Linking Online Misuse-Resistant Authenticated Encryption and Blockwise Attack Models

Guillaume Endignoux and Damian Vizár

EPFL, Switzerland, {guillaume.endignoux,damian.vizar}@epfl.ch

Abstract. Real-world applications of authenticated encryption often require the encryption to be computable online, e.g. to compute the i^{th} block of ciphertext after having processed the first i blocks of plaintext. A significant line of research was dedicated to identifying security notions for online authenticated encryption schemes, that capture various security goals related to real-life scenarios. Fouque, Joux, Martinet and Valette proposed definitions of privacy and integrity against adversaries that can query their oracles in a blockwise-adaptive manner, to model memory-constrained applications. A decade later, Fleischmann, Forler and Lucks proposed the notion of online nonce misuse-resistant authenticated encryption (OAE) to capture the security of online authenticated encryption under nonce-reuse.
In this work we investigate the relation between these notions. We first recast the blockwise notions of Fouque et al. to make them compatible with online authenticated encryption schemes that support headers. We then show that OAE and the conjunction of the blockwise notions are "almost" equivalent. We identify the missing property on the side of blockwise notions, and formalize it under the name PR-TAG. With PR-TAG being just an auxiliary definition, the equivalence we finally show suggests that OAE and the blockwise model for online authenticated encryption capture essentially the same notion of security.

Keywords: Symmetric-key Cryptography · Authenticated Encryption · Online Encryption · Security Notions

1 Introduction

Authenticated encryption (AE) is a symmetric-key cryptographic primitive that provides confidentiality (privacy[1]) and integrity (together with authenticity) protection of processed data. After its initial recognition and formalization [BN00, BR00, KY01], AE became a popular research target. In particular, a significant amount of effort has been invested in the research of security goals for AE, resulting in a number of security notions, e.g. the nonce-based AE with associated data (AEAD) [Rog02], notions capturing security against blockwise attacks [FJMV03, FJP04], the nonce misuse-resistant AE (MRAE) [RS06], online nonce misuse-resistant AE (OAE) [FFL12], robust AE (RAE) [HKR15], online AE (OAE2) [HRRV15], or security notions for streaming channels [FGMP15]. These notions capture security of AE in the context of diverse usage scenarios and adversarial powers. The recent CAESAR competition [Ber] has been both an evidence of the popularity of AE and a catalyst for new research activity.

Online Computable AE. A majority of existing AE schemes internally parse the plaintext into smaller, fixed-size blocks during encryption, and likewise produce the ciphertext as a sequence of such blocks. In many of these schemes (including GCM [MV04] and many of the CAESAR candidates, e.g. [ABL$^+$, IMG$^+$, BDP$^+$, KR]), the encryption algorithm additionally computes the ciphertext blocks in an *online* manner, i.e. the i^{th} block of ciphertext can be computed and written immediately after the first i blocks of plaintext were processed. We call AE schemes with this property online AE schemes.

[1] In this paper, we use the word privacy interchangeably with confidentiality.

The onlineness of encryption is necessary in constrained applications, where it is of importance to compute the ciphertext blocks with constant latency (e.g. streaming), or where a constant memory implementation is required. Online encryption algorithms are also frequent in AE schemes targeted at high performance.

Blockwise-Adaptive Attack Models. While onlineness is useful as a practical feature, it can impact security. Joux, Martinet and Valette observed that if an application, such as a smart card, outputs a ciphertext block each time it is fed a plaintext block, then a potential attacker gets more power: it can adaptively construct its queries block-by-block [JMV02]. They introduced the blockwise-adaptive adversaries and exhibited efficient blockwise-adaptive attacks on real-world schemes which were originally proven secure in models that consider the plaintexts/ciphertexts to be atomic.

A year later, Fouque, Joux, Martinet and Valette (FJMV) proposed security notions for privacy (dubbed IND-BCPA and IND-BCCA) and integrity (dubbed B-INT-CTXT) of randomized AE schemes against blockwise-adaptive adversaries [FJMV03]. Their privacy notions were defined using the left-or-right style of indistinguishability for symmetric key encryption [BDJR97]. Later on, Fouque, Joux and Poupard extended the framework of blockwise security notions for privacy to model the type of adversarial access, distinguishing between the cases where the adversary can query an infinite stream of blocks in a single message, where it can encrypt several messages sequentially, and where it can encrypt several messages concurrently [FJP04]. In the same year, Boldyreva and Taesombut proposed a relaxed version of the original IND-BCCA notion [BT04]. In 2007, Bard proposed a new framework for studying security of online encryption schemes against blockwise-adaptive attacks [Bar07]. However, this framework treated privacy of encryption-only schemes, but not integrity.

Online Authenticated Encryption. The notion of AEAD is perhaps the most popular design target for AE. The popularity stems from its simplicity: it allows one to construct simple, efficient, online AE schemes with deterministic encryption algorithms, such that they only require a unique initialization vector (a.k.a. a nonce) to be used with every encryption to be secure. Even though this simple requirement appears to be rather achievable, Rogaway and Shrimpton pointed out that if violated, it will lead to a complete break of numerous existing AEAD schemes. They proposed the MRAE notion to mitigate the impact of nonce repetition [RS06]. An MRAE scheme will only reveal unavoidable information if nonces get repeated: the complete repetition of all inputs. However, an inherent property of any MRAE scheme is that it cannot be online, as every ciphertext bit must depend on every bit of plaintext.

Fleischmann, Forler and Lucks (FFL) sought to overcome this functional limitation by proposing a security notion for schemes that are online, yet still retain some (lower) level of resistance in case of nonce-misuse [FFL12]. Their OAE notion combines the usual definition for integrity of ciphertexts with an extended version of the notion of online ciphers [BBKN12]. Another particularity of OAE is that it conflates nonce and associated data (previously separate inputs of encryption and decryption algorithms) into a single input called "header". The notion was quickly targeted by several designs [AFF+15, ABL+13]. FFL assert that the security guarantees of OAE under nonce misuse offer meaningful protection, and that these guarantees are the best possible in the given setting. Both these claims have been disputed, and especially the former has been a subject of controversy [HRRV15, AFL+], leaving a question mark over the usefulness of online encryption in presence of nonce misuse.

Deflating the Notion-Space. In this paper, we investigate the relations between the blockwise-adaptive notions for online AE by FJMV and the notion of OAE by FFL. Our motivation is twofold; first, the controversial results about nonce misuse-resistance of any online AE invite to investigate other security properties captured by OAE, and second, we believe that it is of importance to reduce the redundancy among the numerous security notions for online AE, by determining the relations between these notions.

However, a direct comparison of the notions of FFL and FJMV is not possible. The notions by FJMV are defined for randomized AE schemes with no support for headers, while the OAE notion works with deterministic AE schemes that do support headers. We therefore recast the notions of FJMV into the setting of deterministic online AE schemes and define what we believe to be their most natural extension. We then compare these restated blockwise notions (dubbed B-INT-CTXT and D-LORS-BCPA in this paper) with OAE. We first show a rather intuitive result: that OAE implies both B-INT-CTXT and D-LORS-BCPA. We then show, by means of a counterexample, that the conjunction of the latter two notions does not imply OAE. We identify the property used for the counterexample as a minor problem related to the privacy of authentication tags, and formalize the missing property in an auxiliary notion dubbed PR-TAG. We finally show the equivalence between OAE and the conjunction of B-INT-CTXT, D-LORS-BCPA and PR-TAG.

Related Work. Fouque, Joux and Poupard (FJP) show that in case of deterministic online ciphers (as defined in [BBKN12]), the blockwise-adaptive security notion and the conventional security notion are equivalent by a quadratic reduction [FJP04]. Our result resembles theirs in the complexity of the reduction, and the two results are closely related. However, their analysis deals only with (privacy of) plain online ciphers, while our work establishes relations between notions for authenticated encryption. In addition, FJP analyze the relation between standard and blockwise-adaptive versions of the same notion, while our analysis links two notions of different nature (left-or-right vs indistinguishability from a random primitive).

Our Contribution. The main result of our paper is the equivalence between OAE and the adapted version of the blockwise-adaptive AE notions of FJMV, extended with PR-TAG. Considering that PR-TAG captures a property of the authentication tag which is not related to adversarial blockwise adaptability, this equivalence points out that the security guarantees captured by the notion of OAE are essentially equivalent with those captured by the notion of FJMV.

Organization of the Paper. In Section 2, we give a few preliminary notations and results. In Section 3 we give the definition of OAE and the adapted definitions of B-INT-CTXT and D-LORS-BCPA. In Section 4 we establish the relations between the notions.

2 Preliminaries

We define the notations and recall some concepts that are referred to in the paper. Throughout the paper, we denote by $\{0,1\}^*$ the set of finite strings, including the empty string ε. For some positive integer n, we denote by $B_n = \{0,1\}^n$ the set of n-bit blocks and by $B_n^* \subset \{0,1\}^*$ the set of finite strings whose length is a multiple of n. We often call such n the *block length*. Strings from B_n^* naturally split into blocks: given $M \in B_n^*$, we denote by $M[i] \in B_n$ the i^{th} block of M (starting at index 1), and we let $M[i...j] = M[i] \| \dots \| M[j]$, where $\|$ is the concatenation operator. We let $\perp$ denote a distinguished symbol that signifies "undefined".

