Reconsidering Generic Composition: the Tag-then-Encrypt case

Francesco Berti, Olivier Pereira, Thomas Peters

ICTEAM/ELEN/Crypto Group
Université catholique de Louvain
B-1348 Louvain-la-Neuve, Belgium
emails: {francesco.berti,thomas.peters,olivier.pereira}@uclouvain.be

Abstract. Authenticated Encryption (AE) achieves confidentiality and authenticity, the two most fundamental goals of cryptography, in a single scheme. A common strategy to obtain AE is to combine a Message Authentication Code (MAC) and an encryption scheme, either nonce-based or *iv*-based. Out of the 180 possible combinations, Namprempre et al. [25] proved that 12 were secure, 164 insecure and 4 were left unresolved: A10, A11 and A12 which use an *iv*-based encryption scheme and N4 which uses a nonce-based one. The question of the security of these composition modes is particularly intriguing as N4, A11, and A12 are more efficient than the 12 composition modes that are known to be provably secure.
We prove that: (*i*) N4 is not secure in general, (*ii*) A10, A11 and A12 have equivalent security, (*iii*) A10, A11, A12 and N4 are secure if the underlying encryption scheme is either misuse-resistant or "message malleable", a property that is satisfied by many classical encryption modes, (*iv*) A10, A11 and A12 are insecure if the underlying encryption scheme is stateful or untidy. All the results are quantitative.

1 Introduction

Authenticated encryption and generic composition. From its start, the goal of cryptography is to prevent that anyone but the intended receiver can read a message (privacy) and that anyone can send a message impersonating someone else (authenticity). In order to answer this privacy (resp. authenticity) requirement, encryption schemes (resp. Message Authentication Codes (MACs)) were designed independently. When there is a need for both privacy and authenticity, Authenticated Encryption (AE) can be used [7,16,18,6]. Moreover, AE may be used to authenticate associated data (AD), which are data attached to a message which do not need to be private, but do need to be authenticated (e.g., message header [32]). We suppose that both the sender and the receiver share the same private key (symmetric scenario).
There are two possible ways to create an AE scheme: the first is to design it from scratch, using a single key, and the second is to combine an Encryption scheme with a MAC. Examples of the first path are AES-GCM [12], AES-CCM [21], CHACHA20_POLY305 [26] (used in TLS 1.3 [14]), SCT [30] and the

CAESAR candidates [8]. When following the second path, the problem is to decide how to compose the ingredients. This problem is called *generic composition* and was introduced and studied first by Bellare and Namprempre [6]. They and Krawczyk proved the well-known result that *Encrypt-then*-MAC is secure [7,18]. Namprempre et al. have made a deeper analysis [25], which considered in detail the assumptions on the Encryption scheme, whether it is iv-based (ivE [with the iv randomly picked]) or nonce-based (nE [with the nonce n never repeated]) and assumed that the MACs are PRFs. Out of all the possible composition modes, 12 (9 with ivE, 3 with nE) were proved to be secure, 164 to be insecure and 4 were unresolved: N4 which uses a nE and A10, A11, A12 which use an ivE. These four modes, which are depicted in Fig. 1, are based on the Tag-then-Encrypt paradigm: given a nonce n, an associated data a and a message m, the resulting AEs simply output $c = \mathsf{Enc}^{n}_{k_E}(m\|\tau)$ or $c = \mathsf{Enc}^{iv}_{k_E}(m\|\tau)$ for some n/iv, where τ is the tag provided by the MAC, and is computed either as $\mathsf{Mac}_{k_M}(a, m)$ or as $\mathsf{Mac}_{k_M}(m)$ depending on the mode. When an ivE scheme is used, the iv is computed using a PRF MAC that takes as input either n or (n, a). Interestingly three of these modes (N4, A11 and A12) use the n, a and m only once in total during both the computation of iv ($\mathsf{Mac}^{\mathsf{IV}}_{k_M}$) and τ ($\mathsf{Mac}^{\mathsf{Tag}}_{k_M}$), which makes them the most efficient among all Tag-then-Encrypt schemes. In this paper, we investigate the security of these four composition modes, focusing on ciphertext integrity, as Namprempre et al. already established the expected confidentiality guarantees.

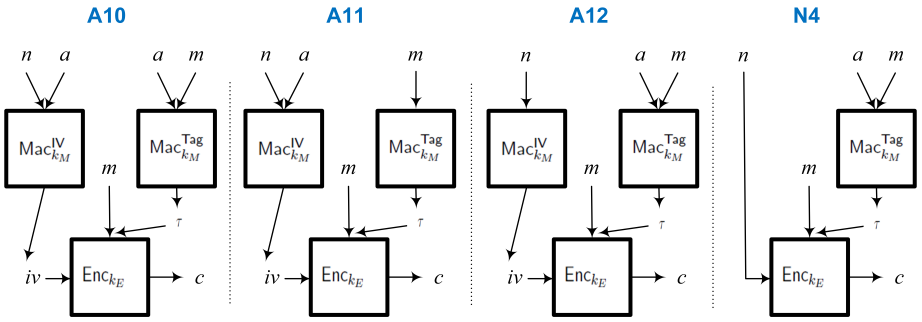

Fig. 1. The four modes A10, A11, A12, and N4.

Our contribution Our investigation gives several new results.

First, the mode N4 does not guarantee ciphertext integrity in general, and we offer a counterexample. The idea of this counterexample is to carefully inject a kind of Trojanin the nE encryption scheme, which can only be activated during the decryption queries using well-crafted ciphertext. The Trojan is triggered through the nonce and a block of the message.

Second, we show that A10, A11 and A12 have equivalent security, by offering security reductions between these three modes. Different techniques are used in

these reductions, which are based on the uniqueness of the nonce and, in other cases, recrafting these nonces.

Third, we push our analysis further, by investigating the security of these 3 modes by making some additional hypothesis on the ivE scheme. We found that these modes are secure if the ivE scheme is either misuse-resistant (that is, repeated nonces can only lead to repeated ciphertexts without further security degradation) or "message-malleable" (that is, given a triple (iv, m, c) with $c = \mathsf{Enc}^{iv}(m)$, it is possible to compute correctly every other triple (iv, m', c') with $c' = \mathsf{Enc}^{iv}(m')$ [resp. $m' = \mathsf{Dec}^{iv}(c')$] for the same iv from m' [resp. c']). Many common schemes, like CTR and OFB [15], CHACHA20 [26] or any other stream ciphers, are "message-malleable", thus we have proved that the three composition modes are secure if implemented with these encryption schemes. This is another evidence of the "*generic composition's sensitivity to definitional and algorithmic adjustments*" [25]. While the proof for misuse-resistant ivE-schemes is relatively straightforward, the proof for "message-malleable" ivE is more interesting as it uses a reduction of a INT-CTXT (ciphertext integrity) adversary to a CPA (Chosen Plaintext Attack) adversary and not only to the properties of the MAC schemes. Interestingly, the N4 mode also becomes secure when the same extra requirements are made for the nE encryption scheme. With respect to the Namprempre et al. [25], we have still to use an additional hypothesis (they used Knowledge of Tag [KoT]), but ours are much easier to prove although they are less general.

Fourth, we find two insecure variants for all three modes, one if the ivE encryption scheme is not tidy, the other if it is stateful. Although Namprempre et al. [25] already used tidiness in security proofs, our ivE scheme correctly encrypts the tag and it decrypts in the "natural" way. Thus, our analysis supports the idea that tidiness is also a security property (already present in Namprempre et al. [25] and in Paterson et al. [28], with respect to CRD). Concerning the attack using a secure stateful scheme (AE stateful schemes were defined by Bellare et al. [4] and their security redefined by Rogaway and Zhang [36]), the idea is to use the state in order to emulate the trojan approach that was used in our attack against mode N4. Namprempre et al. considered only stateless schemes, but it is interesting to see how the security of a mode may depend on the fact of being stateful or stateless. Moreover, stateful AE schemes are an interesting subject of studies [28,5,17,11].

Structure of the paper We give a section introducing all the notions we need (Sec. 2); after that we present the four modes N4, A10, A11 and A12 which we investigate (Sec. 3). Then, we show the proof that mode N4 is not secure (Sec. 4) and the security relations among modes A10, A11 and A12 (Sec. 5). After that, we prove that these modes are secure if we add some hypothesis on the ivE scheme (Sec. 6) and we end analyzing our insecure variants of modes A10, A11, and A12 (Sec. 7).

2 Background

2.1 Notations

We use finite binary strings. The length of the string x is denoted by $|x|$ and the concatenation of the strings x and y is denoted by $x\|y$. The set of all finite strings is denoted by $\{0,1\}^*$. We denote the set of all n-bit strings as $\{0,1\}^n$ and the set of strings of at most n bits as $\{0,1\}^{\leq n}$. Given a string $x = (x_1, x_2, ..., x_l)$ of l bits, we denote with $\pi_t(x)$ the string $(x_1, ..., x_T)$ where $T = min(|x|, t)$.
We reserve calligraphic notation for sets. In particular we denote with $\mathcal{K}, \mathcal{N}$, $\mathcal{IV}$, $\mathcal{A}$, $\mathcal{M}$, $\mathcal{TW}$, $\mathcal{T}$, $\mathcal{X}$ and $\mathcal{C}$ respectively the *key space, nonce space, iv-space, associated data space, message space, tweak space, tag space, input space of the* MAC and the *ciphertext space*. We suppose that $\mathcal{M} = \mathcal{A} = \{0,1\}^*$, that is, these spaces contain all the finite binary strings. We suppose that $\mathcal{C} \subseteq \{0,1\}^*$.
Given the set $\mathcal{Y}$, we write $y \leftarrow \mathcal{Y}$ to denote the uniformly random selection of y in $\mathcal{Y}$.
We reserve sans serif (Alg) notations for algorithms. If the algorithm Alg is probabilistic, we can think of its output as a distribution. We denote with $a \leftarrow \mathsf{Alg}(b, c, d)$ the fact that we sample from the distribution induced by algorithm Alg on inputs (b, c, d), and we obtain a. We may write part of the arguments of the algorithm as subscripts or superscripts, that is, $\mathsf{Alg}_b^c(d) = \mathsf{Alg}_b(c, d) = \mathsf{Alg}(b, c, d)$.
A (q, t)-adversary A is a probabilistic algorithm which can make at most q queries to the oracle(s) he is granted access to, and runs in time bounded by t.
Let algorithm Alg be an algorithm whose inputs are in $\mathcal{S}^1 \times \cdots \times \mathcal{S}^n$ and whose output is in $\mathcal{Y}$. We say that algorithm Alg *does not reveal, via the length of its output, any information about its inputs apart from their lengths* if there exists a deterministic function $f : \mathbb{N}^n \longmapsto \mathbb{N}$ s.t. $|y| = f(|s_1|, ..., |s_n|)$ for all possible inputs $(s_1, ..., s_n)$. We assume that all the Enc and AEnc algorithms we use have this property.
Given a game, where the adversary A is allowed to query many oracles, we use a single counter for all the queries made by adversary A, during the game. The oracle $\perp(\cdot, \cdot)$ always answers $\perp$. When an adversary is playing a game where he has access either to an oracle implemented with algorithm $\mathsf{Alg}(\cdot, \cdot)$ or the oracle $\$(\cdot, \cdot)$ it means that the oracle $\$(\cdot, \cdot)$ answers a random bit string of length $|\mathsf{Alg}(\cdot, \cdot)|$.
We write $\Pr[B; A_1, A_2, ...]$ for the probability of event B after the experiment described by steps $A_1, A_2, ...$.

2.2 Pseudorandom functions (PRF)

We now define the PRF-security notion, the base of many cryptographic primitives:

Definition 1. *A function* $\mathsf{F} : \mathcal{K} \times \mathcal{M} \longmapsto \mathcal{T}$ *is a* (q, t, ϵ)-pseudorandom function (PRF) *if for every* (q, t) *adversary* A*, the advantage :*

$$\mathsf{Adv}_{\mathsf{F}}^{PRF}(\mathsf{A}) := |\Pr[\,\mathsf{A}^{\mathsf{F}_k(\cdot)} \Rightarrow 1\,] - \Pr[\,\mathsf{A}^{\mathsf{f}(\cdot)} \Rightarrow 1\,]|$$

is upper bounded by ϵ where k and f are chosen uniformly at random from their domains, namely $\mathcal{K}$ and the set of functions from $\mathcal{M}$ to $\mathcal{T}$, $\mathcal{FUNC}(\mathcal{M},\mathcal{T})$.
In a similar way, F is a pseudorandom permutation *(PRP) if F_k is a permutation and the above advantage is ϵ bounded when f is selected as a random permutation.*

We remind that a PRP is a PRF (see Proposition 3.27 [15]).

In some of our constructions, we will also use tweakable pseudorandom functions [20]. They are PRFs with an additional input, the tweak: $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \mathcal{M} \longmapsto \mathcal{T}$, and their security advantage is then defined as $\mathsf{Adv}^{\mathrm{TPRF}}_{\mathsf{E}}(\mathsf{A}) := \mathsf{Adv}^{\mathrm{PRF}}_{\mathsf{F}}(\mathsf{A})$ where $\mathsf{F}(k,(tw,m)) := \mathsf{E}(k,tw,m)$. In a similar way, tweakable pseudorandom permutations require that E is indistinguishable from a random permutation for any choice of k and tw.

2.3 Nonce-based Authenticated Encryption (nAE) and Encryption (nE and ivE) schemes

For the syntax of encryption schemes we follow the approach of Namprempre et al. [25] (taken by the work of Rogaway [34]) where the encryption algorithm is deterministic and an "*initialization vector*"(IV) *iv* is surfaced (and it may be seen as part of the AD [35]). Using this approach we classify encryption schemes according to the requirements of this extra input to provide CPA-security.

Definition 2 ([25]). *A scheme for* nonce-based authenticated encryption *(*nAE*) is a triple $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$, where the keyspace $\mathcal{K}$ is a nonempty set, the encryption algorithm* AEnc *is a deterministic algorithm which takes as input the tuple $(k,n,a,m) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$ and outputs a string $c \leftarrow \mathsf{AEnc}_k^{n,a}(m)$ called ciphertext.*
The decryption algorithm ADec *is a deterministic algorithm which takes as input the tuple $(k,n,a,c) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C}$ and outputs $m \leftarrow \mathsf{ADec}_k^{n,a}(c)$ which is either a string $m \in \mathcal{M}$ or the symbol $\perp$ ("invalid").*
We require that the algorithms AEnc *and* ADec *are the inverse of each other, that is:*

- (Correctness) *if $\mathsf{AEnc}_k^{n,a}(m) = c$ then $\mathsf{ADec}_k^{n,a}(c) = m$*
- (Tidiness) *if $\mathsf{ADec}_k^{n,a}(c) = m \neq \perp$ then $\mathsf{AEnc}_k^{n,a}(m) = c$*

If $\mathsf{ADec}_k^{n,a}(c) = \perp$ we say that the algorithm rejects *c, otherwise it* accepts *c.*
A sloppy nAE *scheme satisfies everything but the tidiness condition.*
A nonce-based Encryption scheme (nE) *is a triple $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$, where* Enc *and* Dec *do not take input the AD, that is, $\mathsf{Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \longmapsto \mathcal{C}$ and $\mathsf{Dec} : \mathcal{K} \times \mathcal{N} \times \mathcal{C} \longmapsto \mathcal{M}$.*
An iv-based encryption scheme ivE *is synctactically equivalent to a* nE *scheme, with the only difference that the nonce space $\mathcal{N}$ is replaced with an IV space $\mathcal{IV}$.*

Tidiness, as correctness, is usually seen as a syntactic requirement (for example Namprempre et al., [25]). Instead, in this paper, we show an explicit case where this property is fundamental to provide security (see Section 7.1).
Paterson et al. [28] defined the "collision-resistant decryption" (CRD), which is

a security property. Tidy schemes are inherently CRD-secure, since there is one and only valid ciphertext for each input, but the converse is not valid (because CRD-security is obtained when adversaries are able to break it with negligible probability, while tidiness always works).

The difference between nE schemes and ivE schemes lies in their security requirements. A complete survey about nAE, nE and ivE schemes can be found in Supp. Mat. A.

2.4 Security for nAE, nE and ivE schemes

The security definitions for nAE, nE and ivE schemes are inspired from those in [25] and [35].

Definition 3. *A nonce-based authenticated encryption scheme* (nAE) $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ *is* (q, t, ϵ)-nAE-secure *if the advantage*

$$\mathsf{Adv}^{\mathsf{nAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| \quad (1)$$

is bounded by ϵ *for every* (q, t)*-adversary* A *that respects the following two conditions: (i) If* A *queried the first (encryption) oracle on input* (n, a, m) *and was answered* c*, then he is not allowed to query the second (decryption) oracle on input* (n, a, c)*. (ii)* A *is not allowed to repeat the first component (the nonce) on different left oracle queries.*

$\boldsymbol{\Pi}$ *is* (q, t, ϵ)-nAE − E *secure, if the advantage*

$$\mathsf{Adv}^{\mathsf{nAE-E}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| \quad (2)$$

is bounded by ϵ *for every* (q, t)*-adversary* A *that respects Condition (ii) above.*

A nonce-based encryption scheme (nE) $\Pi := (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* (q, t, ϵ)-nE-secure *if the advantage,*

$$\mathsf{Adv}^{\mathsf{nE}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{Enc}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot)} \Rightarrow 1\right]\right| \quad (3)$$

is bounded by ϵ *for every* (q, t)*-adversary* A *that respects Condition (ii) above.*

An iv-based encryption scheme ivE $\Pi := (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* (q, t, ϵ)-ivE-secure *if the advantage*

$$\mathsf{Adv}^{\mathsf{ivE}}_{\Pi}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{Enc}^{\$}_k(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot)} \Rightarrow 1\right]\right| \quad (4)$$

is bounded by ϵ *for every* (q, t)*-adversary. Here the oracle* $\mathsf{Enc}^{\$}(m)$ *picks a random* $iv \leftarrow \mathcal{IV}$*, then computes* $c \leftarrow \mathsf{Enc}_k(iv, m)$ *and returns* (iv, c)*.*

As a result of this definition, the only difference between ivE and nE security is the requirement on their auxiliary input: non-repeating nonces for nE and random *iv*s for ivE. We observe that ivE-security implies nE security when uniformly

random *iv*s are expected to differ with overwhelming probability. The contrary does not hold: the CTR mode is well-known illustration (details are provided in Supp. Mat. G.1).

