 2 decryption queries, all of length about $2n$ blocks. We remark that Andreeva et al. [ABL+14] already claimed that their attack against OCB could be directly generalized to COPA. In more detail, they observed that both OCB and COPA generate the tag using the XOR of message blocks, and that therefore the same attack strategy applies. The attack we describe in Section 4 implements this generalization.

Nonce-Misusing Attack for Any Mixing. In Section 5 we consider arbitrary mixing function ρ and present a nonce-misusing forgery in about $4n$ encryption and $4n$ decryption queries, all of length at most about $3n$ blocks. The crux of the attack is that, regardless of the mixing function, one can generate a state collision after 3 message blocks with only 4 encryption and 4 decryption queries. The attack generalizes the previous one in the sense that it also applies to XOR mixing, however, the current attack is in the nonce-misuse setting while the former attack is in the nonce-respecting setting.

Nonce-Respecting Attack for Any Mixing. The nonce-misusing forgery relies on the observation that different queries may have colliding states after triples of blocks, and it does not work in the nonce-respecting setting. In Section 6 we extend our focus, and present a nonce-respecting attacker that makes 1 encryption query and $2n$ decryption queries, and that forges with the same success probability. The attack differs from the nonce-misusing attack in that our new adversary makes significantly larger queries, i.e., of about n^2 blocks. The attack covers any mixing function, and in particular the 1312 mixing used in CAESAR submission COLM and its predecessors ELmE and ELmD:

$$\rho(X, W) = (X \oplus 3W, X \oplus 2W)\,.$$

2 Notation and Security Model

For $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of bit strings of size n. Let $\mathrm{GF}(2^n)$ be the finite field of order 2^n. An element $a = a_{n-1} \cdots a_1 a_0 \in \{0,1\}^n$ can be represented as a polynomial $a(\mathtt{x}) = a_{n-1}\mathtt{x}^{n-1} + \cdots + a_1\mathtt{x} + a_0 \in \mathrm{GF}(2^n)$. Likewise, a can be represented by an integer in $\{0, \ldots, 2^n - 1\}$ which is the evaluation of the polynomial a at $\mathtt{x} = 2$. For two elements $a, b \in \{0,1\}^n$, addition $a \oplus b$ is defined as addition of the polynomials,

$a(\mathtt{x}) + b(\mathtt{x}) \in \mathrm{GF}(2^n)$. Multiplication $a \otimes b$ is defined with respect to the irreducible polynomial $f(\mathtt{x})$ used to represent $\mathrm{GF}(2^n)$: $a(\mathtt{x}) \cdot b(\mathtt{x}) \bmod f(\mathtt{x})$.

By $\mathrm{P}(n)$ we denote the set of all permutations on $\{0,1\}^n$. For a finite set A, $a \xleftarrow{\$} A$ denotes the uniform random drawing of an element a from A. An adversary $\mathcal{A}^{\mathcal{O}}$ is a probabilistic algorithm that has query access to an oracle, or list of oracles, $\mathcal{O}$.

2.1 Block Ciphers

For $k, n \in \mathbb{N}$, a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a mapping such that $E_K = E(K, \cdot)$ is a permutation for every $K \in \{0,1\}^k$. Its security is captured by the SPRP security, which measures the distance between E_K, E_K^{-1} for random key $K \xleftarrow{\$} \{0,1\}^k$ and π, π^{-1} for a random permutation $\pi \xleftarrow{\$} \mathrm{P}(n)$. The attacks in this work are generic, and do not rely on potential weaknesses in the block cipher that is used in the authenticated encryption schemes.

2.2 Authenticated Encryption

We focus on authenticated encryption in the context of the release of unverified plaintext (RUP), and as in [ABL+14] we separate the decryption algorithm into plaintext computation and verification functionalities. An authenticated encryption scheme AE is a triplet of algorithms $\mathrm{AE} = (\mathcal{E}, \mathcal{D}, \mathcal{V})$, where:

$$\begin{aligned} \mathcal{E} &: (K, N, A, M) \mapsto (C, T)\,, \\ \mathcal{D} &: (K, N, A, C, T) \mapsto M\,, \\ \mathcal{V} &: (K, N, A, C, T) \mapsto \top/\bot\,. \end{aligned}$$

Here, K is a key, N a nonce, A associated data, M a message, C its ciphertext, and T the verification tag, and it is required that $\mathcal{D}(K, N, A, \mathcal{E}(K, N, A, M)) = M$ and $\mathcal{V}(K, N, A, \mathcal{E}(K, N, A, M)) = \top$ for any K, A, M.

The conventional security properties of AE are confidentiality, that ciphertexts are indistinguishable from random, and integrity, that a tag is unforgeable. In this paper we focus on integrity in the RUP setting, which differs from conventional integrity by giving the adversary access to the plaintext-computation algorithm $\mathcal{D}$ in addition to the encryption $\mathcal{E}$ and verification $\mathcal{V}$ algorithms.

Definition 1. Let $\mathrm{AE} = (\mathcal{E}, \mathcal{D}, \mathcal{V})$ be an authenticated encryption scheme. The INT-RUP advantage of an adversary $\mathcal{A}$ is defined as

$$\mathsf{INT\text{-}RUP}_{\mathrm{AE}}(\mathcal{A}) = \mathbf{Pr}\left(\mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \mathcal{V}_K} \text{ forges}\right)\,, \tag{1}$$

where $\mathcal{A}$ may not make a query of the form $\mathcal{V}_K(N, A, C, T)$ where $\mathcal{E}_K(N, A, M) = (C, T)$ is a previous encryption query, and where "forges" represents the event that some $\mathcal{V}_K$-query returns $\top$.

We say the adversary is *nonce-respecting* if it does not repeat nonces across encryption queries, otherwise the adversary is said to be *nonce-misusing*. We remark that the adversary may always repeat nonces in queries to $\mathcal{D}_K$ and $\mathcal{V}_K$.

3 COLM Type Structure

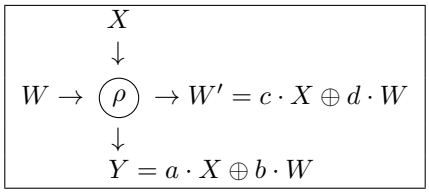
COLM is an authenticated encryption scheme by Andreeva et al. [ABD+15], and a CAESAR competition contestant. It is a merge of two earlier CAESAR submissions, COPA [ABL+15, ABL+13] and ELmD/ELmE [DN15, DN14]. We consider a generic COLM

type structure, and demonstrate how it covers CAESAR submission COLM, as well as COPA and ELmD/ELmE.