2.1 Online permutations

We define the following functions on B_n^*: the *block count* $\textsc{BlCount} : B_n^* \to \mathbb{N}$ as $\textsc{BlCount}(M) = p$ for all $M \in B_n^p$, the *longest common prefix* between two strings $\text{LCP}_n : B_n^* \times B_n^* \to B_n^*$ defined by $\text{LCP}_n(M_1, M_2) = M$ where $M_1 = M||M_1'$, $M_2 = M||M_2'$ and M_1' and M_2' have no common prefix (i.e. $M_1' = \varepsilon$ or $M_2' = \varepsilon$ or $M_1'[1] \neq M_2'[1]$), and the *length of the longest common prefix* $\text{LLCP}_n : B_n^* \times B_n^* \to \mathbb{N} = \textsc{BlCount} \circ \text{LCP}_n$.

Online permutations have been extensively studied in [BBKN12], we recall some relevant properties here. We denote by $\textsc{Perm}[n]$ the set of permutations of B_n. We denote by $\textsc{OPerm}[n]$ the set of online, length-preserving permutations of B_n^*, i.e. for all $\pi \in \textsc{OPerm}[n]$ we have that (*online*) for all $M_1, M_2 \in B_n^*$, the first $\text{LLCP}_n(M_1, M_2)$ blocks of $\pi(M_1)$ and $\pi(M_2)$ are identical, (*length-preserving*), for all $M \in B_n^*$, $\textsc{BlCount}(\pi(M)) = \textsc{BlCount}(M)$. We note that $\textsc{OPerm}[n]$

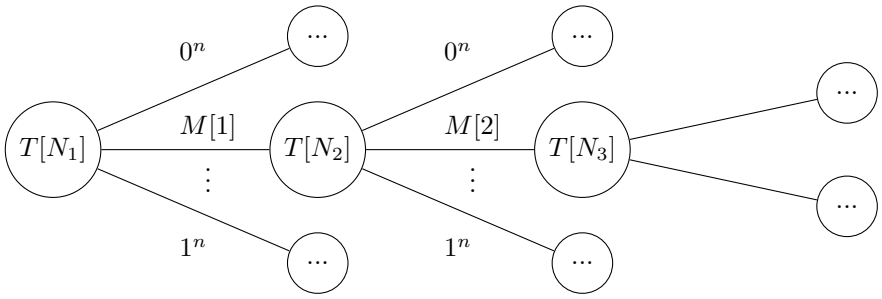

Figure 1: Tree representation of an online permutation and computation of $C = \pi_T(M)$.

is stable by the composition operation $\circ$ and that LLCP_n is stable by composition with an online permutation, i.e. $\forall \pi \in \mathrm{OPerm}[n]$, $\forall M_1, M_2 \in B_n^*$, $\mathrm{LLCP}_n(\pi(M_1), \pi(M_2)) = \mathrm{LLCP}_n(M_1, M_2)$.

Canonical tree representation. We denote by $\mathrm{Tree}[n]$ the set of infinite 2^n-ary trees, such that every tree $T \in \mathrm{Tree}[n]$ verifies the following properties: each node N of T is labeled with a permutation $T[N] \in \mathrm{Perm}[n]$, and the 2^n (outgoing) edges starting from a node N are each labeled with a distinct $x \in B_n$.

We recall that there is a bijection $T \mapsto \pi_T$ between $\mathrm{Tree}[n]$ and $\mathrm{OPerm}[n]$. Given a tree $T \in \mathrm{Tree}[n]$, its image π_T can be obtained by traversing the tree. More precisely, for any $M \in B_n^*$ we evaluate $C = \pi_T(M)$ as follows. We first set $i = 1$ and the root of T as the current node N_1, and then for each input block $M[i]$ we use the permutation $T[N_i]$ of the current node to compute $C[i] = T[N_i](M[i])$ and follow the edge labeled with $M[i]$ to move to the next node N_{i+1} (Figure 1).

Given a permutation $\pi \in \mathrm{OPerm}[n]$ and a message $M \in B_n^*$ with $l = \mathrm{BlCount}(M)$, we denote by $\pi[M] \in \mathrm{Perm}[n]$ the permutation defined by $\pi[M] : B \mapsto \pi(M||B)[l+1]$. In other words, if T is the labeled tree associated to π, then $\pi[M]$ is the label of the node reached by following the edges $M[1], ..., M[l]$ starting from the root of T. For example, on Figure 1, we identify $\pi[\varepsilon] = T[N_1]$, $\pi[M[1]] = T[N_2]$ and $\pi[M[1..2]] = T[N_3]$.

We note that while $\mathrm{OPerm}[n]$ is an infinite set, it can be sampled "uniformly" thanks to the canonical tree representation and lazy sampling. To sample a random $\pi \in \mathrm{OPerm}[n]$, we start with an unlabeled tree, and as we walk through the tree according to the incoming queries, we lazily sample the labeling permutations that are needed. With the example of Figure 1, computing $\pi_T(M[1..2])$ requires to sample $T[N_1]$ and $T[N_2]$.

2.2 Online authenticated encryption schemes

Given a *tag-length* parameter τ, we let $\mathcal{T} = B_\tau$ and call it the *tag space*. We will denote by $\mathcal{H}$ a non-empty set called the *header space*. As a practical example, $\mathcal{H}$ can be $\{0,1\}^*$ or B_h for some h. We let $\mathcal{C} = B_n^* \times \mathcal{T}$ and call it the *ciphertext space*, i.e. a ciphertext logically consists of a *ciphertext core* – that comprises encrypted blocks – and a *tag*. Hence we decompose ciphertexts with the canonical projections $\mathrm{Core} : \mathcal{C} \to B_n^*$ and $\mathrm{Tag} : \mathcal{C} \to \mathcal{T}$.

An *online authenticated encryption scheme* is a triplet $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{K}$ is a a finite *key space*, $\mathcal{E} : \mathcal{K} \times \mathcal{H} \times B_n^* \to \mathcal{C}$ is a deterministic encryption algorithm, and $\mathcal{D} : \mathcal{K} \times \mathcal{H} \times \mathcal{C} \to B_n^* \cup \{\perp\}$ is a deterministic decryption algorithm. $\mathcal{T}$ is the tag space of Π, $\mathcal{H}$ is its header space and n is its block size. We require that Π is *correct*, i.e. for all $K \in \mathcal{K}$, $H \in \mathcal{H}$ and $M \in B_n^*$, we have $\mathcal{D}(K, H, \mathcal{E}(K, H, M)) = M$. We further require that the encryption is *online*, i.e. for all $K \in \mathcal{K}$ and $H \in \mathcal{H}$, $\mathrm{Core} \circ \mathcal{E}(K, H, \cdot) \in \mathrm{OPerm}[n]$, or informally that the i-th block of the ciphertext core only depends on the first i blocks of the plaintext.

2.3 Security Definitions

We formalize security with help of code-based games proposed by [BR04]. A game G_Π for a scheme Π consists of an **Initialize** procedure, procedures that model oracle queries and a **Finalize** procedure. All these procedures are defined in terms of the scheme Π.

When we say that an adversary $\mathscr{A}$ plays the game G_Π, we mean the sequential execution of: first the **Initialize** procedure, then the algorithm of the adversary using the oracle procedures defined by G_Π, and last the **Finalize** procedure using as input the final output of the adversary. The result returned by the **Finalize** procedure is called the output of this execution. For some games, we do not specify the **Finalize** procedure: in that case it is the trivial procedure that forwards the output of the adversary. For an adversary $\mathscr{A}$, we denote by $\Pr[\mathscr{A}^{G_\Pi} \Rightarrow x]$ the probability that when $\mathscr{A}$ plays the game G instantiated with the scheme Π, the output of the **Finalize** procedure is x.

Two games G and G' are said to be identical until bad if they both contain a statement $\boxed{\mathsf{bad} \leftarrow \text{true};}$ such that their code is identical until this statement is executed. We recall the fundamental lemma of game playing.

Lemma 1 (Fundamental lemma of game playing [BR04])**.** *Let G and G' be two games identical until bad. Then for any adversary $\mathscr{A}$ and any output x:*

$$\Pr[\mathscr{A}^{G_\Pi} \Rightarrow x] - \Pr[\mathscr{A}^{G'_\Pi} \Rightarrow x] \leq \Pr[\mathscr{A}^{G_\Pi} \textit{ sets } \mathsf{bad}]$$

Randomized algorithms We denote by $x \xleftarrow{\$} S$ the sampling of an element x from a set S with uniform distribution. We note that we assume the use of lazy sampling when the set S is "large" (e.g. $\textsc{Perm}[n]$) or infinite endowed with a natural definition of uniform distribution (e.g. $\textsc{OPerm}[n]$), and for statements of the form **for** $a \in A$ **do** $x_a \xleftarrow{\$} S$ when A is a "large" set. All such samplings in a single algorithm are always independent.

Resource-parametrized adversarial advantage For each security property $\textsc{Prop}$, we define the advantage of an adversary $\mathscr{A}$ in attacking $\textsc{Prop}$ of a scheme Π. This is a real number that we denote by $\mathbf{Adv}^{\textsc{Prop}}_\Pi(\mathscr{A})$. To capture the security of a scheme Π for the notion $\textsc{Prop}$, we define the maximum advantage that can be achieved by any adversary $\mathscr{A}$ that is only limited in its resources. These resources are always: t, the time complexity of $\mathscr{A}$; q, the number of multi-block messages queried by $\mathscr{A}$; b, the total number of blocks queried by $\mathscr{A}$; μ, the maximum number of blocks in a message queried by $\mathscr{A}$. An adversary that uses at most these resources is called a (t, q, b, μ)-adversary . We denote by $\mathbf{Adv}^{\textsc{Prop}}_\Pi(t, q, b, \mu)$ the maximum of $\mathbf{Adv}^{\textsc{Prop}}_\Pi(\mathscr{A})$ over (t, q, b, μ)-adversaries $\mathscr{A}$. We further say that a scheme Π is $(t, q, b, \mu; \varepsilon)$-secure for $\textsc{Prop}$ if $\mathbf{Adv}^{\textsc{Prop}}_\Pi(t, q, b, \mu) \leq \varepsilon$.