In some cases, it is desirable to guarantee some security even if nonces are repeated: this is called resistance to nonce misuse, or simply misuse resistance.

Definition 4. *If we drop Condition (ii) on the non repetition of the nonces in the* nAE *(resp.* nE*) security definitions, then we augment the security notions with* misuse resistance*. Namely, we say that the* nAE *(resp.* nE*) scheme is* (q, t, ϵ)-mrAE *(resp.* (q, t, ϵ)-mrE*) secure.*

We point out that in the mrE definition the adversary has only access to an encryption oracle. An example of an nE scheme which is mrE and not mrAE is given in Supp. Mat. H.
The mrE definition is trivially extended to ivE schemes, since the syntax of nE schemes and ivE schemes is identical.

2.5 Chosen-plaintext attack security with chosen nonce

We define mCPA security for nE and ivE schemes in the multi-challenge setting, following [15], [6]. This security notion is implied by the ivE, nE, and nAE security notions, and is equivalent to the more common single-challenge notion (details are provided in Supp. Mat. A.5 and A.6).

Definition 5. *A nonce-based Encryption scheme* nE $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* (q, t, ϵ)-mCPA *secure, or* (q, t, ϵ)*-secure against chosen plaintext attacks for multiple encryptions, if:*

$$\mathsf{Adv}^{\mathsf{mCPA}}_{\Pi}(\mathsf{A}) := \left| \frac{1}{2} - \Pr\left[b' = b; b \leftarrow \{0,1\},\ b' \leftarrow \mathsf{A}^{\mathsf{Enc}^b_k(\cdot,\cdot,\cdot)} \right] \right|$$

is bounded by ϵ *for any* (q, t)*-adversary. Here the oracle* $\mathsf{Enc}^b_k(\cdot,\cdot,\cdot)$ *is an oracle, which on input* $(n, m_0, m_1) \in \mathcal{N} \times \mathcal{M}^2$ *outputs* $c \leftarrow \mathsf{Enc}_k(n, m_b)$ *for a random secret bit* $b \leftarrow \{0,1\}$*, which the oracle has picked at the start of the game. When the adversary* A *queries* $\mathsf{Enc}^b_k(\cdot,\cdot,\cdot)$*, he must choose two messages* m_0 *and* m_1 *s.t.* $|m_0| = |m_1|$*. Moreover he cannot repeat the first input (the nonce) in different queries.*

There is a completely similar definition for ivE schemes. We only have to replace $\mathsf{Enc}^b_k(\cdot,\cdot,\cdot)$ with $\mathsf{Enc}^{b,\$}_k(\cdot,\cdot)$, and to adapt the $\$(\cdot,\cdot,\cdot)$ oracle accordingly. Similarly there is a similar notions for nAE schemes, obtained from the previous one by replacing $\mathsf{Enc}_k(\cdot,\cdot)$ with $\mathsf{AEnc}_k(\cdot,\cdot,\cdot)$ and adapting $\$(\cdot,\cdot,\cdot)$ accordingly.

2.6 Authenticity (INT-CTXT)

Following Bellare et al. [6], we focus on the notion of ciphertext integrity with a single decryption query. Several variants are available in the literature, which we present and prove to be equivalent in Supp. Mat. A.7.

Definition 6. *A nonce-based authenticated encryption scheme* nAE $\boldsymbol{\Pi} = (\mathcal{K},$ AEnc, ADec) *is* (q, t, ϵ)-INT-CTXT1(Ciphertext integrity with only 1 decryption query)-secure *if*

$$\mathsf{Adv}^{\text{INT-CTXT1}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \Pr\left[\perp \neq m^* \leftarrow \mathsf{ADec}_k(n^*, a^*, c^*);\ (n^*, a^*, c^*) \leftarrow \mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot)}\right]$$

is bounded by ϵ *for every* (q, t) *adversary. The adversary* A *is not allowed to repeat the first component (the nonce) on different oracle queries. Moreover he is not allowed to output* (n^*, a^*, c^*) *if he received* c^* *as* $c^* \leftarrow \mathsf{AEnc}_k(n^*, a^*, m^*)$ *for a certain input* (n^*, a^*, m^*) *that he asked to the first oracle.*

As we can expect, an nAE scheme that offers both mCPA and INT-CTXT1 security is an nAE scheme, and we prove this in Supp. Mat. A.7.

2.7 Message Authentication Code (MAC)

Apart from an encryption scheme, all our composition modes are based on a deterministic notion of Message Authentication Code (MAC).

Definition 7. *A* Message Authentication Code MAC *is a triple* $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *where the keyspace* $\mathcal{K}$ *is a non-empty set, the tag-generation algorithm* Mac *is a deterministic algorithm that takes as input the couple* $(k, m) \in \mathcal{K} \times \mathcal{M}$ *and outputs the tag* $\tau \leftarrow \mathsf{Mac}_k(m)$ *from the tag space* $\mathcal{T}$*. The verification algorithm* Vrfy *takes as input a triple* (k, m, τ) *in* $\mathcal{K} \times \mathcal{M} \times \mathcal{T}$ *and outputs* $\top$ *(accept) or* $\perp$ *(reject). We ask that* $\mathsf{Vrfy}(k, m, \mathsf{Mac}(k, m)) = \top$.
A string-input MAC strMAC *has as input space a set of strings, that is* $\mathcal{M} \subseteq \{0,1\}^*$.
A vector-input MAC vecMAC *has as input space* $\mathcal{M}$ *which has one or more component and it can accept tuples of strings as input.*

Usually the security for MACs is expressed as unforgeability, but our composition modes rely on a Mac function that is a $(q, t, \epsilon_{\text{PRF}}) - \text{PRF}$.

Definition 8. *([25]) A* MAC $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *is* $(q, t, \epsilon) - \text{PRF}$*-secure if*

$$\mathsf{Adv}^{PRF}_{\Pi}(\mathsf{A}) := \mathsf{Adv}^{PRF}_{\mathsf{Mac}}(\mathsf{B})$$

is bounded by ϵ *for any* (q, t) *adversary* B *and if* $\mathsf{Vrfy}(k, m, \mathsf{Mac}(k, m)) = \top$ *iff* $\tau = \mathsf{Mac}(k, m)$.

For completeness, the standard definitions are put in Supp. Mat. A.9.

3 Problem

As discussed earlier, Namprempre et al. [25] left open the problem of the nAE security of 4 modes based on the Tag-then-Encrypt paradigm, which have been shown in Fig. 1.

Formally, the first three modes compose an ivE scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ and two vecMAC schemes using the same key, $\mathsf{MAC}^{\mathsf{IV}} = (\mathcal{K}_M, \mathsf{Mac}^{\mathsf{IV}}, \mathsf{Vrfy}^{\mathsf{IV}})$ and $\mathsf{MAC}^{\mathsf{Tag}} = (\mathcal{K}_M, \mathsf{Mac}^{\mathsf{Tag}}, \mathsf{Vrfy}^{\mathsf{Tag}})$ in this way:

– A10: $\mathsf{AEnc}^{n,a}_{k_E,k_M}(m) := c$ with $iv = \mathsf{Mac}^{\mathsf{IV}}_{k_M}(n,a)$, $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(a,m)$ and $c = \mathsf{Enc}_{k_E}(iv, m||\tau)$
– A11: $\mathsf{AEnc}^{n,a}_{k_E,k_M}(m) := c$ with $iv = \mathsf{Mac}^{\mathsf{IV}}_{k_M}(n,a)$, $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(m)$ and $c = \mathsf{Enc}_{k_E}(iv, m||\tau)$
– A12: $\mathsf{AEnc}^{n,a}_{k_E,k_M}(m) := c$ with $iv = \mathsf{Mac}^{\mathsf{IV}}_{k_M}(n)$, $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(a,m)$ and $c = \mathsf{Enc}_{k_E}(iv, m||\tau)$

The fourth mode composes a nE Encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ and a vecMAC $= \mathsf{MAC} = (\mathcal{K}_M, \mathsf{Mac}, \mathsf{Vrfy})$:

– N4: $\mathsf{AEnc}^{n,a}_{k_E,k_M}(m) := c$ with $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(a,m)$ and $c = \mathsf{Enc}_{k_E}(n, m||\tau)$

For clarity we reserve bold notations $\mathbf{m}$ for the messages inputs of the nAE scheme $\boldsymbol{\Pi}$ and normal notations m for the messages inputs to the underlying nE (or ivE)-scheme Π (so, we typically have that $m = \mathbf{m}\|\tau$).

If Π is tidy and the MAC is PRF-secure, then the AE scheme $\boldsymbol{\Pi}$, obtained composing these components, is tidy. These modes also offer CPA security, which directly results from the underlying encryption schemes (a proof of this statement is available in Supp. Mat. Thm. 3 and 4).

As a result, the open question lies in the INT-CTXT security of these modes.

4 Attack against mode N4

We provide here an attack against the mode N4, explicitly presenting an nAE-scheme $\boldsymbol{\Pi}$, based on an nE Encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ and a vecMAC $\mathsf{MAC} = (\mathcal{K}_M, \mathsf{Mac}, \mathsf{Vrfy})$ which is PRF-secure. For simplicity, we consider only the case when the message $\mathbf{m}$ of $\boldsymbol{\Pi}$ is N-bit long and the tag is N-bit long, leaving the general case to Supp. Mat. D. The nE Encryption scheme, which encrypts $2N$-bit long message, is nE-secure and tidy, but the nAE-scheme $\boldsymbol{\Pi}$ obtained composing them according to mode N4, is not secure and, in particular, it is not INT-CTXT1-secure as we show a forgery.
The idea of the forgery is to force the tag τ of a couple $(a, \mathbf{m})$ to be encrypted identically for two different nonces, while keeping the nE-security.

4.1 Construction

Following the definition of mode $N4$, an authenticated ciphertext is computed as $c = \mathsf{Enc}_{k_E}(n, \mathbf{m}||\mathsf{Mac}_{k_M}(a, \mathbf{m}))$, for which Mac is a PRF. We now define the nE scheme Π.

The keys produced in Π are made of two components (k, v^*): the key $k \in \mathcal{K}$ of a TPRF E and a random value v^*, which has the size of block of E, that is, N bits. This value v^* will be leaked to Adv when asking for the encryption of a message with the nonce $n = 1$, and will then be used to trigger a kind of Trojan in the encryption scheme. That Trojan will have the following behavior: for nonces $n = 1, 2$, and if the first message block is v^*, then the last ciphertext block will be computed in a way that ignores the value of n.

This behavior is benign when considering the nE security of Π: the only way to observe it would be to make two encryption queries with nonces 1 and 2, and first message block v^*. But doing this would require guessing v^* before querying with nonce 1 (the nE adversary is nonce respecting), and this cannot be done but with probability 2^{-N}: it would require guessing v^*.

As we will see, it is not benign anymore when considering the ciphertext integrity property: there, Adv is free to use the nonces 1 and 2 in its decryption query, even if these nonces were used in encryption queries.

To make things concrete, we define the encryption process Enc of Π using a TPRF $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \{0,1\}^N \longmapsto \mathcal{T} = \{0,1\}^N$ with tweak space $\mathcal{TW} = \{0,1,2\} \times \{0,1\}$. For a message $m = (m_1, m_2) \in \{0,1\}^{2N}$, the ciphertext $\mathsf{Enc}_k^n(m)$ is made of three blocks (c_0, c_1, c_2) computed as follows:

- $c_0 = \mathsf{E}_k^{(0,0)}(n)$ unless $n = 1$, in which case $c_0 := v^*$.
- $c_1 = m_1 \oplus \mathsf{E}_k^{(1,0)}(n)$.
- $c_2 = m_2 \oplus \mathsf{E}_k^{(2,0)}(n)$, unless the condition $[(n = 1 \vee n = 2) \wedge m_1 = v^*]$ is met, in which case $c_2 = m_2 \oplus \mathsf{E}_k^{(2,1)}(0)$.

With such a definition, the block c_0 looks random for any input, and its only purpose is to leak v^* when $n = 1$. The block c_1 is a traditional encryption of the message block m_1 using the TPRF E. The block c_2 is computed in the same way (just incrementing the tweak), except under a very specific condition: the nonce is either 1 or 2, and the first message block $m_1 = v^*$. Under that condition, the ciphertext block becomes independent of the nonce. As explained above, this condition is designed in such a way that it cannot lead to any observable event when Adv can only access an encryption oracle in a nonce respecting way: that would require querying Enc on a message starting with v^* on both $n = 1$ and $n = 2$, but v^* is only learned after a query with $n = 1$, and it is then not permitted to make a second query with $n = 1$ and v^* as message block.

The decryption of Π works in the natural way. In particular, in order to guarantee the tidiness of the nE encryption scheme, Dec must verify the correctness of the first ciphertext block c_0.

The proofs that Π is nE-secure (Prop. 10) and tidy (Prop. 11) can be found in Supp. Mat. F.2.

4.2 Forgery

The composition of the previous nE scheme Π with a PRF-secure MAC according to mode N4 is not $\mathsf{INT\text{-}CTXT}1$-secure. In fact, we provide a forgery where the adversary A asks the encryption of only two messages:

1. It first asks for an encryption of $(1, a, \mathbf{m})$, for arbitrary choices of a and $\mathbf{m}$. This returns a ciphertext whose first block is v^*, second block is $c_1 = \mathbf{m} \oplus \mathsf{E}_k^{(1,0)}(1)$, and third block is ignored.
2. It then asks for an encryption of $(2, a, v^*)$. This returns a ciphertext whose last block is $c_2 = \mathsf{Mac}_{k_M}(a, v^*) \oplus \mathsf{E}_k^{(2,1)}(0)$.

Eventually, Adv makes a decryption query on $(1, a, (v^*, c_1 \oplus \mathbf{m} \oplus v^*, c_2))$, which is different of the two previously obtained ciphertexts, and has a valid decryption to v^*, hence violating the ciphertext integrity property.

This shows that N4 is not a secure composition mode, in general.

5 Security relations among A10, A11 and A12

While we are able to prove the generic insecurity of N4, we are not able to prove that modes A10,A11 and A12 are either secure or insecure in general. Still, in this section, we prove that these three modes are either all secure or all insecure.

To prove it we need to replace the two $\mathsf{vecMACs}$ $\mathsf{vecMAC}^{\mathsf{IV}}$ and $\mathsf{vecMAC}^{\mathsf{Tag}}$ with two $\overline{\mathsf{vecMAC}}$s based on the random functions f^{IV} and $\mathsf{f}^{\mathsf{Tag}}$. Now the key of the new nAE scheme is $k := (k_E, \mathsf{f}^{\mathsf{IV}}, \mathsf{f}^{\mathsf{Tag}})$. To highlight these changes, we call the new modes $\overline{\text{A10}}, \overline{\text{A11}}$ and $\overline{\text{A12}}$ and the new nAE-schemes $\overline{\boldsymbol{\Pi}}$. The security relations among modes $\overline{\text{A10}}, \overline{\text{A11}}$ and $\overline{\text{A12}}$ immediately lift to modes A10,A11 and A12. The standard details are discussed in Appendix F.3 (Lemma 3).

We show the security equivalence of A10, A11 and A12 based on two events, B and C, that we define below. Consider a $\mathsf{INT\text{-}CTXT1}$ adversary A against an nAE scheme $\overline{\boldsymbol{\Pi}}$ (which is made according to any of $\overline{\text{A10}}$, $\overline{\text{A11}}$ or $\overline{\text{A12}}$). If the q-th decryption query (n^q, a^q, c^q) is valid, then $c^q = \overline{\mathsf{AEnc}_k}(n^q, a^q, \mathbf{m}^q)$ for a certain message $\mathbf{m}^q$, as a result of tidiness. Depending on the value of (n^q, a^q) (or only n^q for $\overline{A12}$), we distinguish between two possibilities, which define event B:

- (n^q, a^q) is fresh, that is, $(n^q, a^q) \neq (n^j, a^j)\ \forall j = 1, ..., q-1$ (we call this event B) [for mode $\overline{\text{A12}}$, we only demand that n^q is fresh, that is $n^q \neq n^j\ \forall j = 1, ..., q-1$].
- $(n^q, a^q) = (n^j, a^j)$ for a $j \in \{1, ..., q-1\}$ (This j is unique since the nonce n cannot be repeated) [for mode $\overline{\text{A12}}$, we only demand that $n^q = n^j$ for a $j \in \{1, ..., q-1\}$].

With regard to $(a^q, \mathbf{m}^q)$ (or only $\mathbf{m}^q$ for mode $\overline{A11}$), we again consider two possibilities, which define event C:

- $(a^q, \mathbf{m}^q)$ is fresh, that is $(a^q, \mathbf{m}^q) \neq (a^j, \mathbf{m}^j)\ \forall j = 1, ..., q-1$ (we call this event C) [for mode $\overline{\text{A11}}$, we only demand that m^q is fresh, that is $\mathbf{m}^q \neq \mathbf{m}^j\ \forall j = 1, ..., q-1$].
- $(a^q, \mathbf{m}^q) = (a^j, \mathbf{m}^j)$ for some $j \in \{1, ..., q-1\}$ (there can be several such j's) [for mode $\overline{\text{A11}}$, we only demand $\mathbf{m}^q = \mathbf{m}^j$ for some $j \in \{1, ..., q-1\}$].