The generic COLM type structure consists of two-layer parallelizable encryption masked with the subkey $L = E_K(0)$ and a counter. COLM mixes the output of the first encryption layer to generate the input to the second encryption layer, using the linear mixing function $\rho : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$, where

$$\rho(X, W) = (Y, W') = (a \cdot X \oplus b \cdot W\,,\ c \cdot X \oplus d \cdot W)\,, \tag{2}$$

with $a, b, c, d \neq 0$. The mixing function can be graphically depicted as follows:



By COLM[ρ] we denote this generic COLM type structure with mixing function ρ. For the case of integral data, where the associated data consists of a blocks and the message of m blocks, COLM[ρ] is depicted in Figure 1. Here, state values are denoted by W_i, the message inputs to ρ by X_i, and the ciphertext outputs of ρ by Y_i.

3.1 COLM

CAESAR submission COLM [ABD+15] follows the above generalized structure with the difference that M_m is replaced by the entire checksum as well, and with the following mixing function:

$$\rho_{1312}(X, W) = (X \oplus 3W, X \oplus 2W)\,. \tag{3}$$

We remark that the encryption of two checksums (rather than M_m followed by its checksum) is merely syntactic and does not influence the attacks in this work.

3.2 COPA

The COPA [ABL+15, ABL+13] authenticated encryption scheme differs slightly from the COLM type structure in three aspects:

- It is not based on a nonce; the processing of associated data starts one block earlier;
- The compression of associated data is performed PMAC-style: the evaluation of E_K on the last associated data block is moved to the state. Additionally, the secret key L is XORed into the state afterwards;
- The maskings $2^i 3^j 7^k$ are slightly different.

These aspects do not violate generality. As a matter of fact, the attacks performed in this work are always done for the same associated data and thus state value W_0, and the attacks do not make use of any property of the masking values. Leaving aside these minor aspects, COLM covers COPA via mixing function

$$\rho_{\oplus}(X, W) = (X \oplus W, X \oplus W)\,. \tag{4}$$

For completeness, COPA is depicted in Figure 2.

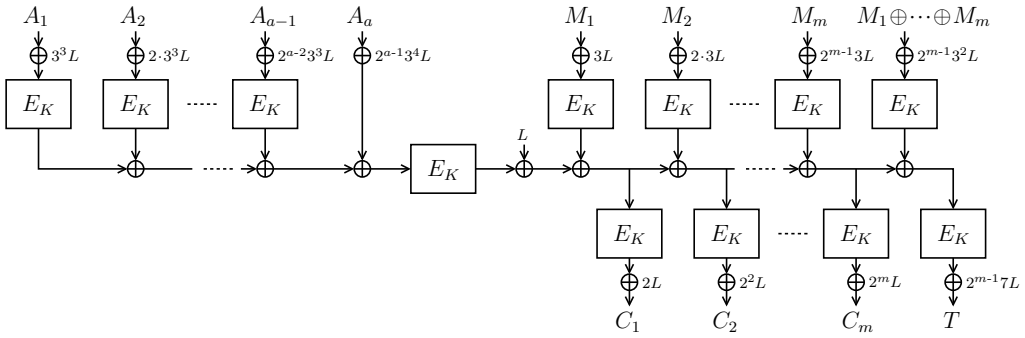


Figure 2: COPA for integral data. Here, $L = E_K(0)$.

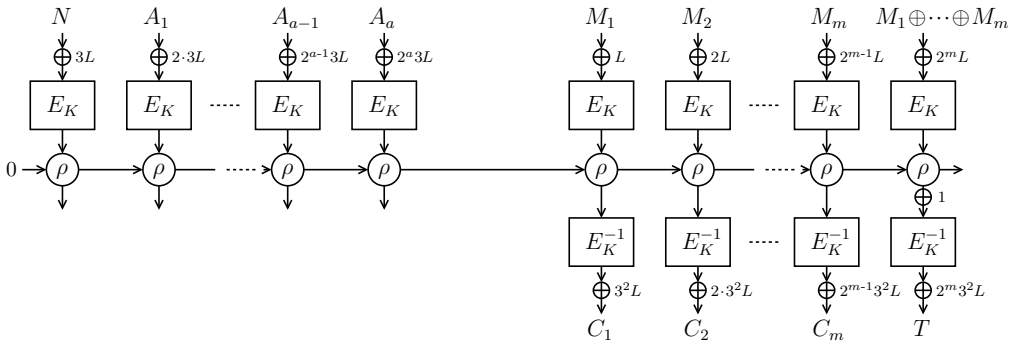


Figure 3: ELmD for integral data. Here, $L = E_K(0)$.

3.3 ELmD/ELmE

ELmD is an authenticated encryption scheme by Datta and Nandi [DN15]. It is closely related to the ELmE construction by the same authors [DN14], that in turn is closely related to COPA but differs in various fundamental aspects. In more detail, ELmD closely follows the COLM type structure of Figure 1, with the following differences:

- The mixing function ρ is also used for the compression of associated data;
- The maskings $2^i3^j7^k$ are slightly different, and in addition, 1 is XORed right before the last call to E in order to prevent length extension attacks (for COLM and COPA this is not needed as security against length extension attacks is done via the masking);
- In the encryption part, the lower-layer block ciphers are evaluated in inverse direction.

As before, these aspects do not violate generality, as our attacks are always done for the same associated data and thus state value W_0. Leaving aside these minor aspects, COLM covers ELmE/ELmD via mixing function ρ_{1312} of (3). For completeness, ELmD is depicted in Figure 3.

4 Nonce-Respecting INT-RUP Attack for XOR Mixing

We prove that COLM with the XOR mixing function $\rho_\oplus$ of (4) is insecure under the release of unverified plaintext. The attack directly applies to COPA and in fact matches the suggested generalization of the attack by Andreeva et al. [ABL+14] against OCB.

Theorem 1. *Let $\ell, n \geq 1$ be such that ℓ is even and $\ell \geq 2n$. There exists a nonce-respecting adversary $\mathcal{A}$ such that*

$$\mathsf{INT\text{-}RUP}_{\mathrm{COLM}[\rho_\oplus]}(\mathcal{A}) \geq 1 - 2^{n-\ell/2}\,, \tag{5}$$

where $\mathcal{A}$ makes 1 encryption query and 2 decryption queries, each of length ℓ blocks.