3 Existing security notions and their variants

In this section, we present the existing security notions investigated in this paper, namely the recent notion of misuse-resistant online authenticated encryption [FFL12], and several notions of blockwise privacy and integrity, that were proposed a decade earlier [FJMV03, FJP04]. We adapt the latter definitions to the syntax of online authenticated encryption schemes as proposed in [FFL12].

3.1 Misuse-resistant online authenticated encryption

The notion of (nonce) misuse-resistant online authenticated encryption was given by Fleischmann et al. [FFL12]. Hoang et al. pointed out that the original definition was incomplete and reformulated it [HRRV15]. We retain the latter version of the notion. Roughly speaking, a scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is OAE secure if the outputs of $\mathcal{E}$ resemble core ciphertexts computed by a random online permutation

Game OAE-REAL$_\Pi$	Game OAE-IDEAL$_\Pi$
proc Initialize $K \xleftarrow{\$} \mathcal{K}$ **proc Enc**(H, M) **return** $\mathcal{E}(K, H, M)$ **proc Dec**(H, C) **return** $\mathcal{D}(K, H, C)$	**proc Initialize** **for** $H \in \mathcal{H}$ **do** $\pi_H \xleftarrow{\$} \text{OPERM}[n]$ **for** $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$ **proc Enc**(H, M) **return** $(\pi_H(M), T_{H,M})$ **proc Dec**(H, C) **return** $\perp$

Figure 2: Games OAE-REAL$_\Pi$ (left) and OAE-IDEAL$_\Pi$ (right) used to define OAE.

sampled independently for each header, followed by random tags sampled independently for each header-message pair, and if it is simultaneously hard to guess inputs to $\mathcal{D}$ that decrypt correctly. This is formalized in Definition 1.

Definition 1 (OAE [FFL12])**.** Consider the games OAE-REAL and OAE-IDEAL defined in Figure 2. For an online authenticated encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, and an adversary $\mathscr{A}$ that never queries the **Dec** oracle with a result of a previous **Enc** query, we define the OAE advantage of $\mathscr{A}$ against Π as:

$$\mathbf{Adv}^{\text{OAE}}_{\Pi}(\mathscr{A}) = \Pr[\mathscr{A}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \Pr[\mathscr{A}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1].$$

3.2 Blockwise integrity of ciphertexts

FJMV proposed a notion of integrity in the context of a blockwise chosen plaintext attack [FJMV03]. Compared to the classical integrity of ciphertexts notion [BN00, KY01], the adversary is given a *blockwise* encryption oracle along with a standard decryption oracle, and wins if it can produce an existential forgery.

In its original form, the notion of FJMV is defined for randomized schemes that do not support headers. We therefore recast the integrity notion of FJMV to make it compatible with deterministic online AE schemes that take a header along with the message to encrypt (or decrypt). We give in Definition 2 what we believe to be the natural extension of the original notion of FJMV.

Definition 2 (B-INT-CTXT)**.** Consider the game B-INT-CTXT defined in Figure 3. For an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, we define the B-INT-CTXT advantage of an adversary $\mathscr{A}$ against Π as:

$$\mathbf{Adv}^{\text{B-INT-CTXT}}_{\Pi}(\mathscr{A}) = \Pr[\mathscr{A}^{\text{B-INT-CTXT}_\Pi} \Rightarrow 1].$$

The **Enc** and the **GetTag** queries together form a complete blockwise encryption oracle. The current adversarial plaintext is encrypted and accumulated block-by-block in the variable $\widetilde{M}$ through **Enc** queries, while a **GetTag** query returns the tag for the current (possibly empty) plaintext. The first if-statement in a **Dec** query makes sure that the adversarial forgery attempt is valid.

3.3 Blockwise privacy

FJMV proposed a notion of indistinguishability of ciphertetxts in the context of a blockwise chosen plaintext attack [FJMV03]. The adversary was given more adaptive power: it was allowed to get the encryption of each block before requesting the encryption of the next block. The definition of FMJV uses the left-or-right style of indistinguishability, common for early notions of

Game B-INT-CTXT$_\Pi$

proc Initialize
  $\mathsf{win} \leftarrow 0$
  $K \xleftarrow{\$} \mathcal{K}$
  $\mathcal{X} \leftarrow \emptyset$
  $\widetilde{H} \leftarrow \perp$
  $\widetilde{M} \leftarrow \varepsilon$
  $j \leftarrow 0$
proc Enc(H, P) ▷$P \in B_n$
  if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
  $\widetilde{M} \leftarrow \widetilde{M} || P$
  $C \leftarrow \textsc{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$
  $j \leftarrow j + 1$
  return $C[j]$

proc GetTag(H)
  if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
  $C \leftarrow \mathcal{E}(K, \widetilde{H}, \widetilde{M})$
  $\mathcal{X} \leftarrow \mathcal{X} \cup \{(\widetilde{H}, C)\}$
  $\widetilde{H} \leftarrow \perp$
  $\widetilde{M} \leftarrow \varepsilon$
  $j \leftarrow 0$
  return $\textsc{Tag}(C)$
proc Dec(H, C)
  $M \leftarrow \mathcal{D}(K, H, C)$
  if $(H, C) \in \mathcal{X}$ **then** $M \leftarrow \perp$
  if $M \neq \perp$ **then** $\mathsf{win} \leftarrow 1$
  return M
proc Finalize()
  return win

Figure 3: Game B-INT-CTXT$_\Pi$ used to define blockwise integrity of ciphertexts.

privacy [BDJR97, BN00]. The definition did not, however, explicitly state whether it allowed the adversary to query an infinite stream of blocks only, or if starting new blockwise queries was allowed. Later, Fouque, Joux and Poupard described several versions of the blockwise indistinguishability notion, that allowed for both infinite streams of blocks and multiple queries, further distinguishing between sequential and concurrent execution of multiple queries [FMP03, FJP04]. We focus on the version that allows to make multiple queries in a sequential manner that we call LORS-BCPA (as in [FJP04]).

Recasting LORS-BCPA As before, we attempt to recast the original definition for randomized encryption algorithms to make it compatible with deterministic online authenticated encryption schemes that take a header alongside a plaintext as input. This proves to be a non-trivial task because of the left-or-right flavour of the indistinguishability. Allowing the adversary to issue encryption queries with no restrictions would allow it to trivially break any (not just online) deterministic AE scheme using two queries with the same header and repeating a message only on the left side. Fixing the header turns the underlying cipher in a permutation, so two ciphertexts are equal if and only if the corresponding plaintexts are equal. Figure 4 shows an example of such an attacker $\mathscr{A}_r$, where $0_\mathcal{H}$ is an arbitrary element of the header space $\mathcal{H}$.

Such attacks can be thwarted by forbidding the adversary to repeat headers in its queries. However, imposing the non-repetition of headers seems to be an unnecessarily limiting constraint, that prevents more than just the unavoidable trivial attacks. In case of deterministic online AE schemes, it is the online property itself that allows trivial attacks to be mounted. An example of a subtler attack that leverages the online property is described in Figure 4; adversary $\mathscr{A}'_r$ only repeats the first block on the left side, and leverages the online property of the scheme.

We propose to restrict the LORS-BCPA notion to a class of adversaries specified in Definition 3 whose queries verify certain conditions that avoid trivial attacks, but can for example repeat headers. We will call adversaries that respect these conditions *online-respecting* adversaries.

Definition 3 (Online-respecting adversary)**.** Consider an adversary $\mathscr{A}$ that plays the LORS-BCPA game and queries a sequence of multi-block messages $((H_i, M_{0,i}, M_{1,i}))_i \in (\mathcal{H} \times B_n^* \times B_n^*)^*$ to the **LR** oracle. We say that $\mathscr{A}$ is *online-respecting* if for all pairs of indices (i, j) such that $H_i = H_j$, we have $\mathrm{LLCP}_n(M_{0,i}, M_{0,j}) = \mathrm{LLCP}_n(M_{1,i}, M_{1,j})$.

In other words, if two left messages requested with the same header share a common prefix of l blocks, then the associated right messages must also share a common prefix of exactly l blocks,

Adversary $\mathscr{A}_r$	Adversary $\mathscr{A}'_r$
for $i \in \{0, ..., 2\}$ **do** $M_i \xleftarrow{\$} B_n$ ▷ such that M_i are distinct	**for** $i \in \{0, ..., 6\}$ **do** $M_i \xleftarrow{\$} B_n$ ▷ such that M_i are distinct
$C_a \leftarrow \mathbf{LR}(0_{\mathcal{H}}, M_0, M_1)$	$C_a \leftarrow \mathbf{LR}(0_{\mathcal{H}}, M_0 \| M_1, M_2 \| M_3)$
$C_b \leftarrow \mathbf{LR}(0_{\mathcal{H}}, M_0, M_2)$	$C_b \leftarrow \mathbf{LR}(0_{\mathcal{H}}, M_0 \| M_4, M_5 \| M_6)$
output $C_a \neq C_b$	**output** $C_a[0] \neq C_b[0]$

Figure 4: Header-repeating adversaries against *blockwise left-or-right* notions.

and conversely. The *online-respecting* property can be rephrased using online permutations, as in Proposition 1.