Clearly by total law of probability

$$\Pr[\mathsf{A}\text{ wins}] = \Pr[\mathsf{A}\text{ wins } \cap C] + \Pr[\mathsf{A}\text{ wins } \cap B \cap \overline{C}] + \Pr[\mathsf{A}\text{ wins } \cap \overline{B} \cap \overline{C}]$$

With the following lemma we treat the first two addends of the previous equation:

Lemma 1. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *[for mode* $\overline{A12}$*,* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \longmapsto \mathcal{IV}$ *] and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *[for mode* $\overline{A11}$*,* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{M} \longmapsto \mathcal{T}$ *] be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE *scheme obtained composing* f^{IV}*,* $\mathsf{f}^{\mathsf{Tag}}$ *and* Π *according to mode* $\overline{A10}$ *or* $\overline{A11}$ *or* $\overline{A12}$*. Then we can bound*

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

The proof is completely standard and can be found in Supp. Mat. F.3 (the ideas of this proof are already present in Namprempre et al. [25]. The proofs of the security implications between the 3 "A" modes then results from implications in the case A wins $\cap \overline{B} \cap \overline{C}$, which we examine in the rest of this section.

In order to make our notations more precise, if either f^{IV} or $\mathsf{f}^{\mathsf{Tag}}$ have different signatures for two modes that we compare, we use a subscript to denote the mode that is used (e.g. $\mathsf{f}^{\mathsf{IV}_{10}}$ for mode A10).
In some proves we use hash function and their collision resistance, for more details about this see Katz and Lindell [15] or Supp. Mat. A.10.

5.1 The INT-CTXT1-security of $\overline{\mathbf{A12}}$ implies the INT-CTXT1-security of $\overline{\mathbf{A10}}$

Proposition 1. *Let* $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Then, if mode* $\overline{A12}$ *implemented with the random function* $\mathsf{f}^{\mathsf{IV}_{12}} : \mathcal{N} \longmapsto \mathcal{IV}$ *is* $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure then mode* $\overline{A10}$ *is* $(q-1, t, q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure*

The proof can be found in Supp. Mat. F.3.
Let $\mathsf{f}'^{\mathsf{IV}_{12}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ be defined $\mathsf{f}'^{\mathsf{IV}_{12}}(n, a) := \mathsf{f}^{\mathsf{IV}_{12}}(n)\ \forall n \in \mathcal{N}, a \in \mathcal{A}$ (it is an extension of $\mathsf{f}^{\mathsf{IV}_{12}}$). The proof is based on the fact that it is impossible using only encryption queries to mode $\overline{\text{A10}}$ to distinguish if it is used $\mathsf{f}^{\mathsf{IV}_{10}}$ or $\mathsf{f}'^{\mathsf{IV}_{12}}$ (as in mode $\overline{\text{A12}}$), since it is not possible for the adversary A to force the nAE algorithm to call $\mathsf{f}^{\mathsf{IV}_{10}}$ on inputs (n, a_1) and (n, a_2) (with $a_1 \neq a_2$) during encryption queries. Moreover, the couple (n^q, a^q) of the decryption query must not be fresh (due to event $\overline{B}$), thus, using $\mathsf{f}'^{\mathsf{IV}_{12}}$ is indistinguishable from using $\mathsf{f}^{\mathsf{IV}_{10}}$.

5.2 The INT-CTXT1-security of $\overline{\mathbf{A11}}$ implies the INT-CTXT1-security of $\overline{\mathbf{A10}}$

Proposition 2. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}_{10}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be a* $(0, t, \epsilon_{cr})$ *collision resistant hash function. Then, if mode* $\overline{A11}$*, implemented with the random function* $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$ *and with any* $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|})$$-\mathsf{ivE}$*-secure Encryption scheme, is* $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure then mode* $\overline{A10}$ *is* $(q-1, t, \epsilon)$-$\mathsf{INT\text{-}CTXT1}$*-secure, where*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\mathsf{INT\text{-}CTXT1}}.$$

The complete proof can be found in Supp. Mat. F.3.
The idea is to reduce the $\mathsf{INT\text{-}CTXT1}$ adversary A against scheme $\overline{\boldsymbol{\Pi}}$ (mode $\overline{\mathrm{A10}}$), which uses the ivE scheme Π, to a $\mathsf{INT\text{-}CTXT1}$ adversary C against scheme $\overline{\boldsymbol{\Pi}'}$ (mode $\overline{\mathrm{A11}}$), which uses the ivE scheme Π'. When the adversary A makes an encryption query $(n^i, a^i, \mathbf{m}^i)$ the adversary C makes an encryption query $(n^i, a^i, \mathbf{m}'^i)$ with $\mathbf{m}'^i = \mathsf{H}(a^i)\|\mathbf{m}^i$. The ivE scheme Π' encrypts $m'^i = (\mathsf{H}(a^i)\|m^i[=\mathbf{m}^i\|\tau^i])$ in this way: $\mathsf{Enc}'(m'^i) := \mathsf{H}(a^i) \oplus \mathsf{f}^{\mathsf{Enc}}(iv^i)\|\mathsf{Enc}(iv^i, m^i)$, where $\mathsf{f}^{\mathsf{Enc}}$ is a random function (and it is part of the key the scheme Π'). When the adversary A makes his decryption query (n^q, a^q, c^q) the adversary C simply asks the decryption of $(n^q, a^q, \left[\mathsf{f}^{\mathsf{Enc}}(iv^q) \oplus \mathsf{H}(a^q)\right]\|c^q)$ (the iv^q must be not fresh due to event $\overline{B}$).

5.3 The INT-CTXT-security of $\overline{\mathrm{A10}}$ implies the INT-CTXT-security of $\overline{\mathrm{A12}}$

Proposition 3. *Let* $\mathsf{f}^{\mathsf{IV}_{12}} : \mathcal{N} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE*-scheme obtained composing these components according to mode* $\overline{A12}$*. Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be* $(0, t, \epsilon_{cr})$*.*
Then, if mode $\overline{A10}$*, implemented with the random function* $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and with any* $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|})-\mathsf{ivE}$*-secure Encryption scheme, is* $(q, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure then mode* $\overline{A12}$ *is* $(q-1, t, \epsilon)$-$\mathsf{INT\text{-}CTXT1}$*-secure with*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\mathsf{INT\text{-}CTXT1}}.$$

The complete proof can be found in Supp. Mat. F.3.
The idea of the proof is similar to the previous one (Propo. 2), where we replace $\mathbf{m}^i$ with $\mathbf{m'}^i = (\mathsf{H}(a^i\|\mathbf{m}^i)$.

5.4 The INT-CTXT-security of $\overline{\mathrm{A10}}$ implies the INT-CTXT-security of $\overline{\mathrm{A11}}$

Proposition 4. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE *scheme obtained composing these components according to mode* $\overline{A11}$*. Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be a* $(0, t, \epsilon_{cr})$*-collision resistant hash function.*
Then, if mode $\overline{A10}$*, implemented with the random function* $\mathsf{f}^{\mathsf{Tag}_{10}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$*, is* $(q, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure then mode* $\overline{A11}$ *is* $(q-1, t, \epsilon')$-$\mathsf{INT\text{-}CTXT1}$*-secure with*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\mathsf{INT\text{-}CTXT1}}.$$

The complete proof can be found in Supp. Mat. F.3.
The idea is to reduce the $\mathsf{INT\text{-}CTXT1}$ adversary A against scheme $\overline{\boldsymbol{\Pi}}$ (mode $\overline{\mathrm{A11}}$) to a $\mathsf{INT\text{-}CTXT1}$ adversary C against scheme $\overline{\boldsymbol{\Pi}_{10}}$ (mode $\overline{\mathrm{A10}}$). When the

adversary A makes an encryption query $(n^i, a^i, \mathbf{m}^i)$, the adversary C makes an encryption query $(n^i \| \mathsf{H}(a^i), a, \mathbf{m}^i)$. When the adversary A makes his decryption query (n^q, a^q, c^q) the adversary A' simply asks the decryption of $(n^q \| \mathsf{H}(a^q), a, c^q)$.

6 Secure variants of modes N4, A10, A11 and A12

As a step towards the proof of the generic (in-)security of A10, A11 and A12, we consider two natural conditions on the ivE scheme that are sufficient to guarantee a secure composition. More precisely, we show that, if the ivE scheme is misuse resistant or if it is "message-malleable" (a condition that is satisfied by many standard modes, and that we formalize precisely below), then these modes are secure. Interestingly, these two properties are the two extreme of the range (clearly, it is impossible for a scheme to have both properties).

We prove everything only for mode A10, since the proofs can be straightforwardly extended to the other two modes. In this section we use the same replacement as in the previous one (we replace mode A10 with mode $\overline{\text{A10}}$). Surprisingly, we prove the same results for mode N4.

Then, we conclude this section, comparing our partial results about the (in)-security of modes A10, A11 and A12 with those of Namprempre et al. [25].

6.1 Misuse-resistant ivE scheme

Proposition 5. *Let the* ivE *scheme* Π *be a* $(q, t, \epsilon_{\mathsf{mrE}})$*-misuse resistant* mrE *and* $(q, t, \epsilon_{\mathsf{ivE}}) - \mathsf{ivE}$ *secure, let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions. Then, the scheme* $\overline{\boldsymbol{\Pi}}$ *obtained composing these components according to mode* $\overline{A10}$*, is* $(q-1, t, (q-1)|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + (q-1)\epsilon_{\mathsf{mrE}}) - \mathsf{INT\text{-}CTXT1}$*-secure.*

The details of the proof are available in Supp. Mat. F.4. As seen above, we only need to consider the case not studied in Lemma 1. The idea of the proof is to reduce the $\mathsf{INT\text{-}CTXT1}$ adversary to a mrE-adversary. Since we are not in the cases studied in Lemma 1, the couples (n^q, a^q) and $(a^q, \mathbf{m}^q)$ are not fresh, and it is enough for the mrE adversary to ask one more encryption query guessing that the message encrypted $\mathbf{m}^q \| \tau^q$ is one of the message the $\mathsf{INT\text{-}CTXT1}$ adversary has already asked to encrypt with the same AD a^q (that is, $\mathbf{m}^q \in \mathcal{M}_{a^q}$ where $\mathcal{M}_{a^q} := \{\mathbf{m}_i \ i = 1, ..., q-1 \ s.t. a^i = a^q\}$). If the ciphertext obtained is the ciphertext c^q that he is asked to decrypt, then he outputs 1 and, otherwise, 0. The mrE adversary wins only if he guesses correctly and he can guess correctly at most with probability $(q-1)^{-1}$.
Allowing the mrE adversary to ask $(2q-2)$ encryption queries the scheme $\overline{A10}$ would be $(q, t, \frac{2q-1}{|\mathcal{T}|} + 2\epsilon_{\mathsf{mrE}}) - \mathsf{INT\text{-}CTXT1}$-secure, because the mrE adversary may try every possible message in $\mathcal{M}_{a^q}$ (see for more details Supp. Mat. F.4 Propo. 12).

We remember that for the misuse-resistance of Enc (Def. 3) the adversary has only access to encryption queries.

6.2 "Message-malleable" nE scheme

Definition 9. *A nonce-based encryption scheme* nE $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* message-malleable *if, given an encryption* c *of a message* m *with nonce* n*, an adversary can efficiently decrypt all couples* (n, c')*, i.e., he is able to compute* m' *s.t.* $m' \leftarrow \mathsf{Dec}_k(n, c')$ *without having access to a decryption oracle.*

The same definition may be done for ivE schemes. Many standard schemes (as CTR and OFB [15]) have this "insecurity" property when they are used for fixed length messages. We detail some examples in Supp. Mat. G. Message-malleability is easy to prove in many cases, e.g., when the ciphertext $c = \mathsf{Enc}_k^{iv}(m)$ is computed as a pseudorandom bitstream r computed from the iv and it is XORed with the message m (that is, $c = r \oplus m$), then $\mathsf{Dec}_k^{iv}(c') = c \oplus c' \oplus m$.

Message-malleability allows us to prove the following proposition for $\overline{A10}$, which can be easily extended to modes $\overline{A11}$ and $\overline{A12}$).

Proposition 6. *Let the* ivE *scheme* Π *be* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure,* $(q-1, t, \epsilon_{\mathsf{mCPA}})$-$\mathsf{mCPA}$*-secure and "message-malleable", let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions. Then, the scheme* $\overline{\boldsymbol{\Pi}}$ *obtained composing these components according to mode* $\overline{A10}$*, is* $(q, t, (q-1)\epsilon_{\mathsf{ivE}} + q|\mathcal{T}|^{-1} + 8\epsilon_{\mathsf{mCPA}})$-$\mathsf{INT\text{-}CTXT1}$*-secure.*

The details of the proof are available in Supp. Mat. F.4.
Again, we only need to consider the case that is not covered by Lemma 1. The idea of the proof is to reduce the $\mathsf{INT\text{-}CTXT1}$ adversary to an mCPA-adversary. Since we are not in the cases studied in Lemma 1, the couples (n^q, a^q) (thus iv^q) and $(a^q, \mathbf{m}^q)$ are not fresh. The mCPA adversary, when he is asked to simulate the AEnc oracle on input (n^i, a^i, m^i) simply computes iv^i and τ^i using the appropriate functions and asks his Enc oracle on input $(iv^i, m^i \| \tau^i, m^i \| r^i)$ where r^i is a random value picked in $\mathcal{T}$, receiving c^i which he forwards to the $\mathsf{INT\text{-}CTXT}$ adversary. When this latter adversary outputs (n^q, a^q, c^q), the mCPA adversary computes iv^q, which, due to the fact that we are in the case not covered by Lemma 1, is iv^j for a $j \in \{1, ..., q-1\}$. Now using the fact that Π is "nonce-message-malleable", he can decrypt c^q as if $c^i = \mathsf{Enc}_{k_E}^{iv^i}(m^i \| \tau^i)$. He outputs 0 if the decryption query is valid, 1 otherwise. We observe that if $c^i = \mathsf{Enc}_{k_E}^{iv^i}(m^i \| r^i)$ the decryption query may be valid with probability $|\mathcal{T}|^{-1}$ since the tags have never been used before the decryption query.

6.3 Extension to N4

Surprisingly, although mode N4 is not secure in general (see Sec. 4), if the nE scheme is either misuse-resistant or message-malleable, mode N4 is $\mathsf{INT\text{-}CTXT1}$-secure and, thus, nAE secure. It is easy to prove easily adapting the proofs of

Propo. 5 and Propo. 6 to the nE case (Prop. 13.
This implies that for N4 it is capital that the adversary can efficiently decrypt *everything*. In fact, the nE scheme used in Sec. 4 is message-malleable except in the case if $n = 1$ or 2 when trying to decrypt or encrypt $(v^*, \cdot)$.

6.4 Comparison to Namprempre et al. [25]

Namprempre et al. [25] gave partial results using the Knowledge-of-Tag property (KoT) (introduced in Supp. Mat. B). That is, adversaries must forge without any (extractable) knowledge of the tag used in the decryption query [25].
With respect to their work, although the main ideas of the proofs are very similar, it is much easier to prove that a scheme is mrE or message-malleable, than to prove that a scheme is KoT-secure (while it may be easy to prove that it is not KoT-secure). In fact, to prove that a scheme is message-malleable it is enough to provide an algorithm which efficiently computes the result. On the other hand to prove that a scheme is not message-malleable (a part from proving that it is mrE), it must be proved that *all* efficient adversaries are not able always to decrypt. Similarly to prove the KoT security it must be proved that for *all* possible efficient extractors the scheme has this property, while to prove that a scheme is not KoT secure, it is enough to provide a counterexample.

7 Insecure variants of modes A10, A11 and A12

While, in the previous section, we proved the security of A10, A11 and A12 by making some extra requirements on the ivE scheme, this section considers the relaxation of some of the requirements on ivE that makes these 3 modes to become insecure. More precisely, we show how to compute forgeries against the INT-CTXT property of mode A10 when the ivE scheme is non tidy or stateful. These attacks imply that the three modes are not nAE-secure, when implemented with such schemes.

7.1 Tidiness as a security property

Given an IV-based encryption $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$, our idea is to turn Π into a sloppy IV-based scheme. This modification augments the ciphertext $c = \mathsf{Enc}_k(iv, m)$ with $c' = \mathsf{Enc}_{k'}(iv, m)$, leading to a double and independent encryption m with the same iv. It is easy to see that, for random iv, the new scheme has pseudorandom ciphertext $C = (c, c')$ as long as Π has pseudorandom ciphertext, (that is, if Π is ivE-secure). However, given iv, if we define the decryption of $C = (c, c')$ simply as $\mathsf{Dec}_k(iv, c)$ without any validity consideration on c', the new scheme is not tidy whether Π is tidy or not. Therefore, since the c' part of C is "out of control", any ciphertext $C' = (c, c'')$ decrypts to m and is deemed valid. Moreover, the A10 composition mode with two PRF-secure vecMACs does not rule out this malleability so that we can build a forgery with a single encryption query. Dropping the tidiness requirement of ivE, and then of nAE, is thus sufficient to leave a security breach in the resulting nAE.