Proof. We will construct an adversary $\mathcal{A}$ that makes all queries for the same associated data. As a first step $\mathcal{A}$ fixes arbitrary N^*, A^*, and $M^* = M_1^* \cdots M_\ell^* \in \{0,1\}^{n\cdot\ell}$ and queries

$$(C_1^* \cdots C_\ell^*, T^*) \leftarrow \mathcal{E}_K(N^*, A^*, M_1^* \cdots M_\ell^*)\,.$$

$\mathcal{A}$ will succeed if it can construct

$$(N^*, A^*, C_1 \cdots C_\ell, T^*) \tag{6}$$

with $C_\ell = C_\ell^*$ and for which the corresponding decrypted message $M_1, \ldots, M_\ell$ satisfies $\bigoplus_{i=1}^{\ell} M_i = \bigoplus_{i=1}^{\ell} M_i^*$. Indeed, from inspection of Figure 2, we see that the forgery of (6) succeeds if

$$E_K^{-1}(C_\ell \oplus 2^\ell L) \oplus E_K^{-1}(T^* \oplus 2^{\ell-1}7L) = E_K\left(\bigoplus_{i=1}^{\ell} M_i \oplus 2^{\ell-1}3^2 L\right)\,,$$

but this holds due to the choice of $C_\ell = C_\ell^*$ and the condition that $\bigoplus_{i=1}^{\ell} M_i = \bigoplus_{i=1}^{\ell} M_i^*$.

$\mathcal{A}$ proceeds as follows:

1. Randomly choose n-bit strings C_i^0 and C_i^1 such that C_i^0, C_i^1, and C_i^* are mutually distinct for $i \in \{1, 3, \ldots, \ell-1\}$, and define the ciphertexts $C^0 = C_1^0 C_2^* C_3^0 \cdots C_{\ell-2}^* C_{\ell-1}^0 C_\ell^*$ and $C^1 = C_1^1 C_2^* C_3^1 \cdots C_{\ell-2}^* C_{\ell-1}^1 C_\ell^*$;
2. Make the following two plaintext-computation queries (note that the tag input to $\mathcal{D}$ is redundant and omitted for simplicity):

$$M_1^{*,0} M_2^{0,*} M_3^{*,0} \cdots M_{\ell-1}^{*,0} M_\ell^{0,*} \leftarrow \mathcal{D}_K(N^*, A^*, C^0)\,,$$
$$M_1^{*,1} M_2^{1,*} M_3^{*,1} \cdots M_{\ell-1}^{*,1} M_\ell^{1,*} \leftarrow \mathcal{D}_K(N^*, A^*, C^1)\,,$$

   where we remark that in COLM$[\rho_\oplus]$, the ith message block is obtained from the $(i-1)$th and ith ciphertext block for $i \geq 2$, and from A and the 1st ciphertext for $i = 1$;
3. Set $b_0 = b_2 = \cdots = b_\ell := *$, and find $b_1, b_3, \ldots, b_{\ell-1} \in \{0,1\}$ such that

$$\bigoplus_{i=1}^{\ell} M_i^{b_{i-1}, b_i} = \bigoplus_{i=1}^{\ell} M_i^*\,. \tag{7}$$

   This is a set of n equations with $\ell/2$ unknowns which can be solved using Gaussian elimination. This system of equations has a solution with probability at least $1 - 2^{n-\ell/2}$ [BM97, App. A];
4. Output forgery

$$(N^*, A^*, C_1^{b_1} \cdots C_{\ell-1}^{b_{\ell-1}} C_\ell^{b_\ell}, T^*)\,.$$

The forgery is successful by design, and the attack works provided that (7) has a solution. □

5 Generalized Nonce-Misusing INT-RUP Attack

We present a nonce-misusing INT-RUP attack against COLM with arbitrary linear mixing function ρ as described in Eq. (2). The attack is much more general than that of Section 4, and as a result is more complex and requires nonce-misuse. The attack crucially relies on a sub-procedure to generate non-trivial state collisions for messages/ciphertexts consisting of 3 blocks. This procedure will first be discussed in the next lemma.

Lemma 1. *Let N be any nonce, A any associated data, $M_1^0 \in \{0,1\}^n$ any message block, and consider the following four queries to* COLM[ρ] *(ignoring tags):*

$$\begin{aligned} C_1^0 C_2^0 C_3^0 &\leftarrow \mathcal{E}_K(N, A, M_1^0 \star \star)\,, \\ M_1^1 M_2^1 M_3^1 &\leftarrow \mathcal{D}_K(N, A, \star C_2^0 \star)\,, \\ M_1^2 M_2^2 M_3^2 &\leftarrow \mathcal{D}_K(N, A, \star \star C_3^0)\,, \\ C_1^3 C_2^3 C_3^3 &\leftarrow \mathcal{E}_K(N, A, \star M_2^1 M_3^2)\,, \end{aligned}$$

where a $\star$ represents any n-bit string. Then, the third state of the final query, W_3^3, is independent of M_1^0.

Proof. Consider Figure 1 and denote the input values to ρ by X_i^j. Denote the state values by W_i^j, where $W_0^0 = W_0^1 = W_0^2 = W_0^3 =: W_0$ since the nonce and associated data input are kept constant throughout. We have:

$$\begin{aligned} W_3^3 &= c \cdot X_3^3 \oplus d \cdot W_2^3 \\ &= c \cdot X_3^3 \oplus cd \cdot X_2^3 \oplus d^2 \cdot W_1^3 \\ &= c \cdot X_3^3 \oplus cd \cdot X_2^3 \oplus cd^2 \cdot X_1^3 \oplus d^3 \cdot W_0\,. \end{aligned}$$

In the second $\mathcal{E}_K$ query, the second and third message blocks are M_2^1 and M_3^2, respectively, therefore we know that $X_2^3 = X_2^1$ and $X_3^3 = X_3^2$. Furthermore, $Y_2^1 = Y_2^0$ and $Y_3^2 = Y_3^0$ since the first and second $\mathcal{D}_K$-queries use C_2^0 and C_3^0 in their input. Therefore

$$\begin{aligned} X_3^3 = X_3^2 &= a^{-1} \cdot \left(Y_3^2 \oplus b \cdot W_2^2\right) = a^{-1} \cdot \left(Y_3^0 \oplus b \cdot W_2^2\right), \\ X_2^3 = X_2^1 &= a^{-1} \cdot \left(Y_2^1 \oplus b \cdot W_1^1\right) = a^{-1} \cdot \left(Y_2^0 \oplus b \cdot W_1^1\right), \end{aligned}$$

and so

$$W_3^3 = a^{-1}c \cdot \left(Y_3^0 \oplus d \cdot Y_2^0\right) \oplus a^{-1}bc \cdot W_2^2 \oplus a^{-1}bcd \cdot W_1^1 \oplus cd^2 \cdot X_1^3 \oplus d^3 \cdot W_0\,. \tag{8}$$