Proposition 1. *Consider an adversary $\mathscr{A}$ that plays the* LORS-BCPA *game and queries a sequence of multi-block messages $((H_i, M_{0,i}, M_{1,i}))_i \in (\mathcal{H} \times B_n^* \times B_n^*)^*$ to the **LR** oracle. Then $\mathscr{A}$ is* online-respecting *if and only if for every header $H \in \mathcal{H}$ there exists an online-permutation $\sigma_H \in \mathrm{OPERM}[n]$ such that for every query (indexed by i) we have $M_{1,i} = \sigma_{H_i}(M_{0,i})$.*

Proof. If the queries respect this condition, the adversary is *online-respecting* because for indices (i, j) such that $H_i = H_j = H$, the length of common prefixes verify the equality $\mathrm{LLCP}_n(M_{1,i}, M_{1,j}) = \mathrm{LLCP}_n(\sigma_H(M_{0,i}), \sigma_H(M_{0,j})) = \mathrm{LLCP}_n(M_{0,i}, M_{0,j})$.

Conversely, if the adversary is *online-respecting*, let's show that suitable online-permutations σ_H exist. For each header $H \in \mathcal{H}$ and each message $M \in B_n^*$, we identify constraints that the permutation $\sigma_H[M]$ must satisfy. Let $l = \mathrm{BLCOUNT}(M)$ and $S_{H,M}$ be the set of queries i such that $H_i = H$ and M is a strict prefix of $M_{0,i}$. Then by the *online-respecting* property, for all $i, j \in S_{H,M}$, $M_{0,i}[l+1] = M_{0,j}[l+1] \Leftrightarrow M_{1,i}[l+1] = M_{1,j}[l+1]$, because $M_{0,i}[1..l] = M_{0,j}[1..l] = M$. This implies that there exists a bijection (i.e. a permutation) $\sigma_H[M]$ such that for all $i \in S_{H,M}$, $M_{1,i}[l+1] = \sigma_H[M](M_{0,i}[l+1])$. With such construction of the nodes $\sigma_H[M]$, the online permutations σ_H verify $M_{1,i} = \sigma_{H_i}(M_{0,i})$. □

We finally define the D-LORS-BCPA (a.k.a. deterministic-LORS-BCPA) notion for deterministic online AE schemes that considers online-respecting adversaries in Definition 4.

Definition 4 (D-LORS-BCPA)**.** Consider the game LORS-BCPA defined in Figure 5. For an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, we define the D-LORS-BCPA advantage of an online-respecting adversary $\mathscr{A}$ against Π as:

$$\mathbf{Adv}_{\Pi}^{\text{D-LORS-BCPA}}(\mathscr{A}) = 2 \cdot \Pr[\mathscr{A}^{\text{LORS-BCPA}_{\Pi}} \Rightarrow 1] - 1.$$

Intuitively, the LORS-BCPA security game preserves the left-or-right character of the original notions by FJMV and an adversary can construct queries adaptively, block-by-block. The D-LORS-BCPA notion then additionally requires the adversary to be *online-respecting*, which is necessary to prevent trivial victories against deterministic schemes.

Remark 1. FJMV have shown that blockwise security notions are stronger than non-blockwise ones in the case of randomized encryption [FJP04]. However, they noted that in the case of deterministic schemes with online-respecting adversaries, a blockwise encryption oracle can be straightforwardly simulated using an atomic encryption oracle by keeping a variable like $\widetilde{M}$ in Figure 5. This reduction is, however, not tight but quadratic, as it grows the number of adaptively queried blocks m to $\sum_{i=1}^{m} = \frac{m(m+1)}{2}$ non-adaptively queried blocks. Hence, studying blockwise security notions is still relevant to obtain tighter relations.

Game LORS-BCPA$_\Pi$

proc Initialize
$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$\widetilde{H} \leftarrow \perp$
$\widetilde{M} \leftarrow \varepsilon$
$j \leftarrow 0$
proc LR(H, P_0, P_1) $\triangleright P_0, P_1 \in B_n$
if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
$\widetilde{M} \leftarrow \widetilde{M} || P_b$
$C \leftarrow \textsc{Core}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$
$j \leftarrow j + 1$
return $C[j]$

proc GetTag(H)
if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
$T \leftarrow \textsc{Tag}(\mathcal{E}(K, \widetilde{H}, \widetilde{M}))$
$\widetilde{H} \leftarrow \perp$
$\widetilde{M} \leftarrow \varepsilon$
$j \leftarrow 0$
return T
proc Finalize(β)
return $\beta = b$

Figure 5: Game LORS-BCPA$_\Pi$ used to define blockwise privacy.

4 Relations between blockwise notions and OAE

In this section, we first prove that OAE security implies D-LORS-BCPA and B-INT-CTXT security, up to a quadratic increase in resources. We then show that the converse is not true, and propose a new auxiliary notion called PR-TAG. Finally, we show that there is an equivalence between OAE security and the conjunction of D-LORS-BCPA, B-INT-CTXT and PR-TAG security.

4.1 Separating OAE and Blockwise Notions

OAE → D-LORS-BCPA

Theorem 1. *Let* Π *be an online authenticated encryption scheme. Then*

$$\boldsymbol{Adv}_\Pi^{\text{D-LORS-BCPA}}(t, q, b, \mu) \leq 2 \cdot \boldsymbol{Adv}_\Pi^{\text{OAE}}(t', q', b', \mu)$$

where $t' = t + c \cdot q', q' = q + b, b' = b + \min\left(q \cdot \frac{\mu(\mu+1)}{2}, \frac{b(b+1)}{2}\right)$ *for a positive constant* c.

Proof. Let $\mathscr{A}_1$ be an online-respecting (t, q, b, μ)-D-LORS-BCPA adversary against scheme Π. We construct adversary $\mathscr{B}_1$ as shown on Figure 6. The number of messages queried by $\mathscr{B}_1$ is at most q', because at most b messages are queried via **LR**, and at most q messages are queried via **GetTag**. The time complexity of $\mathscr{B}_1$ is $t' = t + c \cdot q'$ because a constant time is spent for each query of $\mathscr{B}_1$. The number of blocks queried by $\mathscr{B}_1$ is at most b' because at most b blocks are queried via **GetTag** and for each message query, at most $\sum_{i=1}^{\mu} i$ blocks are queried via **LR**, and in total at most $\sum_{i=1}^{b} i$ blocks are queried via **LR**. The maximum number of blocks in a single query remains unchanged. We then have the following relations between the advantages of $\mathscr{A}_1$ and $\mathscr{B}_1$.

$$\begin{aligned}
\mathbf{Adv}_\Pi^{\text{OAE}}(\mathscr{B}_1) &= \Pr[{\mathscr{B}_1}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \Pr[{\mathscr{B}_1}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] \\
&= \Pr[{\mathscr{B}_1}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \frac{1}{2} \\
&= \Pr[{\mathscr{A}_1}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1] - \frac{1}{2} \\
&= \frac{1}{2}\mathbf{Adv}_\Pi^{\text{D-LORS-BCPA}}(\mathscr{A}_1)
\end{aligned}$$

The first equality comes from the fact that if $\mathscr{B}_1$ interacts with the OAE-IDEAL game, the distribution of the replies of $\mathscr{A}_1$'s **LR** oracle is independent from b. Indeed, $\mathscr{A}_1$ is online-respecting

Adversary $\mathscr{B}_1$

$b \xleftarrow{\$} \{0,1\}$
$\widetilde{H} \leftarrow \perp$
$\widetilde{M} \leftarrow \varepsilon$
$j \leftarrow 0$
Run $\mathscr{A}_1$
On query $\mathbf{LR}(H, P_0, P_1)$ of $\mathscr{A}_1$
  if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
  $\widetilde{M} \leftarrow \widetilde{M} || P_b$
  $C \leftarrow \textsc{Core}(\mathbf{Enc}(\widetilde{H}, \widetilde{M}))$
  $j \leftarrow j + 1$
  return $C[j]$ **to** $\mathscr{A}_1$

On query $\mathbf{GetTag}(H)$ of $\mathscr{A}_1$
  if $\widetilde{H} = \perp$ **then** $\widetilde{H} \leftarrow H$
  $T \leftarrow \textsc{Tag}(\mathbf{Enc}(\widetilde{H}, \widetilde{M}))$
  $\widetilde{H} \leftarrow \perp$
  $\widetilde{M} \leftarrow \varepsilon$
  $j \leftarrow 0$
  return T **to** $\mathscr{A}_1$
On $\mathbf{Finalize}(\beta)$ of $\mathscr{A}_1$
  output $\beta = b$

Figure 6: Adversary $\mathscr{B}_1$ for the proof of Theorem 1.

so by Proposition 1, the left and right queries are identical up to online-permutations σ_H, and by Lemma 5, the distribution of the replies is independent from b.

The second equality comes from the construction of adversary $\mathscr{B}_1$, that perfectly simulates the LORS-BCPA game when the underlying oracle is the OAE-REAL game. □

OAE → B-INT-CTXT

Theorem 2. *Let* Π *be an online authenticated encryption scheme. Then*

$$\boldsymbol{Adv}^{\text{B-INT-CTXT}}_{\Pi}(t, q, b, \mu) \leq \boldsymbol{Adv}^{\text{OAE}}_{\Pi}(t', q', b', \mu)$$

where $t' = t + c \cdot q', q' = q + b, b' = b + \min\left(q \cdot \frac{\mu(\mu+1)}{2}, \frac{b(b+1)}{2}\right)$ *for a positive constant* c.