More formally, we build $\Pi' = (\mathcal{K}, \mathsf{Enc}', \mathsf{Dec}')$ with keyspace $\mathcal{K}^2$, message space $\mathcal{M}$ and ciphertext space $\mathcal{C}^2$ as follows: $\mathsf{Enc}'_{(k,k')}(iv, m)$ outputs $C = (c, c')$ where $c = \mathsf{Enc}_k(iv, m)$ and $c' = \mathsf{Enc}_{k'}(iv, m)$; $\mathsf{Dec}'_{(k,k')}(iv, C)$ parses the ciphertext as $C = (c, c')$ and outputs $m = \mathsf{Dec}_k(iv, c)$. For any $c'' \neq c'$, we have $\mathsf{Enc}'(iv, \mathsf{Dec}'(iv, (c, c''))) = (c, c') \neq (c, c'')$ so that Π' is not tidy.

Let nAE be the authenticated encryption obtained from the A10 mode whose ciphertext has the form $C = (c, c')$ where $c = \mathsf{Enc}_k(iv, \mathbf{m}\|\tau)$ and $c' = \mathsf{Enc}_{k'}(iv, \mathbf{m}\|\tau)$ with $iv = \mathsf{Mac}^{\mathsf{IV}}_{k_M}(n, a)$ and $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(a, \mathbf{m})$. Now, we consider the forger A which makes a single encryption query on any triple $(n, a, \mathbf{m})$ and receives back $C = (c, c')$ as above. Then, A picks any (samplable) $c'' \in \mathcal{C}$ distinct of c' and outputs $C^\star = (c, c'')$. Following the description of the A10 mode we find that the decryption starts by running $iv = \mathsf{Mac}^{\mathsf{IV}}_{k_M}(n, a)$ and then $\mathsf{Dec}'_{(k,k')}(iv, C^\star) = \mathsf{Dec}_k(iv, c) = \mathbf{m}\|\tau$. Finally, since the check $\tau = \mathsf{Mac}^{\mathsf{Tag}}_{k_M}(a, \mathbf{m})$ passes $\mathbf{m} \neq \perp$ is returned although $C^\star \neq C$.

Message-malleability. In order to further emphasize the crucial role of the tidiness in the insecurity of the authenticated encryption based on Π', we stress that if the underlying IV-based scheme Π is tidy and message-malleable (Def. 9), the A10 composition implemented with Π leads to an nAE-secure scheme (as shown in Sec. 6.2). However, even if Π' is not tidy, it is easy to see that Π' remains message-malleable while we proved that it never leads to a nAE-secure scheme. As a summary, (non) tidiness alone has an intrinsic propensity to degrade the nAE-security of the AEnc based on the Tag-then-Encrypt paradigm.

7.2 Forgery against stateful A10, A11 & A12

In stateful AE schemes the AEnc and ADec algorithms receive at the start of the game an additional input, the *state*, which is updated during every call and kept in memory to be reused in the following call. The scheme we use has a stateless ADec algorithm, that is, it does not use the state and every reordering and omission is tolerable (L_0 of Rogaway et al. [36]). (for more details see Supp. Mat. F.5). With respect to their work we allow the adversary to choose the state at the start of the game.

The idea of this forgery is to use the state, which in our case is simply a counter of the encryption queries, as the nonce was used in the attack against mode N4 (Sec. 4). At the end of the section we discuss the meaning of tidiness for stateful schemes.

The ivE we present is an adaptation of the nE scheme used in Sec. 4. As there, we present it only for N-bit long message, leaving the general case in Supp. Mat. 'E. The main changes are:

- We use a TPRP $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \{0,1\}^N \longmapsto \{0,1\}^N$ instead of a TPRF.
- A new block c_{-1} is added to the ciphertext, in order to give the decryption algorithm the actual value of the counter *ctr* which is *an internal state only of the encryption device*, and $c_{-1} = \mathsf{E}^{(0,1)}_k(ctr)$. The Dec algorithm inverts

this to retrieve the correct ctr. The block c_{-1} is random since it is always obtained with different inputs (as long as the number of encryption queries is $<< 2^n$).
- To compute this block, the TPRF E is called with a tweak $(0,1)$ that is never used else
- The boxed **if** is triggered by the value of the counter ctr (not of the nonce) and m
- The iv replaces the nonce n in the input of the TPRF E.

Note again that, due to mode A10, the messages which the nAE scheme $\boldsymbol{\Pi}$ can encrypt, are N bits long, while those which Π can encrypt are $2N$ bits long. The full details can be found in Supp. Mat. F.5 as well with the general scheme for any message in $\{0,1\}^*$.

The forgery is an easy adaptation of that presented in Sec. 4 (the full details are in Supp. Mat. F.5).

The scheme Π is clearly ivE-secure (the details are in Supp. Mat. F.5), the only important change with Sec. 4 is the fact that we have to consider also the block c_{-1}). Now we have to discuss what means for a stateful nAE (or nE or ivE) scheme to be *tidy*.
For stateless nAE schemes the definition was given in Def. 12 (similarly for nE and ivE): if $\mathsf{ADec}_k^{n,a}(c) = m \neq \perp$ then $\mathsf{AEnc}_k^{n,a}(m) = c$.

Now if the nAE scheme is stateful it means that $\mathsf{AEnc}_k^{n,a}(m)$ is no more defined, because the state s may influence the output of $\mathsf{AEnc}_k^{(\cdot,\cdot)}(\cdot)$. Thus, denoting with $\mathcal{S}$ the set of possible states, we redefine tidiness as:

Definition 10. *We say that an* nAE *scheme is* tidy *if* $\mathsf{ADec}_k^{n,a}(c) = m$ *then* $c \in \{\mathsf{AEnc}_{k,s}^{n,a}(m)\}_{s\in\mathcal{S}}$.
Similarly an nE *(resp. an* ivE*) scheme is* tidy *if* $\mathsf{Dec}_k^{n,a}(c) = m$ *(resp.* $\mathsf{Dec}_k^{iv,a}(c) = m$ *then* $c \in \{\mathsf{Enc}_{k,s}^{n,a}(m)\}_{s\in\mathcal{S}}$ *(resp.* $c \in \{\mathsf{Enc}_{k,s}^{iv,a}(m)\}_{s\in\mathcal{S}}$*).*

According with this new definition, the ivE scheme Π which we have just used, presented in Fig. 7 is tidy, as it follows from a close inspection of the pseudocode provided, thus the nAE scheme $\boldsymbol{\Pi}$ is tidy.

We have also to redefine for stateful schemes all the notions presented in Sec. 2. We do it allowing the adversary *at the start of the game* to set the state of the scheme as he wishes.

8 Conclusion

In this paper we have studied four generic composition modes, N4, A10, A11 and A12, for building authenticated encryption for an encryption scheme and a PRF MAC. The security of these four modes was left open in previous works,

and three of them are the most efficient among the 180 possible modes based on these building blocks.

We have proved that mode N4 is not secure in general, and that modes A10, A11 and A12 have equivalent security. Moreover we have proved that if these four modes are instantiated with many common schemes (like CTR, OFB) they are all secure. Finally, we have showed that tidiness (again) and being stateless can have a decisive impact on security, as the application of A10, A11 and A12 on untidy or stateful modes can lead to insecure solutions.

Our analysis still leaves as an open problem to decide if modes A10, A11, and A12 are secure in general.

References

1. Vijayalakshmi Atluri, editor. *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002*. ACM, 2002.
2. Mihir Bellare, Oded Goldreich, and Anton Mityagin. The power of verification queries in message authentication and authenticated encryption. *IACR Cryptology ePrint Archive*, 2004:309, 2004.
3. Mihir Bellare and Sriram Keelveedhi. Authenticated and misuse-resistant encryption of key-dependent data. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 610–629. Springer, 2011.
4. Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Authenticated encryption in SSH: provably fixing the SSH binary packet protocol. In Atluri [1], pages 1–11.
5. Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the encode-then-encrypt-and-mac paradigm. *ACM Trans. Inf. Syst. Secur.*, 7(2):206–241, 2004.
6. Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Okamoto [27], pages 531–545.
7. Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In Okamoto [27], pages 317–330.
8. Dan J Bernstein. Caesar call for submissions, final, january 27 2014.
9. Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Ciphertext integrity with misuse and leakage: Definition and efficient constructions with symmetric primitives. In Jong Kim, Gail-Joon Ahn, Seungjoo Kim, Yongdae Kim, Javier López, and Taesoo Kim, editors, *Proceedings of the 2018 on Asia Conference on Computer and Communications Security, AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*, pages 37–50. ACM, 2018.
10. Francesco Berti, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. On leakage-resilient authenticated encryption with decryption leakages. *IACR Trans. Symmetric Cryptol.*, 2017(3):271–293, 2017.

11. Colin Boyd, Britta Hale, Stig Frode Mjølsnes, and Douglas Stebila. From stateless to stateful: Generic authentication and authenticated encryption constructions with application to TLS. 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 55–71. Springer, 2016.
12. Morris J Dworkin. Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac. Technical report, 2007.
13. Shay Gueron and Yehuda Lindell. GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte. In Ray et al. [31], pages 109–119.
14. IETF. The transport layer security (tls) protocol version 1.3 draft-ietf-tls-tls13-28. Technical report, 2018. https://tools.ietf.org/html/draft-ietf-tls-tls13-28.
15. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2014.
16. Jonathan Katz and Moti Yung. Unforgeable encryption and chosen ciphertext secure modes of operation. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 284–299. Springer, 2000.
17. Tadayoshi Kohno, Adriana Palacio, and John Black. Building secure cryptographic transforms, or how to encrypt and MAC. *IACR Cryptology ePrint Archive*, 2003:177, 2003.
18. Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is ssl?). In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 310–331. Springer, 2001.
19. Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.
20. Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.
21. David A. McGrew. An interface and algorithms for authenticated encryption. *RFC*, 5116:1–22, 2008.
22. Bart Mennink. Optimally secure tweakable blockciphers. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 428–448. Springer, 2015.
23. Atsushi Mitsuda and Tetsu Iwata. Tweakable pseudorandom permutation from generalized feistel structure. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *Provable Security, Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008. Proceedings*, volume 5324 of *Lecture Notes in Computer Science*, pages 22–37. Springer, 2008.

24. Yusuke Naito. Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. *IACR Trans. Symmetric Cryptol.*, 2017(2):1–26, 2017.
25. Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton. Reconsidering generic composition. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 257–274. Springer, 2014.
26. Yoav Nir and Adam Langley. Chacha20 and poly1305 for IETF protocols. *RFC*, 7539:1–45, 2015.
27. Tatsuaki Okamoto, editor. *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*. Springer, 2000.
28. Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton. Tag size does matter: Attacks and proofs for the TLS record protocol. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 372–389. Springer, 2011.
29. Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek. Leakage-resilient authentication and encryption from symmetric cryptographic primitives. In Ray et al. [31], pages 96–108.
30. Thomas Peyrin and Yannick Seurin. Counter-in-tweak: Authenticated encryption modes for tweakable block ciphers. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 33–63. Springer, 2016.
31. Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*. ACM, 2015.
32. Phillip Rogaway. Authenticated-encryption with associated-data. In Atluri [1], pages 98–107.
33. 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.
34. Phillip Rogaway. Nonce-based symmetric encryption. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*, pages 348–359. Springer, 2004.
35. 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.

36. Phillip Rogaway and Yusi Zhang. Simplifying game-based definitions - indistinguishability up to correctness and its application to stateful AE. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2018.

Supplementary material

A Detailed background

A.1 Pseudorandom functions (PRF)

For completeness we represent the PRF section, expanding them:

Definition 1. *A function* $\mathsf{F} : \mathcal{K} \times \mathcal{M} \longmapsto \mathcal{T}$ *is a* (q, t, ϵ)-pseudorandom function (PRF) *if for every* (q, t) *adversary* A*, the advantage :*

$$\mathsf{Adv}_{\mathsf{F}}^{PRF}(\mathsf{A}) := |\Pr[\,\mathsf{A}^{\mathsf{F}_k(\cdot)} \Rightarrow 1\,] - \Pr[\,\mathsf{A}^{\mathsf{f}(\cdot)} \Rightarrow 1\,]|$$

is upper bounded by ϵ *where* k *and* f *are chosen uniformly at random from their domains, namely* $\mathcal{K}$ *and the set of functions from* $\mathcal{M}$ *to* $\mathcal{T}$*,* $\mathcal{FUNC}(\mathcal{M}, \mathcal{T})$*.*
In a similar way, F *is a* pseudorandom permutation *(PRP) if* F_k *is a permutation and the above advantage is* ϵ *bounded when* f *is selected as a random permutation.*

We remind that a PRP is a PRF (see Propo. 3.27 [15]).

A function, which is PRF-secure is often the base which encryption schemes are based on (see, for example, [15]). To add more flexibility the notion of tweakable pseudorandom functions was introduced by Liskov et al. [20].

Definition 11. *[20] A tweakable pseudorandom function* $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \mathcal{M} \longmapsto \mathcal{T}$ *is* $(q, t, \epsilon) - TPRF$ *(*tweakable pseudorandom*)-secure if for every* $(q, t) - TPRF$ *-adversary* A *the advantage*

$$\mathsf{Adv}_{\mathsf{E}}^{TPRF}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{E}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathsf{f}(\cdot,\cdot)} \Rightarrow 1\right]\right|$$

is bounded by ϵ *for any* (q, t) *adversary.*
Here $\mathsf{f}(\cdot, \cdot)$ *is a random function, that is a function picked uniformly at random from the sets of all the functions having the same signature as* $\mathsf{E}_k(\cdot, \cdot)$*.*
If $\mathcal{M} = \mathcal{T}$ *and, for every* $k \in \mathcal{K}$ *and for every* $tw \in \mathcal{TW}$*, the function* $\mathsf{E}_k^{tw}(\cdot)$ *is a permutation,* E *is called a* (q, t, ϵ)-tweakable pseudorandom permutation (TPRP)*. In the advantage expression,* $\mathsf{f}(tw, \cdot)$ *is then selected as an independent random permutation on* $\mathcal{M}$ *for every value of* tw*.*

There are many ways to build a TPRF from a PRF (and a TPRP from a PRP), for example see [33], [23], [23], and [22] or directly [19], and [24].

A.2 Nonce-based Authenticated Encryption (nAE) schemes

Definition 12 ([25]). *A scheme for* nonce-based Authenticated Encryption *(*nAE*) is a triple* $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$*, where the keyspace* $\mathcal{K}$ *is a nonempty set, the encryption algorithm* AEnc *is a deterministic algorithm which takes as input the tuple* $(k, n, a, m) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$ *and outputs a string* $c \leftarrow \mathsf{AEnc}_k^{n,a}(m)$

called ciphertext.
The decryption algorithm ADec *is a deterministic algorithm which takes as input the tuple* $(k, n, a, c) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C}$ *and outputs* $m \leftarrow \mathsf{ADec}_k^{n,a}(c)$ *which is either a string* $m \in \mathcal{M}$ *or the symbol* $\perp$ *("invalid").*
We require that the algorithms AEnc *and* ADec *are the inverse of each other, that is:*

- (Correctness) *if* $\mathsf{AEnc}_k^{n,a}(m) = c$ *then* $\mathsf{ADec}_k^{n,a}(c) = m$
- (Tidiness) *if* $\mathsf{ADec}_k^{n,a}(c) = m \neq \perp$ *then* $\mathsf{AEnc}_k^{n,a}(m) = c$

If $\mathsf{ADec}_k^{n,a}(c) = \perp$ *we say that the algorithm* rejects c*, otherwise it* accepts c*.*
A sloppy nAE *scheme satisfies everything but the tidiness condition.*

Tidiness, as correctness, is usually seen as a syntactic requirement (for example Namprempre et al., [25]). Instead, in this paper, we show an explicit case where this property is fundamental to provide security (see Section 7.1).

Definition 13 ([25]). *A nonce-based authenticated encryption scheme* (nAE) $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ *is* $(q, t, \epsilon) - \mathsf{nAE}$-secure *if the advantage*

$$\mathsf{Adv}_{\boldsymbol{\Pi}}^{\mathsf{nAE}}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right] \right|$$

is bounded by ϵ *for every* (q, t)*-adversary.*
If the adversary A *queried the first (encryption) oracle on input* (n, a, m) *and he was answered* c*, the adversary* A *is not allowed to query the second (decryption) oracle on input* (n, a, c)*. Moreover the adversary* A *is not allowed to repeat the first component (the nonce) on different left oracle queries.*

If we want that the nAE scheme provides only privacy, we can use the following definition:

Definition 14. *A nonce-based authenticated encryption scheme* (nAE) $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* $(q, t, \epsilon) - \mathsf{nAE} - \mathsf{E}$-secure *if the advantage*

$$\mathsf{Adv}_{\boldsymbol{\Pi}}^{\mathsf{nAE}-\mathsf{E}}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1\right] \right|$$

is bounded by ϵ *for every* (q, t)*-adversary.*
The adversary A *is not allowed to repeat the first component (the nonce) on different oracle queries.*

In our paper, as in Namprempre et al. [25], to obtain an authenticated encryption scheme we combine an encryption scheme (either ivE or nE) and a MAC. We present now these constructions along with their security properties, after having introduced their key component, the PRFs.