Note that

$$\begin{aligned} Y_3^0 \oplus d \cdot Y_2^0 &= \Big(a \cdot X_3^0 \oplus b \cdot (c \cdot X_2^0 \oplus d \cdot (c \cdot X_1^0 \oplus d \cdot W_0))\Big) \\ &\quad \oplus d \cdot \Big(a \cdot X_2^0 \oplus b \cdot (c \cdot X_1^0 \oplus d \cdot W_0)\Big) \\ &= a \cdot X_3^0 \oplus (bc \oplus ad) \cdot X_2^0\,, \end{aligned}$$

and (8) satisfies

$$W_3^3 = c \cdot X_3^0 \oplus a^{-1}c(bc \oplus ad) \cdot X_2^0 \oplus a^{-1}bc \cdot W_2^2 \oplus a^{-1}bcd \cdot W_1^1 \oplus cd^2 \cdot X_1^3 \oplus d^3 \cdot W_0\,.$$

These values are all independent of M_1^0 by construction. □

In order for Lemma 1 to apply, we need to query $\mathcal{E}_K$ and $\mathcal{D}_K$ under the same nonce and in a particular order. The rationale behind the attack is that the value X_1^0 coming from the first query contributes to the state value in the second and third query at different places, and by clever composition of the last encryption query, it eventually disappears for that query.

We can make two important observations on Lemma 1:

1. At the cost of four encryption queries, and four decryption queries, each of length 3 blocks (plus the prefixed associated data), one can derive two tuples $M_1M_2M_3 \neq M_1'M_2'M_3'$ such that their final states satisfy $W_3 = W_3'$. This is done by applying Lemma 1 to two distinct messages $M_1^0 \neq M_1^{0'}$, where the two applications are performed for *the same messages* at the $\star$ positions, and by subsequently defining

$$M_1M_2M_3 := M_1^3M_2^1M_3^2 \text{ and } M_1'M_2'M_3' := M_1^3M_2^{1'}M_3^{2'}.$$

   Note that, indeed, we must keep M_1^3 the same in both applications of the procedure: the final states of the two evaluations are independent of M_1^0 and $M_1^{0'}$, but they do depend on whatever is entered at the $\star$'s;

2. The two queries of above observation need not necessarily been done for the same nonce and associated data, as long as the state value prior to the compression of the first message block, W_0, is the same for all queries. Likewise, suppose that $M, M' \in \{0,1\}^{n\cdot\alpha}$ are two distinct messages for which $\mathcal{E}_K(N, A, M) = C$ and $\mathcal{E}_K(N, A, M') = C'$ have the same αth state $W_\alpha = W_\alpha$, one can prepend M (resp. C) to the encryption (resp. decryption) queries corresponding to the message M_1^0, and likewise M' and C' for the queries corresponding to message $M_1^{0'}$, and the resulting tuples $M_1M_2M_3 \neq M_1'M_2'M_3'$ satisfy that $M \parallel M_1M_2M_3$ and $M' \parallel M_1'M_2'M_3'$ have the same final state $W_{\alpha+3} = W_{\alpha+3}$. We will refer to this principle as "stretching the collision."

Using Lemma 1, and particularly above two observations, we can derive our nonce-misusing attack on COLM.

Theorem 2. *Let $\ell, n \geq 1$ be such that $\ell \geq 3n$. There exists a nonce-misusing adversary $\mathcal{A}$ such that*

$$\mathsf{INT\text{-}RUP}_{\mathrm{COLM}[\rho]}(\mathcal{A}) \geq 1 - 2^{n-\ell/3}, \tag{9}$$

where $\mathcal{A}$ makes $4\ell/3+1$ encryption queries and $4\ell/3$ decryption queries, each of length at most ℓ blocks.

Proof. Define $\mu = \ell/3$ and assume, without loss of generality, that μ is integral. We will construct an adversary $\mathcal{A}$ that makes all queries for the same nonce and associated data. Inspired by Lemma 1, the attack will be performed in *chunks of* 3 *blocks*, where we will use an overline ($\overline{M}$) to make explicit that we are referring to a chunk.

At a high level, the attack consists of two parts. In the first part, the adversary $\mathcal{A}$ constructs two messages $\overline{M}_1^0 \cdots \overline{M}_\mu^0 \in \{0,1\}^{n\cdot 3\mu}$ and $\overline{M}_1^1 \cdots \overline{M}_\mu^1 \in \{0,1\}^{n\cdot 3\mu}$ that satisfy $W_{3i}^0 = W_{3i}^1$ for all $i = 1, \ldots, \mu$. These two messages will be constructed chunk-wise. Then, in the second part, the adversary uses a trick comparable to that in Theorem 1 to construct a forgery with the correct checksum.

As a first step, $\mathcal{A}$ fixes any nonce N and associated data A.

- **First chunk.** Using observation (1), obtain two message chunks $\overline{M}_1^0 \neq \overline{M}_1^1$ that satisfy $W_3^0 = W_3^1$. The step consists of 2 executions of the procedure of Lemma 1;
- ***i*th chunk for $i = 2, \ldots, \mu$.** Using observation (2) we stretch the collision as follows: for $M = \overline{M}_1^0 \cdots \overline{M}_{i-1}^0$ and $M' = \overline{M}_1^1 \cdots \overline{M}_{i-1}^1$, obtain two message chunks $\overline{M}_i^0 \neq \overline{M}_i^1$ for which

$$\mathcal{E}_K(N, A, M \parallel \overline{M}_i^0) \text{ and } \mathcal{E}_K(N, A, M' \parallel \overline{M}_i^1)$$

  have the same $(3i)$th state $W_{3i}^0 = W_{3i}^1$. For each iteration, the step consists of 2 executions of the procedure of Lemma 1;

- We have now obtained two messages $M^0 = \overline{M}_1^0 \cdots \overline{M}_\mu^0$ and $M^1 = \overline{M}_1^1 \cdots \overline{M}_\mu^1$ such that $\overline{M}_i^0 \neq \overline{M}_i^1$ and $W_{3i}^0 = W_{3i}^1$ for all $i = 1, \ldots, \mu$;
- Fix any $M = M_1 \cdots M_\ell \in \{0,1\}^{n \cdot \ell}$ such that $M \notin \{M^0, M^1\}$, and query
$$(C, T) \leftarrow \mathcal{E}_K(N, A, M)\,.$$
We will use T as our target tag;[1]
- Find $b_1, \ldots, b_\mu \in \{0,1\}$ such that
$$\bigoplus_{i=1}^{\mu} M_{3i-2}^{b_i} \oplus M_{3i-1}^{b_i} \oplus M_{3i}^{b_i} = \bigoplus_{i=1}^{\ell} M_i\,. \tag{10}$$
This is a set of n equations with μ unknowns which can be solved using Gaussian elimination. This system of equations has a solution with probability at least $1 - 2^{n-\mu}$ [BM97, App. A];
- Output forgery
$$(N, A, \overline{C}_1^{b_1} \cdots \overline{C}_\mu^{b_\mu}, T)\,.$$

The forgery is successful by design, and the attack works provided that (10) has a solution. It consists of $2\mu = 2\ell/3$ applications of the procedure of Lemma 1, each of which costs 2 encryption and 2 decryption queries. In addition, one encryption query is made to determine T. □

6 Generalized Nonce-Respecting INT-RUP Attack

In addition to the result of Section 5, it turns out that the COLM type structure can also be attacked in the nonce-respecting setting, be it with messages of length at least n^2 blocks. The attack resembles ideas of the attack against ELmE with intermediate tags in [DN14, Section 5.2]. Just like the attack of Section 5, the new attack also consists of a sub-procedure in Lemma 2 to derive colliding state values, but to comply with the condition that nonces should never be repeated in encryption queries, queries are only made in inverse direction.