Proof. Let $\mathscr{A}_2$ be a (t, q, b, μ)-B-INT-CTXT adversary against scheme Π. We construct adversary $\mathscr{B}_2$ as shown on Figure 7. The number of messages queried by $\mathscr{B}_2$ is at most q', because at most b messages are queried via **Enc**, and at most q messages are queried via **GetTag** and **Dec**. The time complexity of $\mathscr{B}_2$ is $t' = t + c \cdot q'$ because a constant time is spent for each query of $\mathscr{B}_2$. The number of blocks queried by $\mathscr{B}_2$ is at most b' because at most b blocks are queried via **GetTag** and **Dec** and for each message query, at most $\sum_{i=1}^{\mu} i$ blocks are queried via **Enc**, and in total at most $\sum_{i=1}^{b} i$ blocks are queried via **Enc**. The maximum number of blocks in a single query remains unchanged. We then have the following relations between the advantages of $\mathscr{A}_2$ and $\mathscr{B}_2$.

$$\begin{aligned}
\mathbf{Adv}^{\text{OAE}}_{\Pi}(\mathscr{B}_2) &= \Pr[{\mathscr{B}_2}^{\text{OAE-REAL}_{\Pi}} \Rightarrow 1] - \Pr[{\mathscr{B}_2}^{\text{OAE-IDEAL}_{\Pi}} \Rightarrow 1] \\
&= \Pr[{\mathscr{A}_2}^{\text{B-INT-CTXT}_{\Pi}} \Rightarrow 1] - 0 \\
&= \mathbf{Adv}^{\text{B-INT-CTXT}}_{\Pi}(\mathscr{A}_2)
\end{aligned}$$

In the case of the OAE-IDEAL game, the adversary $\mathscr{B}_2$ always outputs 0. In the case of the OAE-REAL game, adversary $\mathscr{B}_2$ outputs 1 if and only if adversary $\mathscr{A}_2$ forges a valid ciphertext-tag pair. □

D-LORS-BCPA + B-INT-CTXT ↛ OAE

Proposition 2. *If there exists an online authenticated encryption scheme* Π *which is* D-LORS-BCPA *and* B-INT-CTXT *secure, then there exists a scheme* Π' *which is* D-LORS-BCPA *and* B-INT-CTXT *secure but not* OAE *secure.*

Adversary $\mathscr{B}_2$

$\mathsf{found} \leftarrow 0$
$\mathcal{X} \leftarrow \emptyset$
$\widetilde{H} \leftarrow \bot$
$\widetilde{M} \leftarrow \varepsilon$
$j \leftarrow 0$
Run $\mathscr{A}_2$
On query $\mathbf{Enc}(H, P)$ of $\mathscr{A}_2$
  if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$
  $\widetilde{M} \leftarrow \widetilde{M} || P$
  $C \leftarrow \textsc{Core}(\mathbf{Enc}(\widetilde{H}, \widetilde{M}))$
  $j \leftarrow j + 1$
  return $C[j]$ **to** $\mathscr{A}_2$
On query $\mathbf{GetTag}(H)$ of $\mathscr{A}_2$
  if $\widetilde{H} = \bot$ **then** $\widetilde{H} \leftarrow H$
  $C \leftarrow \mathbf{Enc}(\widetilde{H}, \widetilde{M})$
  $\mathcal{X} \leftarrow \mathcal{X} \cup \{(\widetilde{H}, C)\}$
  $\widetilde{H} \leftarrow \bot$
  $\widetilde{M} \leftarrow \varepsilon$
  $j \leftarrow 0$
  return $\textsc{Tag}(C)$ **to** $\mathscr{A}_2$
On query $\mathbf{Dec}(H, C)$ of $\mathscr{A}_2$
  $M \leftarrow \mathbf{Dec}(H, C)$
  if $(H, C) \in \mathcal{X}$ **then** $M \leftarrow \bot$
  if $M \neq \bot$ **then** $\mathsf{found} \leftarrow 1$
  return M **to** $\mathscr{A}_2$
On **Finalize**() of $\mathscr{A}_2$
  output found

Figure 7: Adversary $\mathscr{B}_2$ for the proof of Theorem 2.

Algorithm $\mathcal{E}'(K, H, M)$

$C \leftarrow \mathcal{E}(K, H, M)$
$T' \leftarrow \textsc{Tag}(C) || 1$
return $(\textsc{Core}(C), T')$

Algorithm $\mathcal{D}'(K, H, C)$

$T || b \leftarrow \textsc{Tag}(C)$
if $b \neq 1$ **then return** $\bot$
$C' \leftarrow (\textsc{Core}(C), T)$
return $\mathcal{D}(K, H, C')$

Adversary $\mathscr{A}_3$

$M \xleftarrow{\$} B_n$
$T || \beta \leftarrow \textsc{Tag}(\mathbf{Enc}(H, M))$
output β

Figure 8: Definitions of Π' (left and middle) and adversary $\mathscr{A}_3$ (right) for the proof of Proposition 2.

Proof. Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a D-LORS-BCPA and B-INT-CTXT secure scheme, with *tag-length* τ. We will construct a scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ with *tag-length* $\tau + 1$ that is D-LORS-BCPA and B-INT-CTXT secure, but not OAE secure.

The idea is to append a constant bit to the tag, so that it is easily distinguishable from a random string (Figure 8). Clearly, appending this constant bit does not change the D-LORS-BCPA nor B-INT-CTXT advantages. However, adversary $\mathscr{A}_3$ (Figure 8) can obtain a constant advantage over OAE by making a single query. The OAE advantage of adversary $\mathscr{A}_3$ is equal to $\frac{1}{2}$ since β is always equal to 1 in the OAE-REAL game, and is uniformly distributed in the OAE-IDEAL game, so $\mathbf{Adv}^{\mathrm{OAE}}_{\Pi'}(\mathscr{A}_3) = \Pr[\mathscr{A}_3{}^{\text{OAE-REAL}_{\Pi'}} \Rightarrow 1] - \Pr[\mathscr{A}_3{}^{\text{OAE-IDEAL}_{\Pi'}} \Rightarrow 1] = 1 - \frac{1}{2} = \frac{1}{2}$. □

4.2 Towards an equivalence result

As shown in Proposition 2, D-LORS-BCPA security and B-INT-CTXT security combined are not sufficient to provide OAE security. As suggested by the proof of Proposition 2, this comes from the fact that the tag does not have to be uniformly distributed to provide D-LORS-BCPA and B-INT-CTXT. We define a new auxiliary notion called PR-TAG that captures the pseudo-randomness of the tag in a chosen plaintext attack, and we show an equivalence result with OAE.

Pseudo-random tag We introduce the PR-TAG (pseudo-random tag) notion a.k.a. indistinguishability from a random tag. More precisely, an adversary wins the PR-TAG game if it can distinguish real ciphertexts from pairs composed of the real core ciphertext and a random tag. This is captured in Definition 5.

Game PR-TAG-REAL$_\Pi$	Game PR-TAG-IDEAL$_\Pi$
proc Initialize $K \xleftarrow{\$} \mathcal{K}$ **proc Enc**(H, M) **return** $\mathcal{E}(K, H, M)$	**proc Initialize** $K \xleftarrow{\$} \mathcal{K}$ **for** $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$ **proc Enc**(H, M) $C \leftarrow \textsc{Core}(\mathcal{E}(K, H, M))$ **return** $(C, T_{H,M})$

Figure 9: Games PR-TAG-REAL$_\Pi$ (left) and PR-TAG-IDEAL$_\Pi$ (right) used to define PR-TAG.

Adversary $\mathscr{B}_4$	On query **Enc**(H, M) of $\mathscr{A}_4$
for $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$ Run $\mathscr{A}_4$	$C \leftarrow \textsc{Core}(\textbf{Enc}(H, M))$ **return** $(C, T_{H,M})$ **to** $\mathscr{A}_4$ On **Finalize**(β) of $\mathscr{A}_4$ **output** $1 - \beta$

Figure 10: Adversary $\mathscr{B}_4$ for the proof of Theorem 3.

Definition 5 (PR-TAG)**.** Consider the games PR-TAG-REAL and PR-TAG-IDEAL defined in Figure 9. For an online authenticated encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, we define the PR-TAG advantage of an adversary $\mathscr{A}$ against Π as:

$$\mathbf{Adv}_\Pi^{\text{PR-TAG}}(\mathscr{A}) = \Pr[\mathscr{A}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1] - \Pr[\mathscr{A}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1]$$

OAE → PR-TAG We first prove that OAE security implies PR-TAG security, up to twice the advantage.

Theorem 3. *Let Π be an online authenticated encryption scheme. Then*

$$\boldsymbol{Adv}_\Pi^{\text{PR-TAG}}(t, q, b, \mu) \leq 2 \cdot \boldsymbol{Adv}_\Pi^{\text{OAE}}(t', q, b, \mu)$$

where $t' = t + c \cdot q$ for a positive constant c.