A.3 Encryption schemes (nE and ivE)

Definition 15 ([25]). *A* nonce-based Encryption scheme (nE) *is a triple* $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$*, where the keyspace* $\mathcal{K}$ *is a non-empty set, the encryption algorithm* Enc *is a deterministic algorithm that takes as input the tuple* $(k, n, m) \in \mathcal{K} \times \mathcal{N} \times \mathcal{M}$ *and outputs a string* $c \leftarrow \mathsf{Enc}_k^n(m)$*.*
The decryption algorithm Dec *is a deterministic algorithm which takes as input the tuple* $(k, n, c) \in \mathcal{K} \times \mathcal{N} \times \mathcal{C}$ *and outputs either a string* $m \in \mathcal{M}$ *or the symbol* $\perp$ *("invalid").*
As for nAE *the properties of correctness and tidiness are required, making* Enc *and* Dec *one the inverse of the other, that is,* $\mathsf{Dec}_k^n(\mathsf{Enc}_k^n(m)) = m$ *and if* $\mathsf{Dec}_k^n(c) \neq \perp$, $\mathsf{Enc}_k^n(\mathsf{Dec}_k^n(c)) = c$*.*

We observe that an nAE scheme is an nE scheme: in fact it is enough to consider as the nonce $n' := (n \| a)$ and it is syntactically an nE scheme.

Definition 16. *A nonce-based encryption scheme* (nE) $\Pi := (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* $(q, t, \epsilon) -$ nE-secure *if the advantage*

$$\mathsf{Adv}_{\Pi}^{\mathsf{nE}}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\mathsf{Enc}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot)} \Rightarrow 1\right] \right|$$

is bounded by ϵ *for every* (q, t)*-adversary.*
The adversary A *is not allowed to repeat the first component (the nonce) on different oracle queries.*

If instead of a nonce, an iv is used, we have:

Definition 17 ([25]). *An* iv-based encryption scheme (ivE) *is a triple* $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$*, where the keyspace* $\mathcal{K}$ *is a non-empty set, the encryption algorithm* Enc *is a deterministic algorithm which takes as input the tuple* $(k, iv, m) \in \mathcal{K} \times \mathcal{IV} \times \mathcal{M}$ *and outputs the string* $c \leftarrow \mathsf{Enc}_k^{iv}(m)$*.*
The decryption algorithm Dec *is a deterministic algorithm which takes as input the tuple* $(k, iv, c) \in \mathcal{K} \times \mathcal{IV} \times \mathcal{C}$ *and outputs either a string* $m \in \mathcal{M}$ *or the symbol* $\perp$ *("invalid").*
As for nAE *and* nE*, the properties of correctness and tidiness are required, making* Enc *and* Dec *one the inverse of the other.*

The two Definitions 15 and 17 are semantically identical. However the security properties they aim are different. In fact:

Definition 18 ([35]). *An iv-based Encryption scheme* ivE $\Pi := \mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* $(q, t, \epsilon) -$ ivE-secure *if the advantage*

$$\mathsf{Adv}_{\Pi}^{\mathsf{ivE}}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\mathsf{Enc}_k^{\$}(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot)} \Rightarrow 1\right] \right|$$

is bounded by ϵ *for every* (q, t)*-adversary.*
Here the oracle $\mathsf{Enc}^{\$}(m)$ *first picks a random* $iv \leftarrow \mathcal{IV}$*, then it computes* $c \leftarrow \mathsf{Enc}_k(iv, m)$ *and it returns* (iv, c)*.*

We can observe that ivE-security implies nE security, because if the iv are picked uniformly at random, they are all different with overwhelming probability. The contrary does not hold, e.g. CTR (for details see Supp. Mat. G.1). The difference between ivE-security and nE-security is how the nonces or the ivs are treated, that is the nonce must be unique, while the iv must be randomly chosen.
When the only request is not to repeat the nonce, it is possible to allow the adversary to completely control the nonce, since it is efficiently checkable if the adversary respects the non-repeating property. This is not the case if it is necessary to check if the ivs are picked uniformly at random, so it is not possible to give the control of the ivs to the adversary.

A.4 Nonce(iv)-misuse

Naturally we may wonder what happens if we get rid of the requirements about the nonces or the ivs in Definitions 13, 16, 14 and 18. For certain schemes it is devastating. We have already observed that, if the ivs are not randomly picked, some iv-based encryption schemes may have problems, e.g. CTR and OFB (see Supp. Mat. G.1).
This can be the case even for nonce-based encryption schemes. In fact, if to an adversary A, who had asked the encryption of (n, m) receiving the ciphertext c, is given the ciphertext c' obtained as the encryption of (n, m'), the adversary A may recover m'. Examples of such Encryption schemes are given in Supp. Mat. G.1 for a fixed length scheme, that is, schemes that encrypt only messages of the same fixed length, or in Supp. Mat. G.2 for a various length scheme. We have called these schemes "message malleable" (Def. 9). Moreover, there are schemes, which are not message-malleable, but which are insecure if the nonces are repeated (for example, the scheme used in Sec. 4 or CBC).

However, it is possible to produce encryption schemes whose outputs look still completely random even if the nonces are repeated, provided that the nonces are not repeated with the same message. This security property (mrAE) was introduced by Rogaway and Shrimpton [35] for nonce-based Authenticated Encryption schemes nAE:

Definition 19 ([35]). *A nonce-based Authenticated Encryption scheme* (nAE) $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ *is* $(q, t, \epsilon) -$ mrAE-secure (misuse resistant) *if the advantage*

$$\mathsf{Adv}^{\mathsf{mrAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right|$$

is bounded by ϵ for every (q, t)-adversary.
If the adversary A *queried the first (encryption) oracle on input (n, a, m) obtaining c, he is not allowed to query the second (decryption) oracle on input (n, a, c).*

This is exactly Def. 13 where we have got rid of the hypothesis about the non-repeating of the nonces in encryption queries.

A similar notion can be given for nonce-based encryption scheme:

Definition 20. *A nonce-based encryption scheme* (nE) $\Pi := (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* $(q, t, \epsilon) -$ mrE-secure (misuse resistant) *if the advantage*

$$\mathsf{Adv}^{\mathsf{mrE}}_{\Pi}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{Enc}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot)} \Rightarrow 1\right]\right|$$

is bounded by ϵ *for every* (q, t)*-adversary.*

This is exactly Def. 16 where we have got rid of the hypothesis about the non-repeating of the nonces in encryption queries.

Clearly this security notion is stronger than the nE one, that is mrE implies nE (similarly mrAE implies nAE). In fact, in these two security definition we have got rid of the hypothesis that the nonce is a *nonce*, that is, it is never repeated. Such schemes are called *nonce misuse resistant* and there is a flourishing literature about them [30], [9], [10], [13], [3], and [35].

An nAE scheme may be mrE and not mrAE: consider an mrE scheme, for which the decryption algorithm gives, for invalid ciphertexts the key. The example is given in Sec. H.

A.5 The Chosen-Plaintext Attack(CPA) security

The ivE and the nE (and the $\mathsf{nAE} - \mathsf{E}$) notions implies the natural extention of CPA (Chosen-Plaintext Attack) security IV-based and nonce-based encryption:

Definition 21. *A nonce-based scheme* nE $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *is* $(q, t, \epsilon)-$CPA(Chosen Plaintext Attack)-secure *if the advantage*

$$\mathsf{Adv}^{\mathsf{CPA}}_{\Pi}(\mathsf{A}) := \left|\frac{1}{2} - \Pr\left[b' = b; b \xleftarrow{\$} \{0,1\},\ (\mathsf{st}, n, m_0, m_1) \leftarrow \mathsf{A}_1^{\mathsf{Enc}_k(\cdot,\cdot)},\right.\right.$$
$$\left.\left. c \leftarrow \mathsf{Enc}^n_k(m_b),\ b' \leftarrow \mathsf{A}_2^{\mathsf{Enc}_k(\cdot,\cdot)}(\mathsf{st}, c)\right]\right|$$

is bounded by ϵ *for every* (q, t) *adversary. The adversary* A *is composed by two algorithms* $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$*. The first algorithm* A_1*, after having queried its oracle* q_1 *times, outputs* st*, which is the information it wants to give to the second algorithm* A_2*, a nonce* n *and two messages* m_0 *and* m_1 *in* $\mathcal{M}$*, which have the same length* $|m_0| = |m_1|$*. The algorithm* A_1 *may not repeat the first component on different oracle queries. The nonce* n *in the output of adversary* A_1 *cannot be a nonce used in an oracle query.*
The algorithm A_2 *may ask at most* q_2 *oracle queries, provided that* $q_1 + q_2 \leq q$*.*

It may not repeat the first component on different oracle queries. Moreover it cannot use, as the first component of one of its queries, the nonce n output by algorithm A_1, or a nonce used in an oracle query by the first algorithm A_1 (that is, a nonce can never be repeated during the whole game).
The ciphertext $c \leftarrow \mathsf{Enc}_k(n, m_b)$ is called challenge ciphertext.

This is the CPA-definition of Katz and Lindell [15] tailored for nE schemes. There is a completely similar definition for ivE schemes. We have only to replace $\mathsf{Enc}_k(\cdot,\cdot)$ with $\mathsf{Enc}_k^{\$}(\cdot)$, and to change the $\$(\cdot,\cdot)$ oracle accordingly. Similarly there is a similar notions for nAE schemes, obtained from the previous one by replacing $\mathsf{Enc}_k(\cdot,\cdot)$ with $\mathsf{AEnc}_k(\cdot,\cdot,\cdot)$ and changing $\$(\cdot,\cdot,\cdot)$ accordingly. The CPA security of ivE corresponds to the usual CPA security notion when the encryption is made probabilistic: it picks itself the random IV.

The nE (and the ivE) security implies the CPA-security since after having replaced the encryption Enc algorithm with \$ it is not possible to guess better than with a random guess what plaintext the challenge ciphertext encrypts. Thus, we have proved the following:

Proposition 7. *Let $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ be a $(q, t, \epsilon_{\mathsf{nE}})-\mathsf{nE}$ secure (r. $(q, t, \epsilon_{\mathsf{ivE}})-\mathsf{ivE}$) encryption scheme. Then Π is $(q-1, t, \epsilon_{\mathsf{nE}})-\mathsf{CPA}$ secure (r. $(q-1, t, \epsilon_{\mathsf{ivE}})-\mathsf{CPA}$ secure).*

On the other hand, the nE (r. ivE) security is stronger. In fact, given the nE (r. ivE) CPA-secure scheme $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$, then the nE (r. ivE) scheme $\Pi' = (\mathcal{K}, \mathsf{Enc}', \mathsf{Dec}')$, defined by $\mathsf{Enc}'_k(n, m) := \mathsf{Enc}_k(n, m)\|1$ (r. $\mathsf{Enc}'_k(iv, m) := \mathsf{Enc}_k(iv, m)\|1$), is as CPA secure as Π, but it is not nE (r. ivE) secure since the last bit of every ciphertext is 1 (and not random).

There is also a version of the CPA security, where, instead of having a single ciphertext c which is either the encryption of (n, m_0) or (n, m_1) (with $|m_0| = |m_1|$), the adversary A has multiple ciphertexts c^i which are either all the encryptions of (n^i, m_0^i) or all the encryptions of (n^i, m_1^i) (as usual with $|m_0^i| = |m_1^i|$). Thus we have the following definition, which we have already introduced:

Definition 5. *A nonce-based Encryption scheme nE $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ is (q, t, ϵ)-mCPA secure, or (q, t, ϵ)-secure against chosen plaintext attacks for multiple encryptions, if:*

$$\mathsf{Adv}^{\mathsf{mCPA}}_{\Pi}(\mathsf{A}) := \left| \frac{1}{2} - \Pr\left[b' = b; b \leftarrow \{0,1\},\ b' \leftarrow \mathsf{A}^{\mathsf{Enc}_k^b(\cdot,\cdot,\cdot)} \right] \right|$$

is bounded by ϵ for any (q, t)-adversary. Here the oracle $\mathsf{Enc}_k^b(\cdot,\cdot,\cdot)$ is an oracle, which on input $(n, m_0, m_1) \in \mathcal{N} \times \mathcal{M}^2$ outputs $c \leftarrow \mathsf{Enc}_k(n, m_b)$ for a random secret bit $b \leftarrow \{0, 1\}$, which the oracle has picked at the start of the game. When the adversary A queries $\mathsf{Enc}_k^b(\cdot,\cdot,\cdot)$, he must choose two messages m_0 and m_1 s.t. $|m_0| = |m_1|$. Moreover he cannot repeat the first input (the nonce) in different queries.

This is the $\mathsf{IND-CPA}$ of Bellare and Namprempre [6] tailored for nE schemes. We observe that the mCPA-security is a generalization of the CPA-security because the adversary A can use the oracle $\mathsf{Enc}_k^b(\cdot,\cdot,\cdot)$ to emulate the oracle $\mathsf{Enc}_k(\cdot,\cdot)$ simply asking (n,m,m) (in fact, in that case the answer will be $c \leftarrow \mathsf{Enc}_k(n,m)$ independently of the value of b).
An analogous definition exists for ivE encryption schemes.
As already stated, the security properties mCPA and CPA are equivalent. In fact:

Theorem 1. *Let $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ be a nonce-based encryption scheme nE which is $(q-1,t,\epsilon)$-CPA-secure. Then the scheme is $(q,t,2(q-1)\epsilon)-\mathsf{mCPA}$-secure.*

The proof, inspired by the proof of an analogous theorem (Theorem 11.6 for Public Key Encryption schemes in Katz and Lindell [15]) can be found in the following section (Supp. Mat. A.6).
An analogous statement exists for ivE encryption schemes.
The adversaries against the mCPA security need to have one more oracle query then the adversaries against the CPA security they are reduced to, because the CPA adversaries obtain for free the ciphertext $c \leftarrow \mathsf{Enc}_k(n,m_b)$.

A.6 Proof of Theorem 1

We want to prove here that the mCPA (Chosen Plaintext for multiple encryptions) security is equivalent to the CPA security. We remind the theorem we stated in Sec. 2.5 and in Supp. Mat. A.5.

Theorem 1. *Let $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ be a nonce-based encryption scheme nE which is $(q-1,t,\epsilon)$-CPA-secure. Then the scheme is $(q,t,2(q-1)\epsilon)-\mathsf{mCPA}$-secure.*

The proof, inspired by the proof of an analogous theorem (Theorem 11.6 for Public Key Encryption schemes in Katz and Lindell [15]).

Proof. Let A be a $(q,t)-\mathsf{mCPA}$ adversary who asks the q queries (n^i, m_0^i, m_1^i) for $i = 1, ..., q$ during the game.
To prove the equivalence we use a sequence of $q+1$ games and q $(q-1,t)-\mathsf{CPA}$ adversaries to do the transition between this games.

Game 0 Let Game 0 be the game where the oracle $\mathsf{Enc}_k^b(\cdot,\cdot)$ answers always $\mathsf{Enc}_k(n^i, m_0^i)$. This happens in the normal mCPA game when $b = 0$. At the end of the game the adversary outputs a bit. Let E_0 be the probability that at the end of the game the adversary outputs 1 (if he is an mCPA adversary, he looses).

Game j Let Game j be the game where the oracle $\mathsf{Enc}_k^b(\cdot,\cdot)$ answers $\mathsf{Enc}_k(n^i, m_1^i)$ for the first j queries (that is $i \leq j$) and $\mathsf{Enc}_k(n^i, m_0^i)$ for the remaining $q-j$ queries. At the end of the game the adversary outputs a bit. Let E_j be the probability that at the end of the game the adversary outputs 1.

Game q Let Game 0 be the game where the oracle $\mathsf{Enc}_k^b(\cdot,\cdot)$ always answers $\mathsf{Enc}_k(n^i, m_1^i)$. This happens in the normal mCPA game when $b = 1$. At the end of the game the adversary outputs a bit. Let E_0 be the probability that at the end of the game the adversary outputs 1 (if he is an mCPA adversary, he wins).

Transition from Game j to Game j + 1 To do the transition from Game j to Game $j+1$ we use a $(q-1,t)-\mathsf{CPA}$ adversary A_j based on the mCPA adversary A. At the start of the Game a random bit $b \xleftarrow{\$}$ is computed. For the first j queries when the mCPA adversaries queries his oracle on input (n^i, m_0^i, m_1^i), $i \leq j$, the algorithm $\mathsf{A}_{j,0}$ queries his oracle $\mathsf{Enc}_k(\cdot,\cdot)$ on input (n^i, m_0^i) receiving c^i which is forwarded to the adversary A.
For the $j+1$ query $(n^{j+1}, m_0^{j+1}, m_1^{j+1})$ the algorithm $\mathsf{A}_{j,0}$ outputs $(n^{j+1}, m_0^{j+1}, m_1^{j+1})$ (He does not give any information to algorithm $\mathsf{A}_{j,1}$). Then $c \leftarrow \mathsf{Enc}_k(n^i, m_b^j)$ is computed and it is given to the algorithm $\mathsf{A}_{j,1}$ (along with no information due to the choice of $\mathsf{A}_{j,0}$). The algorithm $\mathsf{A}_{j,1}$ forwards c to the mCPA adversary.
For the last $q-j-1$ queries when the mCPA adversaries queries his oracle on input (n^i, m_0^i, m_1^i), $j < i \leq q$, the algorithm $\mathsf{A}_{j,1}$ queries his oracle $\mathsf{Enc}_k(\cdot,\cdot)$ on input (n^i, m_1^i) receiving c^i which is forwarded to the adversary A.
At the end of the game the mCPA adversary outputs a bit b' which is sent to the algorithm $\mathsf{A}_{j,1}$. The algorithm $\mathsf{A}_{j,1}$ outputs this bit as his guess.
When the bit $b = 0$ the CPA adversary A_j is playing Game j, otherwise he is playing Game $j+1$.