The attack is given in full generality, i.e., for arbitrary primitive polynomial $f(\mathtt{x})$ and for any ρ of the form (2). An easier to grasp version of the proof for ρ_{1312} of (3) (but still arbitrary primitive polynomial) is given in Appendix A.

Lemma 2. *Denote the primitive polynomial by* $f(\mathtt{x}) = \mathtt{x}^n + \mathtt{x}^{\kappa_1} + \cdots + \mathtt{x}^{\kappa_l}$ *for some even* l *and* $n > \kappa_1 > \cdots > \kappa_l = 0$.[2] *Let* N *be any nonce,* A *any associated data, and consider the following two queries to* COLM[ρ] *(ignoring tags):*
$$M_1^0 \cdots M_{n+1}^0 \leftarrow \mathcal{D}_K(N, A, C_1^0 C_2^0 \cdots C_{n+1}^0)\,,$$
$$M_1^1 \cdots M_{n+1}^1 \leftarrow \mathcal{D}_K(N, A, C_1^1 C_2^0 \cdots C_{n+1}^0)\,,$$
where $C_1^0 \neq C_1^1$ *and the* C_i^j*'s may take any value. There exists a partition* $\{1, \ldots, n+1\} = I_0 \cup I_1$ *such that the query*
$$C_1^2 \cdots C_{n+1}^2 \leftarrow \mathcal{E}_K(N, A, M_1^{2_1} \cdots M_{n+1}^{2_{n+1}})\,,$$
where $2_i = 0$ *if* $i \in I_0$ *and* $2_i = 1$ *if* $i \in I_1$*, forms a collision on the* $(n+1)$*th state with the second query:* $W_{n+1}^1 = W_{n+1}^2$.

[1] The step is in fact redundant, but it aids the comprehensibility of the attack.

[2] Note that if l were odd, $f(\mathtt{x})$ is divisible by $\mathtt{x}+1$, whereas if $\kappa_l > 0$, $f(\mathtt{x})$ is divisible by $\mathtt{x}$. In both cases, $f(\mathtt{x})$ would not be a primitive polynomial.

Proof. Consider Figure 1 for any linear mixing ρ, where, without loss of generality, $a, b, c, d \neq 0$. Define $e = a^{-1}bc \oplus d$ and denote the input values to ρ by X_i^j, the output values by Y_i^j, and the state values by W_i^j, where $W_0^0 = W_0^1 = W_0^2 =: W_0$ by construction. Without loss of generality, we will select sets I_0 and I_1 such that $1 \in I_0$. We have:

$$\begin{aligned}
W_{n+1}^2 &= cX_{n+1}^{2^{n+1}} \oplus cdX_n^{2^n} \oplus \cdots \oplus cd^n X_1^{2^1} \oplus d^{n+1}W_0 \\
&\overset{(1)}{=} a^{-1}c\Big(Y_{n+1}^{2^{n+1}} \oplus a^{-1}bcY_n^{2^{n+1}} \oplus \cdots \oplus a^{-1}bce^{n-1}Y_1^{2^{n+1}} \oplus be^n W_0\Big) \\
&\quad \oplus a^{-1}cd\Big(Y_n^{2^n} \oplus a^{-1}bcY_{n-1}^{2^n} \oplus \cdots \oplus a^{-1}bce^{n-2}Y_1^{2^n} \oplus be^{n-1}W_0\Big) \\
&\quad \oplus \cdots \\
&\quad \oplus a^{-1}cd^{n-1}\Big(Y_2^{2^2} \oplus a^{-1}bcY_1^{2^2} \oplus beW_0\Big) \\
&\quad \oplus a^{-1}cd^n\Big(Y_1^{2^1} \oplus bW_0\Big) \\
&\quad \oplus d^{n+1}W_0 \\
&\overset{(2)}{=} \bigoplus_{i=2}^{n+1}\left(\bigoplus_{j=0}^{n-i} a^{-2}bc^2d^je^{n-i-j} \oplus a^{-1}cd^{n+1-i}\right)Y_i^0 \\
&\quad \oplus \Xi^0 \cdot Y_1^0 \oplus \Xi^1 \cdot Y_1^1 \\
&\quad \oplus \Big(a^{-1}bce^n \oplus a^{-1}bcde^{n-1} \oplus \cdots \oplus a^{-1}bcd^n \oplus d^{n+1}\Big)W_0\,,
\end{aligned}$$

where (1) holds as

$$X_i^{2^i} = a^{-1}Y_i^{2^i} \oplus a^{-2}bcY_{i-1}^{2^i} \oplus \cdots \oplus a^{-2}bce^{i-2}Y_1^{2^i} \oplus a^{-1}be^{i-1}W_0\,, \tag{11}$$

(2) holds as $Y_i^1 = Y_i^0$ for $i = 2, \ldots, n+1$, and where

$$\begin{aligned}
\Xi^0 &:= \bigoplus_{i \in I_0 \setminus \{1\}} a^{-2}bc^2d^{n+1-i}e^{i-2} \oplus a^{-1}cd^n\,, \\
\Xi^1 &:= \bigoplus_{i \in I_1} a^{-2}bc^2d^{n+1-i}e^{i-2} = \left(\bigoplus_{j=0}^{n-1} a^{-2}bc^2d^je^{n-1-j} \oplus a^{-1}cd^n\right) \oplus \Xi^0\,.
\end{aligned}$$