Proof. Let $\mathscr{A}_4$ be a (t, q, b, μ)-PR-TAG adversary against a scheme Π. We note that since all the oracles available to PR-TAG adversaries are contained in the OAE-REAL and OAE-IDEAL games, we can also view $\mathscr{A}_4$ as an OAE adversary. We insert the OAE-IDEAL game in the expression of the PR-TAG advantage of $\mathscr{A}_4$ and we will bound each half of this new expression:

$$\begin{aligned}
\mathbf{Adv}_\Pi^{\text{PR-TAG}}(\mathscr{A}_4) &= \Pr[{\mathscr{A}_4}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1] - \Pr[{\mathscr{A}_4}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1] \\
&= \Pr[{\mathscr{A}_4}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1] - \Pr[{\mathscr{A}_4}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] \\
&\quad + \Pr[{\mathscr{A}_4}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] - \Pr[{\mathscr{A}_4}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1].
\end{aligned}$$

First, we note that by construction, the game OAE-REAL perfectly simulates the game PR-TAG-REAL for adversaries that only use the **Enc** oracle, such as adversary $\mathscr{A}_4$, which means that $\Pr[{\mathscr{A}_4}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1] = \Pr[{\mathscr{A}_4}^{\text{OAE-REAL}_\Pi} \Rightarrow 1]$ and we obtain

$$\Pr[{\mathscr{A}_4}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1] - \Pr[{\mathscr{A}_4}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] \leq \mathbf{Adv}_\Pi^{\text{OAE}}(t', q, b, \mu).$$

Second, given the PR-TAG adversary $\mathscr{A}_4$, we construct the OAE adversary $\mathscr{B}_4$ as shown on Figure 10. The time complexity of $\mathscr{B}_4$ is $t' = t + c \cdot q$ because a constant time is spent for each query of $\mathscr{A}_4$. The number of message queries and the number of block queries remain unchanged.

By construction, adversary $\mathscr{B}_4$ perfectly simulates game PR-TAG-IDEAL when the underlying game is OAE-REAL. Note that the output bit of adversary $\mathscr{A}_4$ is flipped by adversary $\mathscr{B}_4$, i.e. $\Pr[\mathscr{A}_4{}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1] = 1 - \Pr[\mathscr{B}_4{}^{\text{OAE-REAL}_\Pi} \Rightarrow 1]$.

When the underlying game is OAE-IDEAL, adversary $\mathscr{B}_4$ gives answers to $\mathscr{A}_4$ that are identically distributed to the OAE-IDEAL game, because $\mathscr{B}_4$ redundantly replaces a random tag that was independent from the random core by another independent random tag, and thus $\Pr[\mathscr{A}_4{}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] = 1 - \Pr[\mathscr{B}_4{}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1]$. It follows that

$$\Pr[\mathscr{A}_4{}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] - \Pr[\mathscr{A}_4{}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1] \leq \mathbf{Adv}^{\text{OAE}}_\Pi(t', q, b, \mu).$$

□

D-LORS-BCPA + B-INT-CTXT + PR-TAG → OAE

Theorem 4. *Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an online authenticated encryption scheme. Then*

$$\begin{aligned}\boldsymbol{Adv}^{\text{OAE}}_\Pi(t, q, b, \mu) \leq\ & \boldsymbol{Adv}^{\text{B-INT-CTXT}}_\Pi(t_c, q_c, b_c, \mu_c) + \boldsymbol{Adv}^{\text{PR-TAG}}_\Pi(t_t, q_t, b_t, \mu_t) \\ & + \boldsymbol{Adv}^{\text{D-LORS-BCPA}}_\Pi(t_p, q_p, b_p, \mu_p)\end{aligned}$$

where $t_c = t + c_c \cdot (q + b)$, $q_c = q$, $b_c = b$, $\mu_c = \mu$; $t_t = t + c_t \cdot q$, $q_t = q$, $b_t = b$, $\mu_t = \mu$; $t_p = t + c_p \cdot (q + b)$, $q_p = q$, $b_p = b$, $\mu_p = \mu$ for positive constants c_c, c_t, c_p.

Proof. Let $\mathscr{A}$ be a (t, q, b, μ)-OAE adversary against scheme Π. We define games G_i for $i \in \{0, ..., 4\}$ on Figure 11, Figure 13 and Figure 14. We have, by Lemma 2, Lemma 3 and Lemma 4 proven below that:

$$\begin{aligned}&\Pr[\mathscr{A}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \Pr[\mathscr{A}^{G_{2\Pi}} \Rightarrow 1] \leq \mathbf{Adv}^{\text{B-INT-CTXT}}_\Pi(t_c, q_c, b_c, \mu_c), \\ &\Pr[\mathscr{A}^{G_{2\Pi}} \Rightarrow 1] - \Pr[\mathscr{A}^{G_{3\Pi}} \Rightarrow 1] \leq \mathbf{Adv}^{\text{PR-TAG}}_\Pi(t_t, q_t, b_t, \mu_t), \\ &\Pr[\mathscr{A}^{G_{3\Pi}} \Rightarrow 1] - \Pr[\mathscr{A}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] \leq \mathbf{Adv}^{\text{D-LORS-BCPA}}_\Pi(t_p, q_p, b_p, \mu_p),\end{aligned}$$

which gives us $\mathbf{Adv}^{\text{OAE}}_\Pi(\mathscr{A}) \leq \mathbf{Adv}^{\text{B-INT-CTXT}}_\Pi(t_c, q_c, b_c, \mu_c) + \mathbf{Adv}^{\text{PR-TAG}}_\Pi(t_t, q_t, b_t, \mu_t) + \mathbf{Adv}^{\text{D-LORS-BCPA}}_\Pi(t_p, q_p, b_p, \mu_p)$.

□

Lemma 2. *Let $\mathscr{A}$ be a (t, q, b, μ)-OAE adversary. Let G_0, G_1 and G_2 be the games defined in Figure 11. We have*

$$\Pr[\mathscr{A}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \Pr[\mathscr{A}^{G_{2\Pi}} \Rightarrow 1] \leq \boldsymbol{Adv}^{\text{B-INT-CTXT}}_\Pi(t', q, b, \mu)$$

where $t' = t + c_c \cdot (q + b)$.

Adversary $\mathscr{A}_c$

Run $\mathscr{A}$
On query $\mathbf{Enc}(H, M)$ of $\mathscr{A}$
  $l \leftarrow \textsc{BlCount}(M)$
  $M[1]||...||M[l] \leftarrow M$
  for $j \in \{1, ..., l\}$ **do**
    $C[j] \leftarrow \mathbf{Enc}(H, M[j])$
  $T \leftarrow \mathbf{GetTag}(H)$
  return (C, T) **to** $\mathscr{A}$
On query $\mathbf{Dec}(H, C)$ of $\mathscr{A}$
  return $\mathbf{Dec}(H, C)$ **to** $\mathscr{A}$
On $\mathbf{Finalize}(\beta)$ of $\mathscr{A}$
  output $\emptyset$

Figure 12: Adversary $\mathscr{A}_c$ for the proof of Lemma 2.

Games G_0 and $\boxed{G_1}$

proc Initialize
  $K \xleftarrow{\$} \mathcal{K}$
  $\mathcal{X} \leftarrow \emptyset$
proc Enc(H, M)
  $C \leftarrow \mathcal{E}(K, H, M)$
  $\mathcal{X} \leftarrow \mathcal{X} \cup \{(H, C)\}$
  return C
proc Dec(H, C)
  $M \leftarrow \mathcal{D}(K, H, C)$
  if $(H, C) \in \mathcal{X}$ **then** $M \leftarrow \perp$
  if $M \neq \perp$ **then** $\mathsf{bad} \leftarrow$ true; $\boxed{M \leftarrow \perp}$
  return M

Game G_2

proc Initialize
  $K \xleftarrow{\$} \mathcal{K}$
proc Enc(H, M)
  return $\mathcal{E}(K, H, M)$
proc Dec(H, C)
  return $\perp$

Figure 11: Games G_0, G_1 (left) and G_2 (right) for the reduction of B-INT-CTXT. The boxed statement is present in game G_1 only.

Proof. Let $\mathscr{A}_c$ be the adversary defined from $\mathscr{A}$ on Figure 12. The time complexity of $\mathscr{A}_c$ is $t' = t + c_c \cdot (q + b)$ because a constant time is spent for each block queried by $\mathscr{A}$ to call **Enc**, as well as for each query of $\mathscr{A}$ to call **GetTag** and **Dec**. The number of message queries and the number of block queries remain unchanged.

By definition, we recall that $\mathscr{A}$ never queries to the **Dec** oracle the result of a previous **Enc** query. We then have:

$$\begin{aligned}\Pr[\mathscr{A}^{\text{OAE-REAL}_\Pi} \Rightarrow 1] &= \Pr[\mathscr{A}^{G_{0\Pi}} \Rightarrow 1] \\ &= \Pr[\mathscr{A}^{G_{1\Pi}} \Rightarrow 1] + (\Pr[\mathscr{A}^{G_{0\Pi}} \Rightarrow 1] - \Pr[\mathscr{A}^{G_{1\Pi}} \Rightarrow 1]) \\ &\leq \Pr[\mathscr{A}^{G_{1\Pi}} \Rightarrow 1] + \Pr[\mathscr{A}^{G_{0\Pi}} \text{ sets } \mathsf{bad}]\end{aligned}$$

where the last inequality comes from Lemma 1. Then, we note that $\Pr[A^{G_{1\Pi}} \Rightarrow 1] = \Pr[A^{G_{2\Pi}} \Rightarrow 1]$ because the **Dec** oracle of G_1 always returns $\perp$. We have $\Pr[A^{G_{0\Pi}} \text{ sets } \mathsf{bad}] \leq \mathbf{Adv}_\Pi^{\text{B-INT-CTXT}}(A_c)$ because game G_0 sets bad whenever a ciphertext forgery is found by adversary $\mathscr{A}$, and consequently by adversary $\mathscr{A}_c$. These inequalities prove that $\Pr[A^{\text{OAE-REAL}_\Pi} \Rightarrow 1] - \Pr[A^{G_{2\Pi}} \Rightarrow 1] \leq \mathbf{Adv}_\Pi^{\text{B-INT-CTXT}}(t', q, b, \mu)$. □

Lemma 3. *Let $\mathscr{A}$ be a (t, q, b, μ)-OAE adversary. Let G_3 be the game defined in Figure 13. We have:*

$$\Pr[\mathscr{A}^{G_{2\Pi}} \Rightarrow 1] - \Pr[\mathscr{A}^{G_{3\Pi}} \Rightarrow 1] \leq \boldsymbol{Adv}_\Pi^{\text{PR-TAG}}(t', q, b, \mu)$$

where $t' = t + c_t \cdot q$.