Bound between $\Pr[E_j]$ *and* $\Pr[E_{j+1}]$ We have now to bound $|\Pr[E_j] - \Pr[E_{j+1}]|$. We observe that

$$\Pr[\mathsf{A}_j \text{ wins the } \mathsf{CPA} \text{ Game}] = \Pr[\overline{E_j}|b=0]\Pr[b=0] + \Pr[E_{j+1}|b=1]\Pr[b=1] = \frac{\Pr[\overline{E_j}] + \Pr[E_{j+1}]}{2}$$

Since the nE scheme Π is $(q-1,t,\epsilon)-\mathsf{CPA}$-secure and A_j is a $(q-1,t)-\mathsf{CPA}$ adversary, the probability he wins is bounded by $\frac{1}{2}+\epsilon$. Thus

$$\frac{\Pr[\overline{E_j}] + \Pr[E_{j+1}]}{2} = \frac{1 - \Pr[E_j] + \Pr[E_{j+1}]}{2} \leq \frac{1}{2} + \epsilon$$

$$|\Pr[E_{j+1}] - \Pr[E_j]| \leq 2\epsilon$$

Bound between $\Pr[E_0]$ *and* $\Pr[E_q]$ Now we are able to bound $|\Pr[E_0] - \Pr[E_q]$. It is simply bounded by

$$|\Pr[E_0] - \Pr[E_q]| \leq \sum_{i=0}^{q-1} |\Pr[E_{j+1}] - \Pr[E_j]| = 2(q-1)\epsilon$$

Now we observe that Game 0 simulates correctly the mCPA Game when the secret bit $b = 0$, while Game q simulates correctly the mCPA Game when the secret bit $b = 1$. Thus

$$\Pr[b = b';\ b' \leftarrow \mathsf{A}] = \Pr[\overline{E_0}|b=0]\Pr[b=0] + \Pr[E_q|b=1]\Pr[b=1] =$$

$$\frac{1-\Pr[E_0]+\Pr[E_q]}{2} = \frac{1}{2} + \Pr[E_q] - \Pr[E_0] \leq \frac{1}{2} + 2(q-1)\epsilon$$

which concludes the proof.

A.7 Ciphertext-Integrity

For sake of completeness we give the different definitions of ciphertext integrity present in the literature and we prove the relations among them.

Definition 22. *A nonce-based authenticated encryption scheme* nAE $\boldsymbol{\Pi} = (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ *is* $(q+1, t, \epsilon) - \mathsf{INT\text{-}CTXT}$(Ciphertext integrity)-secure *if*

$$\mathsf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right|$$

is bounded by ϵ *for every* (q, t) *adversary. The adversary* A *is not allowed to query its second oracle on input* (n, a, c) *if he received* c *as answer* $c \leftarrow \mathsf{AEnc}_k(n, a, m)$ *to a certain input* (n, a, m) *that he asked to its first oracle. Moreover the adversary is not allowed to repeat the first component (the nonce) on different queries to the first oracle.*

Since the goal of authenticated encryption is to provide both privacy and authenticity it is normal to expect that if an nAE scheme $\boldsymbol{\Pi} = (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ provides both privacy ($\mathsf{nAE}-\mathsf{E}$, Def. 14) and authenticity ($\mathsf{INT\text{-}CTXT}$, Def. 22), it is nAE-secure. This is the case. In fact, for any adversary A:

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{nAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| = \\
\left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right] + \right. \\
\left. \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| \leq \\
\left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| + \\
\left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right| \leq \\
\mathsf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\boldsymbol{\Pi}}(\mathsf{A}) + \mathsf{Adv}^{\mathsf{nAE}-\mathsf{E}}_{\boldsymbol{\Pi}}(\mathsf{A})
\end{aligned}$$

(in the last inequality, the bound of the second absolute modulus is based on the fact that the oracle $\perp(\cdot,\cdot,\cdot)$ is easily emulated by anyone).

Thus we have proved the following theorem:

Theorem 2. *Let* $\boldsymbol{\Pi}$ *be an* nAE *scheme which is* $(q, t, \epsilon_{\mathsf{nAE}-\mathsf{E}}) - \mathsf{nAE}-\mathsf{E}$ *secure and* $(q, t, \epsilon_{\mathsf{INT\text{-}CTXT}}) - \mathsf{INT\text{-}CTXT}$ *secure. Then* $\boldsymbol{\Pi}$ *is* $(q, t, \epsilon_{\mathsf{nAE}}) - \mathsf{nAE}$ *secure where* $\epsilon_{\mathsf{nAE}} = \epsilon_{\mathsf{nAE}-\mathsf{E}} + \epsilon_{\mathsf{INT\text{-}CTXT}}$.

Often, in the literature [6], this definition is presented in an equivalent way where the adversary try to forge a fresh valid ciphertext. To arrive to this we have to pass through this second definition $\mathsf{INT\text{-}CTXT1}$, where the adversary is allowed to do only one *decryption query* (query to the second oracle):

Definition 23. *A nonce-based authenticated encryption scheme* $\mathsf{nAE}\ \boldsymbol{\Pi} = (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$ *is* $(q+1, t, \epsilon) - \mathsf{INT\text{-}CTXT1v2}$(Ciphertext integrity with only 1 decryption query [version 2])-secure *if*

$$\mathsf{Adv}^{\mathsf{INT\text{-}CTXT1}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]\right|$$

is bounded by ϵ *for every* (q, t) *adversary. Here the oracle* $\perp(\cdot,\cdot,\cdot)$ *always answers* $\perp$*. The adversary* A *is not allowed to query its second oracle on input* (n, a, c) *if he received* c *as answer* $c \leftarrow \mathsf{AEnc}_k(n, a, m)$ *to a certain input* (n, a, m) *that he asked to its first oracle. Moreover the adversary is not allowed to repeat the first component (the nonce) on different queries to the first oracle. Furthermore he is allowed to query the second oracle only once.*

The two previous notions of authenticity can be easily related. In fact, clearly if an nAE scheme $\boldsymbol{\Pi}$ is $(q, t, \epsilon) - \mathsf{INT\text{-}CTXT}$ secure, it is $(q, t, \epsilon) - \mathsf{INT\text{-}CTXT1v2}$ secure. For the converse the following proposition holds

Proposition 8. *Let* $\boldsymbol{\Pi}$ *be a* $(q, t, \epsilon) - \mathsf{INT\text{-}CTXT1v2}$ *secure* nAE *scheme. Then it is* $(q, t, q\epsilon) - \mathsf{INT\text{-}CTXT}$ *secure.*

Before proving it, we consider the following Lemma, which shows one of the best strategy for any adversary to maximize the $\mathsf{INT\text{-}CTXT}$ advantage:

Lemma 2. *Let* $\boldsymbol{\Pi} = (\mathcal{K}, \mathsf{AEnc}, Dec)$ *be an* nAE *scheme. Let* A *be a* $(q, t) - \mathsf{INT\text{-}CTXT}$ *adversary. Let* B *be the* $(q+1, t) - \mathsf{INT\text{-}CTXT}$ *adversary based on* A *in this way: he makes the same encryption and decryption queries as* A*, but he outputs* 1 *iff at least one decryption query is valid (that is,* $\neq\perp$*). Then,* $\mathsf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\boldsymbol{\Pi}}(\mathsf{A}) \leq \mathsf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\boldsymbol{\Pi}}(\mathsf{B})$.

Proof. Let event B be the event that at least one of the decryption queries made by A is valid, that is

$$B := [\exists j \in \{1, ..., q\}\ s.t.\ \perp \neq m^j \mathsf{ADec}_k(n^j, a^j, c^j); (n^j, a^j, c^j) \leftarrow \mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}\setminus\perp(\cdot,\cdot,\cdot)}]$$

The event B does not depend if A has access to the ADec or the $\perp$ oracle, because the $\perp$ oracle is behaving correctly until the first valid decryption query made by A. But, when this happens, event B is already happened, so the fact that $\perp$ is no longer correct does not change the fact that event B has happened or not. We observe that for A

$$\begin{aligned}
\mathsf{A}^{\mathsf{INT\text{-}CTXT}}_{\boldsymbol{\Pi}}(\mathsf{A}) &= \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \\
&= \Big|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] + \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}] \\
&\quad - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B]\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}]\Big| =
\end{aligned}$$

since if event B does not happen, the oracle $\perp$ answers correctly

$$= \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B]\right|$$

On the other hand, for B

$$\begin{aligned}\mathsf{A}_{\boldsymbol{\Pi}}^{\mathsf{INT\text{-}CTXT}}(\mathsf{B}) = \Big|&\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] + \Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}] \\ &- \Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B]\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}]\Big| \\ &\text{by construction of } \mathsf{B} \\ =&\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] = \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] = \Pr[B]\end{aligned}$$

since B asks the same queries as A and outputs 1 iff one of his decryption queries is valid (this may never happen if B has access to the $\perp$ oracle instead of the ADec one.
Thus

$$\begin{aligned}\mathsf{A}_{\boldsymbol{\Pi}}^{\mathsf{INT\text{-}CTXT}}(\mathsf{A}) &= \Big|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B] - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1|B]\Pr[B]\Big| \\ &\leq \Pr[B] = \mathsf{A}_{\boldsymbol{\Pi}}^{\mathsf{INT\text{-}CTXT}}(\mathsf{B})\end{aligned}$$

which concludes the proof.

Now we can prove Prop. 8. The proof is a standard proof where the adversary guesses what decryption query made by A is the correct one.

Proof. Let A be a $(q,t) - \mathsf{INT\text{-}CTXT}$ adversary against scheme $\boldsymbol{\Pi}$, we suppose that he outputs 1 iff he receives one answer for a decryption query different from invalid ($\perp$) [As we have seen (Lem. 2) this is one of the best strategy]. We build a $(q,t) - \mathsf{INT\text{-}CTXT1v2}$ adversary B based on him. The $\mathsf{INT\text{-}CTXT1v2}$ adversary B picks a random number i_g in $\{1,...,q\}$. When A asks an encryption query on input (n^i, a^i, m^i) he asks the same query to his oracle, receiving c^i which he forwards to A. When A asks a decryption query (n^i, a^i, c^i) he simply sees if $i = i_g$. If it is the case, he asks this as his only decryption query and forwards the answer to A; otherwise he answers $\perp$ to the query made by A. At the end of the game, B outputs the bit b that A has output. With probability at least q^{-1} the $\mathsf{INT\text{-}CTXT1v2}$ adversary guesses the first valid decryption query made by the $\mathsf{INT\text{-}CTXT}$ adversary A if A has made at least a valid decryption query. Thus

$$\epsilon \geq \Pr[\mathsf{B}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1] \geq \Pr[i_g \text{ correct }]\Pr[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1]$$

Thus $\Pr[\mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot),\mathsf{ADec}_k(\cdot,\cdot,\cdot)} \Rightarrow 1] \leq q\epsilon$.
This concludes our proof since neither A nor B outputs 1 when they are facing the $\perp(\cdot,\cdot,\cdot)$ oracle instead of $\mathsf{ADec}_k(\cdot,\cdot,\cdot)$ by construction.

This bound in general is tight, that is, there exists at least a scheme for which the equality in the bound holds.

Without loss of generality we may suppose that the decryption query is the last query made by the $\mathsf{INT\text{-}CTXT1v2}$ adversary. In fact the following proposition holds

Proposition 9. *Let* $\boldsymbol{\Pi}$ *be a* $(q, t, \epsilon) -$ INT-CTXT1v2 *secure* nAE *scheme. If we restrict the* INT-CTXT1v2 *adversaries to ask the decryption query as their last one, the bound does not change.*

Proof. We observe that since by our hypothesis on the behaviour of A (Lem. 2), what happens after A has asked is decryption query does not change his output bit. This concludes the proof.

The previous proposition leads to the following definition of INT-CTXT1 presented by Bellare and Namprempre, which is equivalent to the single query version of the strong unforgeability of Bellare et al. [2], which we stated in Sec. 2.6:

Definition 6. *A nonce-based authenticated encryption scheme* nAE $\boldsymbol{\Pi} = (\mathcal{K},$ AEnc, ADec*) is* (q, t, ϵ)-INT-CTXT1(Ciphertext integrity with only 1 decryption query)-secure *if*

$$\mathsf{Adv}^{\mathsf{INT\text{-}CTXT1}}_{\boldsymbol{\Pi}}(\mathsf{A}) := \Pr\left[\perp \neq m^* \leftarrow \mathsf{ADec}_k(n^*, a^*, c^*);\ (n^*, a^*, c^*) \leftarrow \mathsf{A}^{\mathsf{AEnc}_k(\cdot,\cdot,\cdot)}\right]$$

is bounded by ϵ *for every* (q, t) *adversary. The adversary* A *is not allowed to repeat the first component (the nonce) on different oracle queries. Moreover he is not allowed to output* (n^*, a^*, c^*) *if he received* c^* *as* $c^* \leftarrow \mathsf{AEnc}_k(n^*, a^*, m^*)$ *for a certain input* (n^*, a^*, m^*) *that he asked to the first oracle.*

The two definitions INT-CTXT1v2 and INT-CTXT1 are clearly equivalent due to the previous proposition (because outputting 1 only when his decryption query is valid is the best strategy to maximize the advantage). There is one less encryption query, because the decryption query of Def. 23 is given for free here.

Usually, for simplicity, we denote the advantage used in Def. 6 as

$$\Pr[\mathsf{A}^{\mathsf{Enc}} \text{ wins }].$$

A.8 Stateful schemes

Stateful schemes uses an additional input: the state s. This input is set at the start of the game and it is updated in every query.

Definition 24 ([36]). *A scheme for* stateful nonce-based Authenticated Encryption *(*snAE*) is a triple* $\boldsymbol{\Pi} := (\mathcal{K}, \mathsf{AEnc}, \mathsf{ADec})$*, where the keyspace* $\mathcal{K}$ *is a nonempty set, the encryption algorithm* AEnc *is a deterministic algorithm which takes as input the tuple* $(k, s, n, a, m) \in \mathcal{K} \times \mathcal{S} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$ *and outputs a string* $c \leftarrow \mathsf{AEnc}^{n,a}_{k,s}(m)$ *called ciphertext. Moreover a new state* s' *is computed and kept in memory.*
The decryption algorithm ADec *is a deterministic algorithm which takes as input the tuple* $(k, s, n, a, c) \in \mathcal{K} \times \mathcal{S} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C}$ *and outputs* $m \leftarrow \mathsf{ADec}^{n,a}_{k,s}(c)$ *which is either a string* $m \in \mathcal{M}$ *or the symbol* $\perp$ *("invalid"). Moreover a new state* s' *is computed and kept in memory.*

We require that the algorithms AEnc *and* ADec *are the inverse of each other, that is:*

– (Correctness) *if* $\mathsf{AEnc}_{k,s}^{n,a}(m) = c$ *then* $\mathsf{ADec}_{k,s}^{n,a}(c) = m$
– (Tidiness) *if* $\mathsf{ADec}_{k,s}^{n,a}(c) = m \neq \perp$ *then* $\mathsf{AEnc}_{k,s}^{n,a}(m) = c$

If $\mathsf{ADec}_{k,s}^{n,a}(c) = \perp$ *we say that the algorithm* rejects c*, otherwise it* accepts c*.*
A sloppy snAE *scheme satisfies everything but the tidiness condition.*

For the security, we have to choose if we allow reorderings, omissions and replays in the decryption queries. This problem was studied in detail by Rogaway and Zhang [36]. Since we only use a stateless decryption algorithm, (level L_0 of [36]), we allow everything in decryption.

For security notions, we decide to allow the adversary to choose at the start of the game the state of the encryption algorithm. The rest is equivalent.

A.9 Message Authentication Code (MAC)

We define a deterministic notion of Message Authentication Code (MAC) since we are not interested in probabilistic ones (see Katz and Lindell [15] for further details about probabilistic MACs, in particular for their definitions and security properties).

Definition 7. *A* Message Authentication Code MAC *is a triple* $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *where the keyspace* $\mathcal{K}$ *is a non-empty set, the tag-generation algorithm* Mac *is a deterministic algorithm that takes as input the couple* $(k, m) \in \mathcal{K} \times \mathcal{M}$ *and outputs the tag* $\tau \leftarrow \mathsf{Mac}_k(m)$ *from the tag space* $\mathcal{T}$*. The verification algorithm* Vrfy *takes as input a triple* (k, m, τ) *in* $\mathcal{K} \times \mathcal{M} \times \mathcal{T}$ *and outputs* $\top$ *(accept) or* $\perp$ *(reject). We ask that* $\mathsf{Vrfy}(k, m, \mathsf{Mac}(k, m)) = \top$*.*
A string-input MAC strMAC *has as input space a set of strings, that is* $\mathcal{M} \subseteq \{0,1\}^*$*.*
A vector-input MAC vecMAC *has as input space* $\mathcal{M}$ *which has one or more component and it can accept tuples of strings as input.*

Usually the security for MACs is given by the unforgeability security notion. We start presenting the $\mathsf{MAC} - \mathsf{forge}$ experiment:

Definition 25 ([15]). *Given a* MAC $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *and a* (q, t)*-adversary* A*, the* $\mathsf{MAC} - \mathsf{forge}_{\Pi}^{\mathsf{A}}$ *experiment is run in this way:*

1. *A random key* k *is picked uniformly at random* $k \leftarrow \mathcal{K}$*.*
2. *The adversary* A *is given access to* $\mathsf{Mac}_k(\cdot)$*. He can do at most* q *queries to this oracle. He outputs a couple* (m, τ)*. Let* $\mathcal{Q}$ *denote the set of all queries that* A *asked to its oracle.*
3. *The output of the experiment is* 1 *iff* $\mathsf{Vrfy}_k(m, \tau) = \top$ *and* $m \notin \mathcal{Q}$*; otherwise, the output is 0.*

The probability that the adversary A wins the previous experiment, gives birth to the following definition:

Definition 26 ([15]). *A* MAC $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *is* (q, t, ϵ)-unforgeable-*secure if for every* (q, t)-*adversary* A

$$\Pr\left[\mathsf{MAC} - \mathsf{forge}_{\Pi}^{\mathsf{A}} = 1\right] \leq \epsilon$$

However, in our paper as already stated, we need this stronger notion of security:

Definition 8. *([25])* *A* MAC $\Pi = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ *is* $(q, t, \epsilon) - \mathrm{PRF}$-*secure if*

$$\mathsf{Adv}_{\Pi}^{PRF}(\mathsf{A}) := \mathsf{Adv}_{\mathsf{Mac}}^{PRF}(\mathsf{B})$$

is bounded by ϵ *for any* (q, t) *adversary* B *and if* $\mathsf{Vrfy}(k, m, \mathsf{Mac}(k, m)) = \top$ *iff* $\tau = \mathsf{Mac}(k, m)$.