(Note that Ξ^0 includes the term $a^{-1}cd^n$, which comes from the fact that $1 \in I_0$.) An identical reasoning, again relying on (11), shows that

$$\begin{aligned}
W_{n+1}^1 &= \bigoplus_{i=2}^{n+1}\left(\bigoplus_{j=0}^{n-i} a^{-2}bc^2d^je^{n-i-j} \oplus a^{-1}cd^{n+1-i}\right)Y_i^0 \\
&\quad \oplus \left(\bigoplus_{j=0}^{n-1} a^{-2}bc^2d^je^{n-1-j} \oplus a^{-1}cd^n\right)Y_1^1 \\
&\quad \oplus \Big(a^{-1}bce^n \oplus a^{-1}bcde^{n-1} \oplus \cdots \oplus a^{-1}bcd^n \oplus d^{n+1}\Big)W_0\,,
\end{aligned}$$

and thus that $W_{n+1}^1 \oplus W_{n+1}^2 = \Xi^0 \cdot (Y_1^0 \oplus Y_1^1)$. Recall that $e = a^{-1}bc \oplus d$ and define $f = ed^{-1}$. We obtain that

$$\begin{aligned}
ac^{-1}d^{-n}\Xi^0 &= \bigoplus_{i \in I_0 \setminus \{1\}} a^{-1}bcd^{-1}(a^{-1}bcd^{-1} \oplus 1)^{i-2} \oplus 1 \\
&= \bigoplus_{i \in I_0 \setminus \{1\}} (f \oplus 1)f^{i-2} \oplus 1\,.
\end{aligned} \tag{12}$$

Due to our assumption that $a, b, c, d \neq 0$, we have $f \neq 1$. If we can prove the existence of a subset $I'_0 \subseteq \{0, \ldots, n-1\}$ such that

$$\bigoplus_{i \in I'_0} f^i = (f \oplus 1)^{-1}\,, \tag{13}$$

then for $I_0 = \{1\} \cup \{i+2 \mid i \in I'_0\}$, the term of (12) equals 0, and we obtain $W^1_{n+1} = W^2_{n+1}$.

Remains to prove the existence of a set I'_0 such that (13) holds. Denote $F_2 = \mathrm{GF}(2)$ and $F_{2^n} = \mathrm{GF}(2^n)$ for brevity. Consider the field $F_2(f)$, which is a subfield of F_{2^n}. As $f \neq 1$, $(f \oplus 1)^{-1} \in F_2(f)$, and thus there is a polynomial

$$p(f) = b_{n-1} f^{n-1} + b_{n-2} f^{n-2} + \cdots + b_1 f + b_0$$

for $b_0, \ldots, b_{n-1} \in \{0, 1\}$ such that $p(f) = (f \oplus 1)^{-1}$. Here, we used that f is an element of a field which has dimension n over F_2, and thus that the smallest degree polynomial over F_2 with f as a root is at most n. The proof is completed by putting $I'_0 = \{i \mid b_i = 1\}$. □

Lemma 2 structurally differs from Lemma 1. Whereas for Lemma 1 the second, third, and fourth query were carefully composed to eliminate the dependency on X^0_1, in the current setting we cannot make two encryption queries under the same nonce. Instead, The procedure consists of making two decryption queries, and compose their outcomes depending on the actual primitive polynomial, in such a way that the difference initiated by the first block "fades away" after n iterations.

The procedure of Lemma 2 can be used to derive, at the cost of two decryption queries of length $n+1$ blocks, two tuples $M_1 \cdots M_{n+1} \neq M'_1 \cdots M'_{n+1}$ such that their final states satisfy $W_{n+1} = W'_{n+1}$. This is done by defining

$$M_1 \cdots M_{n+1} := M^1_1 \cdots M^1_{n+1} \text{ and } M'_1 \cdots M'_{n+1} := M^2_1 \cdots M^2_{n+1}\,.$$

The ciphertext corresponding to the first message is known: $C_1 \cdots C_{n+1} := C^1_1 C^0_2 \cdots C^0_{n+1}$. The ciphertext corresponding to $M'_1 \cdots M'_{n+1}$ is unknown, and the adversary should not make the corresponding encryption query for nonce N in order not to violate the nonce-respecting condition. Fortunately, there is no need to do so: the "stretching", as it was done in Section 5, works without knowing $C'_1 \cdots C'_{n+1}$. In more detail, denote the $(n+1)$-block message and ciphertext chunks by (M, C) and (M', C'), where C' is unknown. Alongside observation 2 after Lemma 1, one can prepend $C = C_1 \cdots C_{n+1}$ to the ciphertexts in the two decryption queries, and subsequently obtain two new tuples $M_1 \cdots M_{n+1} \neq M'_1 \cdots M'_{n+1}$ such that

$$M \parallel M_1 \cdots M_{n+1}\,, M \parallel M'_1 \cdots M'_{n+1}\,, M' \parallel M_1 \cdots M_{n+1}\,, M' \parallel M'_1 \cdots M'_{n+1}$$

have the same $2(n+1)$th state. In other words, the stretching has been performed without making any encryption query. We can use this idea to derive our nonce-respecting attack on COLM.

Theorem 3. *Let $\ell, n \geq 1$ be such that $\ell \geq (n+1)n$. There exists a nonce-respecting adversary $\mathcal{A}$ such that*

$$\mathsf{INT\text{-}RUP}_{\mathrm{COLM}[\rho]}(\mathcal{A}) \geq 1 - 2^{n - \ell/(n+1)}\,, \tag{14}$$

where $\mathcal{A}$ makes 1 encryption query and $2\ell/(n+1)$ decryption queries, each of length at most ℓ blocks.

Proof. Define $\mu = \ell/(n+1)$ and assume, without loss of generality, that μ is integral. We will construct an adversary $\mathcal{A}$ that makes all queries for the same nonce and associated data. The attack is fairly similar to that of Theorem 2, with the difference that in the

current proof chunks of $n+1$ blocks are involved, and an overline ($\overline{M}$) refers to a chunk of $n+1$ blocks. In more detail, in the first part of the attack, the adversary $\mathcal{A}$ constructs two messages $\overline{M}_1^0 \cdots \overline{M}_\mu^0 \in \{0,1\}^{n\cdot(n+1)\mu}$ and $\overline{M}_1^1 \cdots \overline{M}_\mu^1 \in \{0,1\}^{n\cdot(n+1)\mu}$ that satisfy $W^0_{(n+1)i} = W^1_{(n+1)i}$ for all $i = 1, \ldots, \mu$. The second part of the attack, where a correct checksum is developed, is fairly identical to that of Theorem 2.

As a first step, $\mathcal{A}$ fixes any nonce N and associated data A.