Game G_3

proc Initialize
  $K \xleftarrow{\$} \mathcal{K}$
  for $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$
proc Enc(H, M)
  $C \leftarrow \textsc{Core}(\mathcal{E}(K, H, M))$
  return $(C, T_{H,M})$
proc Dec(H, C)
  return $\perp$

Adversary $\mathscr{A}_t$

Run $\mathscr{A}$
On query **Enc**(H, M) of $\mathscr{A}$
  return Enc(H, M) **to** $\mathscr{A}$
On query **Dec**(H, C) of $\mathscr{A}$
  return $\perp$ **to** $\mathscr{A}$
On **Finalize**(β) of $\mathscr{A}$
  output β

Figure 13: Game G_3 (left) and adversary $\mathscr{A}_t$ (right) for the proof of Lemma 3.

Game G_4

proc Initialize
  $K \xleftarrow{\$} \mathcal{K}$
  for $H \in \mathcal{H}$ **do** $\sigma_H \xleftarrow{\$} \textsc{OPerm}[n]$
  for $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$
proc Enc(H, M)
  $C \leftarrow \textsc{Core}(\mathcal{E}(K, H, \sigma_H(M)))$
  return $(C, T_{H,M})$
proc Dec(H, C)
  return $\perp$

Adversary $\mathscr{A}_p$

for $H \in \mathcal{H}$ **do** $\sigma_H \xleftarrow{\$} \textsc{OPerm}[n]$
for $(H, M) \in \mathcal{H} \times B_n^*$ **do** $T_{H,M} \xleftarrow{\$} \mathcal{T}$
Run $\mathscr{A}$
On query **Enc**(H, M) of $\mathscr{A}$
  $l \leftarrow \textsc{BlCount}(M)$
  $M[1]||...||M[l] \leftarrow M$
  $R[1]||...||R[l] \leftarrow \sigma_H(M)$
  for $j \in \{1, ..., l\}$ **do**
    $C[j] \leftarrow$ **LR**$(H, R[j], M[j])$
  $T \leftarrow$ **GetTag**(H)
  return $(C, T_{H,M})$ **to** A
On query **Dec**(H, C) of $\mathscr{A}$
  return $\perp$ **to** A
On **Finalize**(β) of $\mathscr{A}$
  output β

Figure 14: Game G_4 (left) and adversary $\mathscr{A}_p$ (right) for the proof of Lemma 4.

Proof. Let $\mathscr{A}_t$ be the adversary defined from $\mathscr{A}$ on Figure 13. The time complexity of $\mathscr{A}_t$ is $t' = t + c_t \cdot q$ because a constant time is spent for each query of $\mathscr{A}$. The number of messages queried by $\mathscr{A}_t$ is at most q, the number of blocks queried by $\mathscr{A}_t$ is at most b and the maximum number of blocks in a query of $\mathscr{A}_t$ is at most μ.

We have the following perfect simulations of the PR-TAG games: $\Pr[A^{G_{2\Pi}} \Rightarrow 1] = \Pr[{A_t}^{\text{PR-TAG-REAL}_\Pi} \Rightarrow 1]$ and $\Pr[A^{G_{3\Pi}} \Rightarrow 1] = \Pr[{A_t}^{\text{PR-TAG-IDEAL}_\Pi} \Rightarrow 1]$. From this, and from Definition 5 it follows that $\Pr[A^{G_{2\Pi}} \Rightarrow 1] - \Pr[A^{G_{3\Pi}} \Rightarrow 1] \leq \mathbf{Adv}_\Pi^{\text{PR-TAG}}(A_t) \leq \mathbf{Adv}_\Pi^{\text{PR-TAG}}(t', q, b, \mu)$. □

Lemma 4. *Let $\mathscr{A}$ be a (t, q, b, μ)-*OAE *adversary. We have:*

$$\Pr[\mathscr{A}^{G_{3\Pi}} \Rightarrow 1] - \Pr[\mathscr{A}^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] \leq \boldsymbol{Adv}_\Pi^{\text{D-LORS-BCPA}}(t', q, b, \mu)$$

where $t' = t + c_p \cdot (q + b)$.

Proof. Let $\mathscr{A}_p$ be the adversary defined from $\mathscr{A}$ on Figure 14. The time complexity of $\mathscr{A}_p$ is $t' = t + c_p \cdot (q + b)$ because a constant time is spent for each block queried by $\mathscr{A}$ to call **LR**, as

well as for each query of $\mathscr{A}$ to call **GetTag** or upon **Dec**. The number of messages queried by $\mathscr{A}_p$ is at most q, the number of blocks queried by $\mathscr{A}_p$ is at most b and the maximum number of blocks in a query of $\mathscr{A}_p$ is at most μ.

By Proposition 1, $\mathscr{A}_p$ is online-respecting. Let G_4 be the game defined on Figure 14. If we denote by b the bit chosen by the LORS-BCPA game played by $\mathscr{A}_p$, we have the following perfect simulations. If $b = 1$, then the **LR** oracle always encrypts the message M provided to the **Enc** oracle by adversary $\mathscr{A}$, so game G_3 is simulated. If $b = 0$, then the **LR** oracle always encrypts $\sigma_H(M)$ for the header H and the message M provided to the **Enc** oracle by adversary $\mathscr{A}$, so game G_4 is simulated and we get $\Pr[A^{G_{3\Pi}} \Rightarrow 1] = \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 1]$ and $\Pr[A^{G_{4\Pi}} \Rightarrow 1] = \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 0 | b = 0]$. Since $\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2}$, we have:

$$\begin{aligned}\Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1] = \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 1] \cdot \frac{1}{2} \\ + \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 0] \cdot \frac{1}{2}\end{aligned}$$

from which we can conclude that:

$$\begin{aligned}\mathbf{Adv}^{\text{D-LORS-BCPA}}_\Pi(A_p) &= 2 \cdot \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1] - 1 \\ &= \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 1] \\ &\quad + \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 0] - 1 \\ &= \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 1 | b = 1] - \Pr[{A_p}^{\text{LORS-BCPA}_\Pi} \Rightarrow 0 | b = 0] \\ &= \Pr[A^{G_{3\Pi}} \Rightarrow 1] - \Pr[A^{G_{4\Pi}} \Rightarrow 1]\end{aligned}$$

Recall that for a fixed $K \in \mathcal{K}$ and $H \in \mathcal{H}$, the core encryption algorithm is an online permutation, i.e. $\rho_{K,H} := \textsc{Core}(\mathcal{E}(K, H, \cdot)) \in \textsc{OPerm}[n]$ (see Subsection 2.2). In game G_4, we sample a random $\sigma_H \in \textsc{OPerm}[n]$ and compute $C = \rho_{K,H} \circ \sigma_H(M)$, whereas in game OAE-IDEAL we sample a random $\pi_H \in \textsc{OPerm}[n]$ and compute $C = \pi_H(M)$. By Lemma 5 of Appendix A, these two games produce identical distributions and have equivalent complexity, which shows that $\Pr[A^{G_{4\Pi}} \Rightarrow 1] = \Pr[A^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1]$. It follows that
$\Pr[A^{G_{3\Pi}} \Rightarrow 1] - \Pr[A^{\text{OAE-IDEAL}_\Pi} \Rightarrow 1] = \mathbf{Adv}^{\text{D-LORS-BCPA}}_\Pi(A_p) \leq \mathbf{Adv}^{\text{D-LORS-BCPA}}_\Pi(t', q, b, \mu)$. □

4.3 On the minimality of PR-TAG

In the proof of Lemma 4, we did not make full use of the **GetTag** oracle. Indeed, adversary $\mathscr{A}_p$ only queries this oracle to start a new sequential query, but discards the value of the tag. For this reason, a weaker privacy notion than D-LORS-BCPA, one that completely ignores the authentication tag, would be sufficient to prove the equivalence with OAE: we can replace the **GetTag** oracle in the LORS-BCPA game of Figure 5 by a **Reset** oracle that starts a new query but does not output the tag. Such a weakening of privacy of core ciphertexts is possible, because privacy of tags is already captured by the PR-TAG notion. This raises a question: can the PR-TAG notion be weakened without breaking the equivalence result, or is it only possible to weaken the privacy of the ciphertext core, but PR-TAG cannot be unchanged? Determining the overlap of the PR-TAG property with both B-INT-CTXT and D-LORS-BCPA remains an interesting open question.