In reality we are simply asking that the Mac algorithm is implemented with a PRF (Def. 1).
This notion is stronger because if a MAC is $(q, t, \epsilon) - \mathrm{PRF}$-secure it is $(q, t, \epsilon + |\mathcal{T}|^{-1})$-unforgeable. (A proof of this can be found in Theorem 4.4 [15]).

The unforgeability is not equivalent to the PRF security. As an example consider a MAC scheme $\mathsf{MAC} = (\mathcal{K}, \mathsf{Mac}, \mathsf{Vrfy})$ which is PRF-secure (thus unforgeable). Now we build the MAC scheme $\mathsf{MAC}' = (\mathcal{K}, \mathsf{Mac}', \mathsf{Vrfy}')$, where $\mathsf{Mac}'_k(m) := (\mathsf{Mac}_k(m) \| 1)$. Clearly MAC' is as unforgeable as MAC, because an adversary A' able to forge this scheme is easily reduced to an adversary A able to forge MAC, but it is no more PRF-secure, since the last bit of the output of $\mathsf{Mac}'_k(\cdot)$ is easily predictable.

A.10 Hash functions

We also need hash functions:

Definition 27 ([15]). *An* hash function *is a pair of probabilistic polynomial-time algorithms* $\mathsf{H} = (\mathsf{Gen}, \mathsf{Map})$, *where*

- Gen *is a probabilistic algorithm which outputs a key* $s \leftarrow \mathcal{S}$ *picked uniformly at random*
- $\mathsf{Map} : \{0,1\}^* \longmapsto \mathcal{H}$

The hash functions which are used in practice have the target space $\mathcal{H}$ which is much more little than the input space $\{0,1\}^*$. On the other hand, it should be difficult to find a collision for them, thus their security property is:

Definition 28. *A* $(0, t, \epsilon_{\mathsf{cr}})$-collision resistant hash function $\mathsf{H} : \mathcal{S} \times \{0,1\}^* \to \mathcal{H}$ *is a function that is such that, for every* $(0, t)$-*bounded adversary* A, *the probability that* $\mathsf{A}(s)$ *outputs a pair of distinct messages* $(m_0, m_1) \in \{0,1\}^*$ *such that* $\mathsf{Map}_s(m_0) = \mathsf{Map}_s(m_1)$ *is bounded by* ϵ_{cr}, *where* s *is selected uniformly at random.*

We would like to observe that the key of the hash function is given to the adversary. There is no need to keep it secret. Thus, and to make the notation easier, we will omit the key for hash functions.

B Knowledge-of-Tag

We present here the Knowledge-of-Tag (KoT) security definition, which was used by Namprempre et al. [25] to prove that modes A10, A11 and A12 are secure if the encryption scheme is KoT secure. We use the same formalism as Namprempre et al. [25].
We use a plaintext extractor (Ext), that is, an algorithm that takes as input all the inputs explicitly available to the forging adversary and outputs a string. The forger wins if he is able to produce a new forgery which uses an old iv^i and old couple $m^j \| \tau^j$ for which he does not know τ^j and the extractor fails to determine this $m^j \| \tau^j$. Moreover he can ask to reveal some tag used (which he is not allowed to reuse if he wants to win the game). The idea is that if the forger wins the KoT game he is able to do so without any (extractable) knowledge of the tag τ^i (see pag. 26 [25]).
The details of the game are presented in Tab. 1.

Definition 29. *Let $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ be an iv-based encryption scheme, let Ext be a plaintext extractor, Tag_{sel} be a tag-input selection function.*
The ivE *scheme Π is $(q, t, \epsilon_{KoT}) - \mathsf{KoT}_{\mathsf{Ext},\mathsf{Tag}_{sel},\tau}$-*secure *if for every $(q,t) - \mathsf{KoT}$-adversary the advantage*

$$\mathsf{Adv}^{\mathsf{KoT}}_{\mathsf{Enc},\mathsf{Ext},\mathsf{Tag}_{sel},\tau}(\mathsf{A}) := \Pr[\mathsf{KoT}_{\mathsf{Enc},\mathsf{Ext},\mathsf{Tag}_{sel},\tau}(\mathsf{A}) = 1]$$

is bounded by ϵ_{KoT}.

$\mathsf{KoT}_{\mathsf{Enc},\mathsf{Ext},\mathsf{Tag}_{sel},\tau}(\mathsf{A})$ experiment		

$\mathsf{KoT}_{\mathsf{Enc},\mathsf{Ext},\mathsf{Tag}_{sel},\tau}(\mathsf{A})$:
 	
$i = 0; win = 0$
$k \leftarrow \mathcal{K}$
Run $\mathsf{A}^{\mathsf{Enc},\mathsf{Reveal},\mathsf{Test}}$
Return win
	Oracle $\mathsf{Enc}(n, a, m)$:
	
	$i = i + 1$
	$(n^i, a^i, m^i) = (n, a, m)$
	$iv^i \leftarrow \mathcal{IV}$
	$s^i \leftarrow \mathsf{Tag}_{sel}(n^i, a^i, m^i)$
	if $\mathsf{Tag}[s^i] = \perp$ then
	$\mathsf{Tag}[s^i] \leftarrow \mathcal{T}$
	$\tau[s^i] = \mathsf{Tag}[s^i]$
	$x^i = m^i \| \tau^i$
	$c^i \leftarrow \mathsf{Enc}_k(iv^i, x^i)$
	$\mathcal{Q} = \mathcal{Q} \cup \{(i, iv^i, m^i, c^i)\}$
	Return (iv^i, c^i)
		Oracle $\mathsf{Test}(j^*, c^*)$:
		
		$x \leftarrow \mathsf{Ext}(j^*, c^*, \mathcal{Q}, \mathcal{TAG})$
		$valid = xgood = 0$
		if $\exists x^i$ s.t.:
		1) $c^* = \mathsf{Enc}_k(iv^{j^*}, x^i)$ and
		2) $(\cdot, \tau^i) \in \mathcal{TAG}$ and
		3) $x^i = x^j$
		then
		$valid = 1$
		if $x = x^i$ then $xgood = 1$
		if $valid \wedge \neg xgood$ then
		$win = 1$
		Return 1
		Return 0

	Oracle$\mathsf{Reveal}(j)$: $\mathcal{TAG} = \mathcal{TAG} \cup \{(j, \tau^j)\}$ Return τ^j	

Table 1. The Knowledge-of-Tag (KoT) experiment

C Allowing the vecMACs to share their key

Namprempre et al. [25] allowed the two vecMACs $\mathsf{MAC}^{\mathsf{IV}}$ and $\mathsf{MAC}^{\mathsf{Tag}}$ to share the same key k_M. They did it for practice. Here we want to discuss why this choice does not harm the security of the mode. For this, as Namprempre et al. [25], we suppose that for any couple of vecMACs $(\mathsf{MAC}^{\mathsf{IV}}, \mathsf{MAC}^{\mathsf{Tag}})$, used to instantiate the scheme $\boldsymbol{\Pi}$ according to the modes A10, A11 and A12, their tag generation functions $(\mathsf{Mac}^{\mathsf{IV}}, \mathsf{Mac}^{\mathsf{Tag}})$, can be derived from an underlying PRF Mac.
This is formalized with :

Definition 30 ([25]). *Given two* vecMAC $\mathsf{MAC}^1 = (\mathcal{K}, \mathsf{Mac}^1, \mathsf{Vrfy}^1)$*, with* $\mathsf{Mac}^1 : \mathcal{K} \times \mathcal{M}^1 \longmapsto \mathcal{T}^1 = \{0,1\}^{l_1}$*, and* $\mathsf{MAC}^2(\mathcal{K}, \mathsf{Mac}^2, \mathsf{Vrfy}^2)$*, with* $\mathsf{Mac}^2 : \mathcal{K} \times \mathcal{M}^2 \longmapsto \mathcal{T}^2 = \{0,1\}^{l_2}$*, which share the same key* k*, we say that the PRF* Mac^1 *and* Mac^2 are derived from an underlying PRF *if there exists a PRF* $\mathsf{Mac} : \mathcal{K} \times \{0,1\}^* \longmapsto \{0,1\}^{max(l_1,l_2)}$ *from which the two PRF* $\mathsf{Mac}^{\mathsf{IV}}$ *and* $\mathsf{Mac}^{\mathsf{Tag}}$ *can be derived by either:*

$$\mathsf{Mac}^1_k(x) = \mathsf{Mac}_k(x)[1,...,l_1] \text{ and } \mathsf{Mac}^2_k(x) = \mathsf{Mac}_k(x)[1,...,l_2] \text{ or}$$
$$\mathsf{Mac}^1_k(x) = \mathsf{Mac}_k(c_1,x)[1,...,l_1] \text{ and } \mathsf{Mac}^2_k(x) = \mathsf{Mac}_k(c_2,x)[1,...,l_2]$$
$$\text{for distinct constant } c_1 \text{ and } c_2$$

The first possibility is given only when there is a domain separation*, that is the domains of the function* Mac^1 *and* Mac^2 *are two disjoint sets.*

In this way we encompass more vecMACs, with or without domain separation. For the A modes which we are interested in, the two vecMACs ($\mathsf{MAC}^{\mathsf{IV}}$ and $\mathsf{MAC}^{\mathsf{Tag}}$) have a domain separation. So we can drop the domain-separation constants of the second equation in Def. 30.

D Attack vs mode N4

We provide here the nAE-scheme $\boldsymbol{\Pi}$ used to attack mode N4 with various length input (if the message has N bit the attack was presented in Sec. 4), based on an nE Encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ and a vecMAC $\mathsf{MAC} = (\mathcal{K}_M, \mathsf{Mac}, \mathsf{Vrfy})$ which is PRF-secure. The nE Encryption scheme, which encrypts message of at most LN bits, is nE-secure and tidy, but the nAE-scheme $\boldsymbol{\Pi}$ obtained composing them according to mode N4, is not secure and, in particular, it is not INT-CTXT1-secure as we show a forgery.
The idea of the forgery is to force the tag τ of a couple $(a, \mathbf{m})$ to be encrypted identically for two different nonces, while keeping the nE-security (adversaries have only access to the Enc oracle in the nE-definition).

D.1 Construction

According to mode $N4$, an authenticated ciphertext is computed as
$c = \mathsf{Enc}_{k_E}(n, \mathbf{m} || \mathsf{Mac}_{k_M}(a, \mathbf{m}))$, for which Mac is a PRF. We now define the nE scheme Π that provides Enc.

Π can encrypt messages of at most LN bits, i.e. $\mathcal{M} = \{0,1\}^{\leq LN}$ (that is, all strings with at most LN bits. As a result, and assuming that the output of Mac is N-bit long, the nAE scheme $\boldsymbol{\Pi}$ can be used to encrypt messages which are at most $(L-1)N$ bits long. We outline the definition of Π below, based on a TPRF $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \{0,1\}^N \longmapsto \mathcal{T} = \{0,1\}^N$ with tweak space $\mathcal{TW} = \{0,1,\ldots,L\} \times \{0,1\}$ (Fig. 5).

The keys produced in Π are made of two components (k, v^*): the key $k \in \mathcal{K}$ of the TPRF E and a random value v^*. This value v^* will trigger a kind of Trojan in the encryption scheme, as it will make it possible to force the last ciphertext block to take identical values when two messages with identical last block m_l are encrypted with the two different nonces $n = 1, 2$. This trigger value v^* will be leaked to Adv when asking for the encryption of a message with the nonce $n = 1$, thus only once.

Encryption with Π proceeds as follows:

- The parsing of the message m is done in such a way that the last block m_l (thus the tag τ of the message $\mathbf{m}$) is always full.
- The first ciphertext block c_0 is an arbitrary pseudo-random value if the nonce $n \neq 1$. Instead, if $n = 1$, then $c_0 := v^*$.
- For $i = 1, ..., l-1$, the i-th ciphertext block is computed as $m_i \oplus \mathsf{E}_k^{(i,0)}(n)$.
- The second to last ciphertext block c_l, which encrypts the only message block m_{l-1} which may not be full is computed as $m_{l-1} \oplus \pi_{len}(\mathsf{E}_k^{(l-1,0)}(n))$, with $len = |m_{l-1}|$.
- The last ciphertext block c_l, which is expected to encrypt the tag τ of the message $\mathbf{m}$, is $c_l = \mathsf{E}_k^{(l,0)}(n) \oplus m_l$ (as for the previous blocks) if the condition $(*) : [(n = 1 \vee n = 2) \wedge m_{l-1} = v^*]$ is not met. Instead if this condition is met, $c_l = \mathsf{E}_k^{(l,1)}(0) \oplus m_l$. We observe that, in that case, c_l does not depend on n, which can be 1 or 2.

Condition $(*)$ is chosen in order to be met easily once, but hardly twice during the encryption queries. But it is not difficult to ask a decryption query for which this condition holds. The decryption of Π works as expected. In particular, in order to guarantee the tidiness of the nE encryption scheme, ADec verifies the correctness of the first ciphertext block c_0.

D.2 Forgery

The composition of the previous nE scheme Π with a PRF-secure MAC according to mode N4 is not $\mathsf{INT\text{-}CTXT}1$-secure. In fact we provide a forgery where the adversary A asks the encryption of only two $(l-1)N$-bits long messages, for any number of message block l, then he outputs a valid forgery:

- The adversary A asks to encrypt $(1, a, \mathbf{m}^1)$ for any a and $\mathbf{m}^1 = (\mathbf{m}_1^1, ..., \mathbf{m}_{l-1}^1)$ (with $|\mathbf{m}_{l-1}^1| = N$). He obtains $c^1 = (c_0^1, c_1^1, ..., c_{l-1}^1, c_l^1)$. In particular $c_0^1 = v^*$ and $c_i^1 = \mathsf{E}_k^{i,0}(1) \oplus \mathbf{m}_i^1$ for $i = 1, ..., l-1$.

– The adversary A asks to encrypt $(2, a, \mathbf{m}^2)$ for $\mathbf{m}^2 = (\mathbf{m}^2_1, ..., \mathbf{m}^2_{l-1})$ with $\mathbf{m}^2_{l-1} = v^*$. He obtains $c^2 = (c^2_0, ..., c^2_l)$ where $c^2_l = \mathsf{E}^{l,1}_k(0) \oplus m^2_l$ [with $m^2_l = \tau^2 = \mathsf{Mac}_{k_M}(a, \mathbf{m}^2)$].
– The adversary A asks to decrypt $(1, a, c^3)$ where $c^3_0 = v^* = c^1_0$, $c^3_i = c^1_i \oplus m^1_i \oplus m^2_i$
$\left[= \mathsf{E}^{i,0}_k(1) \oplus m^1_i \oplus m^1_i \oplus m^2_i\right]$ and $c^3_l = c^2_l = \mathsf{E}^{l,1}_k(0) \oplus m^2_l$

The decryption query $(1, a, c^3)$ is valid. In fact since the nonce is 1, c^3_0 must be equal to v^*. Then the the message retrieved from the first $l-1$ blocks is $m^3 = (m^3_1, ..., m^3_{l-1})$ with $m^3_i = m^2_i$ $\forall i = 1, ..., l-1$. In particular, given the choice of $\mathbf{m}^2$ made by A, $\mathbf{m}^3_{l-1} = v^*$. Thus, Condition $(*)$ holds and to retrieve the tag τ^3 (last block of the message) we compute $m^3_l = \mathsf{E}^{l,1}_k(0) \oplus c^3_l$.
The correct tag for the decryption query is $\tau^3 = \tau^2$, since $\mathbf{m}^2 = \mathbf{m}^3$ and adversary A uses the same associated data for both queries. Since Condition $(*)$ holds, the correct encryption of the tag τ^3 is $c^3_l = \mathsf{E}^{(l,1)}_k(0) \oplus \tau^3 = c^2_l$. Thus the decryption query is valid.

The proofs that Π is nE-secure (Prop. 10) and tidy (Prop. 11) can be found in Supp. Mat. F.2 with quantitative results. Here, we want only to highlight that the only problem may come only if the adversary is able to enter *twice* in Condition $(*)$. Since he can only learn v^* by asking an encryption query with $n = 1$ and message $\mathbf{m}^1$, it is highly improbable that $\mathbf{m}^1_{l_1} = v^*$.

E Attack vs stateful scheme

We provide here the stateful nAE-scheme $\boldsymbol{\Pi}$ used to attack stateful mode A10 with various length input (if the message has N bit the attack was presented in Sec. 7.2), based on an ivE Encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ and a vecMAC $\mathsf{MAC} = (\mathcal{K}_M, \mathsf{Mac}, \mathsf{Vrfy})$ which is PRF-secure. The ivE we present is an adaptation of the nE scheme used in Supp. Mat. D. The main changes are:

– We use a TPRP E instead of a TPRF.
– A new block c_{-1} is added to the ciphertext, in order to give the decryption algorithm the actual value of the counter ctr which is *an internal state only of the encryption device*, and $c_{-1} = \mathsf{E}^{(0,1)}_k(ctr)$. The Dec algorithm inverts this to retrieve the correct ctr. The block c_{-1} is random since it is always obtained with different inputs (as long as the number of encryption queries is $\ll 2^n$).
– To compute this block, the TPRF E is called with a tweak $(0, 1)$ that is never used else
– The boxed **if** is triggered by the value of the counter ctr (not of the nonce) and m_{l-1}
– The iv replaces the nonce n in the input of the TPRF E.