- **First chunk.** Using Lemma 2, obtain two message chunks $\overline{M}_1^0 \neq \overline{M}_1^1$ that satisfy $W^0_{n+1} = W^1_{n+1}$. Note that the ciphertext corresponding to $\overline{M}_1^0$ is known, the ciphertext corresponding to $\overline{M}_1^1$ is not known;
- ***i*th chunk for $i = 2, \ldots, \mu$.** Using above stretching observation for $M = \overline{M}_1^0 \cdots \overline{M}_{i-1}^0$ and $M' = \overline{M}_1^1 \cdots \overline{M}_{i-1}^1$ (i.e., by prepending the ciphertext C corresponding to M to the two decryption queries in Lemma 2) obtain two message chunks $\overline{M}_i^0 \neq \overline{M}_i^1$ for which

  $$\mathcal{E}_K(N, A, M \,\|\, \overline{M}_i^0) \text{ and } \mathcal{E}_K(N, A, M' \,\|\, \overline{M}_i^1)$$

  have the same $(n+1)i$th state $W^0_{(n+1)i} = W^1_{(n+1)i}$. Note that these two encryption queries are not actually made. The ciphertext corresponding to $M \,\|\, \overline{M}_i^0$ is known, the ciphertext corresponding to $M' \,\|\, \overline{M}_i^1$ is not known;
- We have now obtained two messages $M^0 = \overline{M}_1^0 \cdots \overline{M}_\mu^0$ and $M^1 = \overline{M}_1^1 \cdots \overline{M}_\mu^1$ such that $\overline{M}_i^0 \neq \overline{M}_i^1$ and $W^0_{(n+1)i} = W^1_{(n+1)i}$ for all $i = 1, \ldots, \mu$;
- Fix any $M = M_1 \cdots M_\ell \in \{0,1\}^{n\cdot\ell}$ such that $M \notin \{M^0, M^1\}$, and query

  $$(C, T) \leftarrow \mathcal{E}_K(N, A, M)\,.$$

  We will use T as our target tag;
- Find $b_1, \ldots, b_\mu \in \{0,1\}$ such that

  $$\bigoplus_{i=1}^{\mu} \left(\bigoplus_{j=0}^{n} M^{b_i}_{(n+1)i-j} \right) = \bigoplus_{i=1}^{\ell} M_i\,. \tag{15}$$

  This is a set of n equations with μ unknowns which can be solved using Gaussian elimination. This system of equations has a solution with probability at least $1 - 2^{n-\mu}$ [BM97, App. A];
- Output forgery

  $$(N, A, \overline{C}_1^{b_1} \cdots \overline{C}_\mu^{b_\mu}, T)\,.$$

The forgery is successful by design, and the attack works provided that (15) has a solution. □

Remark 1. CAESAR submission COLM as described in Section 3.1 is in fact the plain COLM_0 of [ABD+15]. The specification also introduces COLM_{127}, a variant which produces intermediate tags after every 127 blocks. If the scheme would generate tags after every $n = 128$ blocks, above attack could be refurbished to break authenticity of the scheme (in a similar vein as the attack in [DN14, Section 5.2]).

7 Conclusion

We remark that the attacks of Sections 4-6 do not exploit any specific properties of the part that compresses the associated data; they just "start" from the state W_0 initial to the first message block encryption. This means that the attacks also work if more advanced compression of the associated data is performed.

The nonce-respecting forgery attack of Section 6 consists of queries of length more than $(n+1)n$ blocks. In particular, the rationale behind the attack is that if a difference between two evaluations is set at some point, it requires n subsequent iterations for this difference to fade away. To make sure that the checksum at the end of the evaluation matches, n of such blocks of length $n+1$ are required. This rationale suggests two possible future directions for achieving a RUP secure variant of the COLM type structure: (i) restricting to queries of length at most n^2 blocks, and (ii) transforming the state through cryptographic primitive E_K after every n blocks.

The second direction is in fact related to the fact that COLM with intermediate tagging generates intermediate tags after every $n-1$ blocks [ABD+15]: it effectively prevents a difference to fade away right before the generation of an intermediate tag.

A Lemma 2 for 1312 Mixing

We present a simplified version of Lemma 2 specifically focused on ρ_{1312} of (3). This version particularly applies to CAESAR submission COLM [ABD+15]) which uses primitive polynomial $f(\mathtt{x}) = \mathtt{x}^{128} + \mathtt{x}^7 + \mathtt{x}^2 + \mathtt{x} + 1$.

Lemma 3. *Denote the primitive polynomial by* $f(\mathtt{x}) = \mathtt{x}^n + \mathtt{x}^{\kappa_1} + \cdots + \mathtt{x}^{\kappa_l}$ *for some even* l *and* $n > \kappa_1 > \cdots > \kappa_l = 0$.[3] *Let* N *be any nonce,* A *any associated data, and consider the following two queries to* COLM$[\rho_{1312}]$ *(ignoring tags):*

$$M_1^0 \cdots M_{n+1}^0 \leftarrow \mathcal{D}_K(N, A, C_1^0 C_2^0 \cdots C_{n+1}^0)\,,$$
$$M_1^1 \cdots M_{n+1}^1 \leftarrow \mathcal{D}_K(N, A, C_1^1 C_2^0 \cdots C_{n+1}^0)\,,$$

where $C_1^0 \neq C_1^1$ *and the* C_i^j*'s may take any value. Define*

$$I_0 := \{1\} \cup \{n+1-(\kappa_1-1), \ldots, n+1-\kappa_2\} \cup \cdots \cup \{n+1-(\kappa_{l-1}-1), \ldots, n+1-\kappa_l\}\,,$$
$$I_1 := \{1, \ldots, n+1\} \backslash I_0\,.$$

and consider the following query:

$$C_1^2 \cdots C_{n+1}^2 \leftarrow \mathcal{E}_K(N, A, M_1^{2_1} \cdots M_{n+1}^{2_{n+1}})\,,$$

where $2_i = 0$ *if* $i \in I_0$ *and* $2_i = 1$ *if* $i \in I_1$*. Then, the* $(n+1)$*th state of the second and third query satisfy* $W_{n+1}^1 = W_{n+1}^2$.

Proof. Consider Figure 1 and denote the input values to ρ_{1312} by X_i^j, the output values by

[3] Note that if l were odd, $f(\mathtt{x})$ is divisible by $\mathtt{x}+1$, whereas if $\kappa_l > 0$, $f(\mathtt{x})$ is divisible by $\mathtt{x}$. In both cases, $f(\mathtt{x})$ would not be a primitive polynomial.