This also highlights an interesting observation: to show equivalence with OAE, we need to capture the randomness of the authentication tag with an indistinguishable-from-random type of notion, whereas a left-or-right type of notion is sufficient for the core ciphertext. This stems from the fact that, by definition, the core of an online AE scheme has to be an online permutation for a fixed key and header (otherwise encryption or decryption cannot be computed in an online manner). This, together with the result shown in Appendix A, facilitates the equivalence between games OAE-REAL and G_4 used in the proof of Lemma 4.

5 Conclusion

We have shown that, if projected to the setting of deterministic online AE schemes with headers, the blockwise-adaptive security notions of FJMV are equivalent to the notion of OAE *in the essentials*. We have identified the PR-TAG property, as a missing component that is necessary for the equivalence to be properly proven, and we have observed that this property is not related to the blockwise-adaptiveness of the adversary. We leave the establishment of the exact relations of PR-TAG to the remaining blockwise notions as an open question.

Acknowledgments.

Damian Vizár is supported in part by Microsoft Research under MRL Contract No. 2014-006 (DP1061305). We would like to thank the anonymous reviewers for their constructive comments. We would also like to thank Reza Reyhanitabar for initial discussion leading to this work.

References

[ABL+] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda, Nilanjan Datta, and Mridul Nandi. AES-COPA. https://competitions.cr.yp.to/round2/aescopav2.pdf.

[ABL+13] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and authenticated online ciphers. In *Advances in Cryptology - ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 424–443. Springer, 2013.

[AFF+15] Farzaneh Abed, Scott R. Fluhrer, Christian Forler, Eik List, Stefan Lucks, David A. McGrew, and Jakob Wenzel. Pipelineable on-line encryption. In *Fast Software Encryption, FSE 2014*, volume 8540 of *LNCS*, pages 205–223. Springer, 2015.

[AFL+] Farzanah Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. Don't panic! the cryptographer's guide to robust (on-line) encryption. https://www.uni-weimar.de/fileadmin/user/fak/medien/professuren/Mediensicherheit/Research/Drafts/nonce-misuse-oae.pdf.

[Bar07] Gregory V. Bard. Blockwise-adaptive chosen-plaintext attack and online modes of encryption. In *Cryptography and Coding, 11th IMA International Conference, Cirencester, UK*, volume 4887 of *LNCS*, pages 129–151. Springer, 2007.

[BBKN12] Mihir Bellare, Alexandra Boldyreva, Lars R. Knudsen, and Chanathip Namprempre. On-line ciphers and the hash-cbc constructions. *J. Cryptology*, 25(4):640–679, 2012.

[BDJR97] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *Symposium on Foundations of Computer Science, FOCS '97*, pages 394–403, 1997.

[BDP+] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Keyak. https://competitions.cr.yp.to/round2/keyakv2.pdf.

[Ber] D. J. Bernstein. Cryptographic competitions: CAESAR. http://competitions.cr.yp.to.

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology - ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545, 2000.

[BR00] Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In *Advances in Cryptology - ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 317–330. Springer, 2000.

[BR04] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. *IACR Cryptology ePrint Archive*, 2004:331, 2004.

[BT04] Alexandra Boldyreva and Nut Taesombut. Online encryption schemes: New security notions and constructions. In *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 1–14. Springer, 2004.

[FFL12] Ewan Fleischmann, Christian Forler, and Stefan Lucks. Mcoe: A family of almost foolproof on-line authenticated encryption schemes. In *Fast Software Encryption, FSE 2012*, volume 7549 of *LNCS*, pages 196–215, 2012.

[FGMP15] Marc Fischlin, Felix Günther, Giorgia Azzurra Marson, and Kenneth G. Paterson. Data is a stream: Security of stream-based channels. In *Advances in Cryptology - CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 545–564. Springer, 2015.

[FJMV03] Pierre-Alain Fouque, Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette. Authenticated on-line encryption. In *Selected Areas in Cryptography, SAC 2003*, volume 3006 of *LNCS*, pages 145–159, 2003.

[FJP04] Pierre-Alain Fouque, Antoine Joux, and Guillaume Poupard. Blockwise adversarial model for on-line ciphers and symmetric encryption schemes. In *Selected Areas in Cryptography, SAC 2004*, volume 3357 of *LNCS*, pages 212–226, 2004.

[FMP03] Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard. Practical symmetric on-line encryption. In *Fast Software Encryption, FSE 2003*, volume 2887 of *LNCS*, pages 362–375, 2003.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In *Advances in Cryptology - EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, 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 *Advances in Cryptology - CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 493–517. Springer, 2015.

[IMG+] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. CLOC and SILC. https://competitions.cr.yp.to/round2/silcv2.pdf.

[JMV02] Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette. Blockwise-adaptive attackers: Revisiting the (in)security of some provably secure encryption models: Cbc, gem, IACBC. In *Advances in Cryptology - CRYPTO*, volume 2442 of *LNCS*, pages 17–30, 2002.

[KR] Ted Krovetz and Phillip Rogaway. OCB. https://competitions.cr.yp.to/round1/ocbv1.pdf.

[KY01] Jonathan Katz and Moti Yung. Unforgeable encryption and chosen ciphertext secure modes of operation. In *Fast Software Encryption, FSE 2000*, volume 1978 of *LNCS*, pages 284–299. Springer, 2001.

[MV04] David A. McGrew and John Viega. The security and performance of the galois/counter mode (GCM) of operation. In *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 343–355. Springer, 2004.

[Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In *Conference on Computer and Communications, CCS 2002*, pages 98–107. ACM, 2002.

[RS06] Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, 2006.

A Composition of a random online permutation and a fixed online permutation

Lemma 5. *Let ρ be a random permutation sampled from* $\textsc{OPerm}[n]$ *with any distribution. Let σ be a random permutation independent from ρ and uniformly distributed in* $\textsc{OPerm}[n]$ *in the sense of Subsection 2.1. Then the composition $\pi := \rho \circ \sigma$ is uniformly distributed in* $\textsc{OPerm}[n]$*. Besides, the algorithmic complexity to evaluate lazily $\rho \circ \sigma$ is the same as a lazy evaluation of the equivalent random permutation π uniformly distributed in* $\textsc{OPerm}[n]$*, up to a constant factor.*

Proof. Let's consider the tree representations of these online permutations as described in Subsection 2.1. Let T be the tree associated to the online permutation $\rho \circ \sigma$. Each node of T is labeled with a permutation $(\rho \circ \sigma)[M]$, where $M \in B_n^*$ is the input message that leads to this node when one traverses T from the root.

Given $M \in B_n^*$, let $N := \sigma(M)$ and $P := \rho \circ \sigma(M)$. For all $M' \in B_n$, let $N', P' \in B_n$ be defined by $N||N' := \sigma(M||M')$ and $P||P' := \rho \circ \sigma(M||M') = \rho(N||N')$. Then we have by definition:

$$\begin{aligned} N' &= \sigma[M](M') \\ P' &= \rho[N](N') \\ P' &= (\rho \circ \sigma)[M](M') \end{aligned}$$

This implies that:

$$(\rho \circ \sigma)[M] = \rho[N] \circ \sigma[M] = \rho[\sigma(M)] \circ \sigma[M]$$

Consequently, we first have that for all M in B_n^*, $(\rho \circ \sigma)[M]$ is uniformly distributed in $\textsc{Perm}[n]$. Indeed, $\sigma[M]$ is uniformly distributed in $\textsc{Perm}[n]$ and independent from $\sigma(M)$, and ρ is independent from σ, so $\rho[\sigma(M)] \circ \sigma[M]$ is uniformly distributed in $\textsc{Perm}[n]$.

Second, the family $((\rho \circ \sigma)[M])_{M \in B_n^*}$ is a family of independent random permutations. Indeed, each node of $\rho \circ \sigma$ is labeled with a distinct message M, and for each message M the permutations $\rho[\sigma(M)]$ and $\sigma[M]$ are only used to compute $(\rho \circ \sigma)[M]$ – i.e. they are not used to compute any other $(\rho \circ \sigma)[M']$ for $M' \neq M$. Since the family $(\sigma[M])_{M \in B_n^*}$ is a family of independent random permutations, the composed family $(\rho[\sigma(M)] \circ \sigma[M])_{M \in B_n^*}$ is also a family of independent random permutations.

Last, if we let $\pi = \rho \circ \sigma$, the evaluation of π by lazy sampling of π and the evaluation of $\rho \circ \sigma$ by lazy sampling of ρ and σ have the same complexity, up to a constant factor. Indeed, for any message $M \in B_n^*$, if we let $l := \textsc{BlCount}(M)$, to evaluate $\pi(M)$ we need to sample the permutations $\pi[\varepsilon], ..., \pi[M[1...l-1]] \in \textsc{Perm}[n]$. To evaluate $(\rho \circ \sigma)(M)$, we need to know the permutations $(\rho \circ \sigma)[\varepsilon], ..., (\rho \circ \sigma)[M[1...l-1]]$, and for this we need to sample exactly $\sigma[\varepsilon], ..., \sigma[M[1...l-1]]$, as well as $\rho[\sigma(\varepsilon)], ..., \rho[\sigma(M[1...l-1])]$. In other words, to evaluate $\rho \circ \sigma$ on a sequence of messages, we need to explore in the tree of σ the same paths that we explore in the tree of π to evaluate π on those messages, and we need to explore in the tree of ρ the permutation by σ of these paths. This ensures that the complexity of a lazy sampling is the same in both cases, up to a constant factor. □