Y_i, and the state values by W_i^j, where $W_0^0 = W_0^1 = W_0^2 =: W_0$ by construction. We have:

$$\begin{aligned}
W_{n+1}^2 &= X_{n+1}^{2^{n+1}} \oplus 2X_n^{2^n} \oplus \cdots \oplus 2^n X_1^{2_1} \oplus 2^{n+1} W_0 \\
&\overset{(1)}{=} \Big(Y_{n+1}^{2^{n+1}} \oplus 3Y_n^{2^{n+1}} \oplus \cdots \oplus 3Y_1^{2^{n+1}} \oplus 3W_0\Big) \\
&\oplus 2\Big(Y_n^{2^n} \oplus 3Y_{n-1}^{2^n} \oplus \cdots \oplus 3Y_1^{2^n} \oplus 3W_0\Big) \\
&\oplus \cdots \\
&\oplus 2^{n-1}\Big(Y_2^{2_2} \oplus 3Y_1^{2_2} \oplus 3W_0\Big) \\
&\oplus 2^n\Big(Y_1^{2_1} \oplus 3W_0\Big) \\
&\oplus 2^{n+1} W_0 \\
&\overset{(2)}{=} Y_{n+1}^0 \oplus \cdots \oplus Y_2^0 \oplus \Xi^0 \cdot Y_1^0 \oplus \Xi^1 \cdot Y_1^1 \oplus W_0\,,
\end{aligned}$$

where (1) holds as

$$X_i^{2_i} = Y_i^{2_i} \oplus 3Y_{i-1}^{2_i} \oplus \cdots \oplus 3Y_1^{2_i} \oplus 3W_0\,, \tag{16}$$

(2) holds as $Y_i^1 = Y_i^0$ for $i = 2, \ldots, n+1$, and where

$$\begin{aligned}
\Xi^0 &:= \bigoplus_{i \in I_0 \setminus \{1\}} 2^{n+1-i}3 \oplus 2^n\,, \\
\Xi^1 &:= \bigoplus_{i \in I_1} 2^{n+1-i}3 = \left(\bigoplus_{i=0}^{n-1} 2^i 3 \oplus 2^n\right) \oplus \Xi^0\,.
\end{aligned}$$

An identical reasoning, again relying on (16), shows that

$$W_{n+1}^1 = Y_{n+1}^0 \oplus \cdots \oplus Y_2^0 \oplus Y_1^1 \oplus W_0\,,$$

and thus that $W_{n+1}^1 \oplus W_{n+1}^2 = \Xi^0 \cdot (Y_1^0 \oplus Y_1^1)$. Because of our primitive polynomial, and as l is even, we have

$$\begin{aligned}
\Xi^0 &= 2^n \oplus \Big(2^{\kappa_1 - 1}3 \oplus \cdots \oplus 2^{\kappa_2}3\Big) \oplus \cdots \oplus \Big(2^{\kappa_{l-1}-1}3 \oplus \cdots \oplus 2^{\kappa_l}3\Big) \\
&= 2^n \oplus \Big(2^{\kappa_1} \oplus 2^{\kappa_2}\Big) \oplus \cdots \oplus \Big(2^{\kappa_{l-1}} \oplus 2^{\kappa_l}\Big) = 0\,,
\end{aligned}$$

and thus that $W_{n+1}^1 = W_{n+1}^2$. □

Acknowledgments. This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). Nilanjan Datta performed part of his work as a PhD student at Indian Statistical Institute, Kolkata. Atul Luykx is supported by a Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen). Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. The authors would like to thank the anonymous reviewers of ToSC for their comments and suggestions.

References

[ABD+15] Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennink, Mridul Nandi, Elmar Tischhauser, and Kan Yasuda. COLM v1, 2015. Submission to CAESAR competition.

[ABL+13] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and Authenticated Online Ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 424–443. Springer, 2013.

[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, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 105–125. Springer, 2014.

[ABL+15] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. AES-COPA v.2, 2015. Submission to CAESAR competition.

[BDMN16] Lilian Bossuet, Nilanjan Datta, Cuauhtemoc Mancillas-López, and Mridul Nandi. ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. *IEEE Trans. Computers*, 65(11):3318–3331, 2016.

[BDPS13] Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson, and Martijn Stam. On Symmetric Encryption with Distinguishable Decryption Failures. In Moriai [Mor14], pages 367–390.

[Ber16] Dan J. Bernstein. CAESAR use cases, 16 July 2016. CAESAR mailing list.

[BM97] Mihir Bellare and Daniele Micciancio. A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 163–192. Springer, 1997.

[BMR+13] Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen, and Elmar Tischhauser. ALE: AES-Based Lightweight Authenticated Encryption. In Moriai [Mor14], pages 447–466.

[BPS15] Guy Barwell, Daniel Page, and Martijn Stam. Rogue Decryption Failures: Reconciling AE Robustness Notions. In Jens Groth, editor, *Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings*, volume 9496 of *Lecture Notes in Computer Science*, pages 94–111. Springer, 2015.

[CAE14] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, May 2014. http://competitions.cr.yp.to/caesar.html.

[CDN16] Avik Chakraborti, Nilanjan Datta, and Mridul Nandi. INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes. In Kazue Sako, editor, *Topics in Cryptology - CT-RSA 2016 - The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, volume 9610 of *Lecture Notes in Computer Science*, pages 39–54. Springer, 2016.

[DN14] Nilanjan Datta and Mridul Nandi. ELmE: A Misuse Resistant Parallel Authenticated Encryption. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 306–321. Springer, 2014.

[DN15] Nilanjan Datta and Mridul Nandi. ELmD v2.0, 2015. Submission to CAESAR competition.

[FFL12] Ewan Fleischmann, Christian Forler, and Stefan Lucks. McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 196–215. Springer, 2012.

[FJMV03] Pierre-Alain Fouque, Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette. Authenticated On-Line Encryption. In Mitsuru Matsui and Robert J. Zuccherato, editors, *Selected Areas in Cryptography, 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 14-15, 2003, Revised Papers*, volume 3006 of *Lecture Notes in Computer Science*, pages 145–159. Springer, 2003.

[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, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 15–44. Springer, 2015.

[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 Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 493–517. Springer, 2015.

[KR11] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated-Encryption Modes. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 306–327. Springer, 2011.

[KR13] Ted Krovetz and Phillip Rogaway. The OCB Authenticated-Encryption Algorithm. http://datatracker.ietf.org/doc/draft-irtf-cfrg-ocb, June 2013.

[Mor14] Shiho Moriai, editor. *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*. Springer, 2014.

[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, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer, 2004.

[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, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001.*, pages 196–205. ACM, 2001.

[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[RS06] Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 373–390. Springer, 2006.

[TSS09] Patrick P. Tsang, Rouslan V. Solomakhin, and Sean W. Smith. Authenticated streamwise on-line encryption. Dartmouth Computer Science Technical Report TR2009-640, 2009.

[WP13] Hongjun Wu and Bart Preneel. AEGIS: A Fast Authenticated Encryption Algorithm. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 185–201. Springer, 2013.