Note again that, due to mode A10, the messages which the AE scheme $\boldsymbol{\Pi}$ can encrypt, are at most $L-1$ blocks long, while those which Π can encrypt are at

most L blocks long. The full details can be found in Fig. 7.

Tidiness of this scheme follows from a close inspection of the code, while the ivE security of this scheme is presented in Prop. 14 (Supp. Mat. F.5).

Forgery We give the details only for the various length scheme (the details for the scheme presented in Sec. 7.2 are an easy adaptation of this section).
The forgery attack is a straightforward adaptation of the attack presented in Supp. Mat. D.2.

- The adversary A set the counter ctr to 1
- The adversary A asks to encrypt $(n^1, a, \mathbf{m}^1)$ for any a and $\mathbf{m}^1 = \mathbf{m}^1_1, ..., \mathbf{m}^1_{l-1}$ (with $|\mathbf{m}^1_{l-1}| = N$). He obtains $c = \left(c^1_{-1}, c^1_0, c^1_1, ..., c^1_{l-1}, c^1_l\right)$. In particular $c^1_{-1} = \mathsf{E}^{0,1}_k(ctr)$, $c^1_0 = v^*$ and $c^1_i = \mathsf{E}^{i,0}_k(iv^1) \oplus \mathbf{m}^1_i$ for $i = 1, ..., l-1$.
- The adversary A asks to encrypt $(n^2, a, \mathbf{m}^2)$ for $\mathbf{m}^2 = \mathbf{m}^2_1, ..., \mathbf{m}^2_{l-1}, v^*$. He obtains $c^2 = \left(c^2_{-1}, c^2_0, ..., c^2_l\right)$ where $c^2_l = \mathsf{E}^{l,1}_k(0) \oplus m^2_l$ [with $m^2_l = \tau^2 = \mathsf{Mac}_{k_M}(a, \mathbf{m}^2)$].
- The adversary A asks to decrypt (n^1, a, c^3) where $c^3_{-1} = c^1_{-1}$, $c^3_0 = v^* = c^1_0$, implying $ctr = 1$, $c^3_i = c^1_i \oplus m^1_i \oplus m^2_i = (\mathsf{E}^{i,0}_k(iv^1) \oplus m^1_i) \oplus m^1_i \oplus m^2_i$ and $c^3_l = c^2_l = \mathsf{E}^{l,1}_k(0) \oplus m^2_l$

The decryption query (n^1, a, c^3) is valid, substantially for the same reason as in Sec. 4.2, since $c^3 - 1$ encrypts correctly $ctr = 1$. Then, c^3_i correctly encrypts m^2_i. Since $m^3_{l-1} = m^2_{l-1} = v^*$ then c^3_l correctly encrypts τ which is the right tag for $(a, \mathbf{m}^3)$.

F Proofs

F.1 If modes A10,A11 and A12 (and N4) are INT-CTXT secure they are nAE secure

We want to prove that ciphertext integrity is the only problem to prove the nAE security of the mode.

Theorem 3. *Let Π be a $(q, t, \epsilon_{\mathsf{ivE}})$ ivE-secure ivE scheme, let MAC be a (q, t, ϵ_{prf})-PRF-secure MAC. Let $\boldsymbol{\Pi}$ be the nAE scheme obtained composing these components according to mode A10 (r. A11 or A12). Then, if $\boldsymbol{\Pi}$ is $(2q, t, \epsilon_{\mathsf{INT\text{-}CTXT}})$-secure, then it is $(q, t, \epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{\mathsf{ivE}} + \epsilon_{prf}) - \mathsf{nAE}$ secure.*

The proof is really easy, since the output of $\boldsymbol{\Pi}$ is (iv, c) where c is the output of Π. We reuse the proof of Thm. 2

Proof. In the proof of Thm. 2 we have proved that
$\epsilon_{\mathsf{nAE}} \leq \epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{\mathsf{nAE-E}}$.
In particular we have that

$$\mathsf{Adv}^{\mathsf{nAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) = \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| +$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| + \epsilon_{\mathsf{INT\text{-}CTXT}}$$

So, we have to only prove that $\boldsymbol{\Pi}$ is $\mathsf{nAE}-\mathsf{E}$-secure. From now on we consider A as an $\mathsf{nAE}-\mathsf{E}$ adversary. We do it with a series of Games:

Game 0 Is the $\mathsf{nAE}-\mathsf{E}$ game played by the adversary B against scheme $\boldsymbol{\Pi}$.

The $\mathsf{nAE}-\mathsf{E}$ *adversary* B The adversary B is based on A making the same encryption queries as A and answering all decryption query with $\perp$. That is, when the nAE adversary A asks an encryption query on input (n^i, a^i, m^i), the $\mathsf{nAE}-\mathsf{E}$ adversary B asks the same query to his oracle, obtaining c^i which B forwards to A; when A makes a decryption query on input (n^i, a^i, c^i), B first checks if c^i is not an answer to an encryption query (n^j, a^j, m^j), if it is the case he answers m^j to A, otherwise $\perp$. At the end of the game A outputs a bit b which is chosen by B as its output bit b'.

Equivalence between A *and* B Since, by hypothesis, A does not make any valid decryption hypothesis, if B answers $\perp$ to every decryption queries, he correctly simulates the decryption oracle for A. Then:

$$\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1]$$

With the same argument we can prove that

$$\Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1].$$

Game 1 Is the $\mathsf{nAE}-\mathsf{E}$ game where the adversary B is playing against scheme $\boldsymbol{\Pi}'$, where $\boldsymbol{\Pi'} = (\mathcal{K}, \mathsf{AEnc}', \mathsf{ADec}')$ is the scheme $\boldsymbol{\Pi}$ where we have replaced Mac with a random function f.

The PRF adversary C We build a PRF-adversary C based on the $\mathsf{nAE}-\mathsf{E}$ adversary. This adversary faces an oracle, which is either implemented with Mac_{k_M} or with a random function $\mathsf{f}(\cdot,\cdot)$. At the start of the game the PRF adversary C picks a random key k_E for the encryption algorithm Enc. When B makes his encryption query on input (n^i, a^i, m^i), C calls his oracle on input (n^i, a^i) (for mode A12 n^i) to obtain iv^i, then he calls his oracle on input (a^i, m^i) (for mode A11 m^i) to obtain τ^i, after that he computes $c^i = \mathsf{Enc}_{k_E}(iv^i, m^i \| \tau^i)$. At the end he sends c^i to the $\mathsf{nAE}-\mathsf{E}$ adversary B. When B output his output bit b then C output his output bit $b' = b$.

Transition from Game 0 to Game 1 We observe that if the oracle C faces is implemented with Mac_{k_M}, C correctly simulates Game 0 for B, otherwise he correctly simulates Game 1 for B. Thus

$$\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{C}^{\mathsf{Mac}_{k_M}(\cdot,\cdot)} \Rightarrow 1]$$

and

$$\Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{C}^{\mathsf{f}(\cdot,\cdot)} \Rightarrow 1]$$

Thus

$$\left|\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| = \left|\Pr[\mathsf{C}^{\mathsf{Mac}_{k_M}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{C}^{\mathsf{f}(\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{prf}$$

since Mac is $(2q, t, \epsilon_{prf})$-prf secure and C makes at most $2q$ calls to his oracle (2 for each encryption query made by B) and he runs in time t.

Game 2 Is game 1 where the adversary B is playing against scheme $\boldsymbol{\Pi}''$, where $\boldsymbol{\Pi}'' = (\mathcal{K}, \mathsf{AEnc}'', \mathsf{ADec}'')$ is the scheme $\boldsymbol{\Pi}$ where we have replaced in the ivE-secure encryption algorithm $\mathsf{Enc}'(\cdot,\cdot)$ with a random function $\$(\cdot,\cdot)$.

The ivE *adversary* D We build an ivE adversary D based on the $\mathsf{nAE}-\mathsf{E}$ adversary A. This adversary faces an oracle, which is either implemented with $\mathsf{Enc}_{k_E}(\cdot,\cdot)$ or with a random function $\$(\cdot,\cdot)$. At the start of the game the ivE adversary D picks a function $\mathsf{f}(\cdot,\cdot)$. When B makes his encryption query on input (n^i, a^i, m^i), C computes $iv^i = \mathsf{f}(n^i, a^i)$ (for mode A12 $iv^i = \mathsf{f}(n^i)$) and $\tau^i = \mathsf{f}(a^i, m^i)$ (for mode A11 $\tau^i = \mathsf{f}(m^i)$), then he calls his oracle on input $(iv^i, m^i \| \tau^i)$ obtaining c^i which he forwards to B. When B outputs his output bit b then D outputs his output bit $b' = b$.

Transition from Game 1 to Game 2 We observe that if the oracle D faces is implemented with Enc_{k_E}, D correctly simulates Game 1 for B, otherwise he correctly simulates Game 2 for D. Thus

$$\Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{D}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1]$$

and

$$\Pr[\mathsf{B}^{\mathsf{AEnc}''(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{D}^{\$(\cdot,\cdot)} \Rightarrow 1]$$

Thus

$$\left|\Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{AEnc}''(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| = \left|\Pr[\mathsf{D}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{D}^{\$(\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathsf{ivE}}$$

since Π is $(q, t, \epsilon_{\mathsf{ivE}}) - \mathsf{ivE}$ secure and D makes at most q encryption queries and he runs in time t and the iv are randomly picked since they are output by the random function f.

Game 3 In this Game B interacts with $\$(\cdot,\cdot,\cdot)$ instead of AEnc''.

Transition from Game 2 to Game 3 We observe that Game 3 and Game 2 are indistinguishable since every answer to an encryption query is random: in fact, the iv is random, due to Game 1 and the output of $\$(\cdot,\cdot)$ is random. Thus:

$$\Pr[\mathsf{B}^{\mathsf{AEnc}''(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{D}^{\$(\cdot,\cdot)} \Rightarrow 1]$$

Bounding the $\mathsf{nAE}-\mathsf{E}$ *advantage* This concludes the proof since

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| =$$

$$\left|\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{prf} + \epsilon_{\mathsf{ivE}}$$

and consequently we can bound

$$\mathsf{Adv}^{\mathsf{nAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) = \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{prf} + \epsilon_{\mathsf{ivE}}.$$

Theorem 4. *Let* Π *be a* $(q,t,\epsilon_{\mathsf{nE}})$-$\mathsf{nE}$-*secure* nE *scheme, let* MAC *be a* (q,t,ϵ_{prf})-*PRF-secure* MAC*. Let* $\boldsymbol{\Pi}$ *be the* nAE *scheme obtained composing these components according to mode N4. Then, if* $\boldsymbol{\Pi}$ *is* $(q,t,\epsilon_{\mathsf{INT\text{-}CTXT}})$*-secure, then it is* $(q,t,\epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{\mathsf{nE}}) - \mathsf{nAE}$ *secure.*

The proof is completely similar to the previous theorem, simply we do not have to replace the iv.

Proof. In the proof of Thm. 2 we have proved that
$\epsilon_{\mathsf{nAE}} \leq \epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{\mathsf{nAE}-\mathsf{E}}$.
In particular we have that

$$\mathsf{Adv}^{\mathsf{nAE}}_{\boldsymbol{\Pi}}(\mathsf{A}) = \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| +$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| + \epsilon_{\mathsf{INT\text{-}CTXT}}$$

So, we have to only prove that $\boldsymbol{\Pi}$ is $\mathsf{nAE}-\mathsf{E}$-secure. From now on A is an $\mathsf{nAE}-\mathsf{E}$ adversary. We do it with a series of Games:

Game 0 Is the $\mathsf{nAE}-\mathsf{E}$ game played by adversary A against scheme $\boldsymbol{\Pi}$.

The $\mathsf{nAE}-\mathsf{E}$ *adversary* B The adversary B is based on A making the same encryption queries as A and answering all decryption query with $\perp$. That is, when the nAE adversary A asks an encryption query on input (n^i, a^i, m^i), the $\mathsf{nAE}-\mathsf{E}$ adversary B asks the same query to his oracle, obtaining c^i which he forwards to A; when A makes a decryption query on input (n^i, a^i, c^i), B first checks if c^i is not an answer to an encryption query (n^j, a^j, m^j), if it is the case he answers m^j to A, otherwise $\perp$. At the end of the game A outputs a bit b which is chosen by B as its output bit b'.

Equivalence between A *and* B Since, by hypothesis, A does not make any valid decryption hypothesis, if B answers $\perp$ to every decryption queries, he correctly simulates the decryption oracle for A. Then:

$$\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1]$$

With the same argument we can prove that

$$\Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1].$$

Game 1 Is game 1 where the adversary B is playing against scheme $\boldsymbol{\Pi'}$, where $\boldsymbol{\Pi'} = (\mathcal{K}, \mathsf{AEnc}', \mathsf{ADec}')$ is the scheme $\boldsymbol{\Pi}$ where we have replaced in the nE-secure encryption scheme $\mathsf{Enc}'(\cdot,\cdot)$ with a random function $\$(\cdot,\cdot)$.

The nE *adversary* C We build an nE adversary C based on the $\mathsf{nAE}-\mathsf{E}$ adversary A. This adversary faces an oracle, which is either implemented with $\mathsf{Enc}_{k_E}(\cdot,\cdot)$ or with a random function $\$(\cdot,\cdot)$. At the start of the game the nE adversary C picks a random key k_M for the Mac function. When B makes his encryption query on input (n^i, a^i, m^i), C computes $\tau^i = \mathsf{Mac}_{k_M}(a^i, m^i)$, then he calls his oracle on input $(n^i, m^i \| \tau^i)$ obtaining c^i which he forwards to B. When B outputs his output bit b then C outputs his output bit $b' = b$.

Transition from Game 0 to Game 1 We observe that if the oracle C faces is implemented with Enc_{k_E}, C correctly simulates Game 1 for B, otherwise he correctly simulates Game 2 for D. Thus

$$\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{C}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1]$$

and

$$\Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{C}^{\$(\cdot,\cdot)} \Rightarrow 1]$$

Thus

$$\left|\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| = \left|\Pr[\mathsf{C}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{C}^{\$(\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathsf{nE}}$$

since Π is $(q, t, \epsilon_{\mathsf{nE}}) - \mathsf{nE}$ secure and C makes at most q encryption queries and he runs in time t (and the n are all different).

Game 2 In this Game B interacts with $\$(\cdot,\cdot,\cdot)$ instead of AEnc''.

Transition from Game 1 to Game 2 We observe that Game 1 and Game 2 are indistinguishable since every answer to an encryption query is random: in fact, the output of $\$(\cdot,\cdot)$ is random. Thus:

$$\Pr[\mathsf{B}^{\mathsf{AEnc}'(\cdot,\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{C}^{\$(\cdot,\cdot)} \Rightarrow 1]$$

Bounding the $\mathsf{nAE}-\mathsf{E}$ *advantage* This concludes the proof since

$$\left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| =$$

$$\left|\Pr[\mathsf{B}^{\mathsf{AEnc}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\$(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathsf{nE}}$$

and consequently we can bound

$$\mathsf{Adv}^{\mathsf{nAE}}_{\Pi}(\mathsf{A}) = \left|\Pr[\mathsf{A}^{\mathsf{AEnc}(\cdot,\cdot,\cdot),\mathsf{ADec}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1]\right| \leq$$

$$\epsilon_{\mathsf{INT\text{-}CTXT}} + \epsilon_{\mathsf{nE}}.$$

F.2 Proof of nE security and tidiness of the nE scheme of Sec. 4

We are left with the problem to prove the nE security and the tidiness of the scheme Π used in Sec. 4 and described in Fig. 5.

Proposition 10. *Let* $\mathsf{E} : \mathcal{K}\times\mathcal{TW}\times\{0,1\}^N \longmapsto \{0,1\}^N$*, with* $\mathcal{TW} = \{0,1,...,L\}\times\{0,1\}$*, be a* $((L+1)q,t,\epsilon_{TPRF})-$*TPRF secure. Then* Π *is* $(q,t,\epsilon_{TPRF}+2^{-N})-\mathsf{nE}$ *secure if every message has at most* L *blocks.*

Proof. Let A be a $(q,t)-\mathsf{nE}$ adversary who asks messages which have at most L message blocks.
By definition of nE-security (Def. 16), we have to bound

$$\mathsf{Adv}^{\mathsf{nE}}_{\Pi}(\mathsf{A}) := \left|\Pr\left[\mathsf{A}^{\mathsf{Enc}_k(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot,\cdot)} \Rightarrow 1\right]\right|$$

for every $(q,t)-\mathsf{nE}$-adversary.
We will do it using a sequence of games.
First we observe that the length $|\mathsf{Enc}_k(n,m)|$ is equal to $|m|+N$ $\forall(k,n,m) \in \mathcal{K}\times\mathcal{N}\times\mathcal{M}$, so the length of the ciphertext does not give any information about its inputs apart from the length $|m|$.

Game 0. The first game, Game 0, is the game where the nE adversary A is facing Π. At the end of the game, the nE adversary outputs a bit b.
Let E_0 be the event that the bit output at the end of Game 0 by the nE adversary A is 1.

Game 1. First we replace the TPRF $\mathsf{E}^{(\cdot)}(\cdot)$ with a random function $\mathsf{f}^{(\cdot)}(\cdot)$ with the same signature of the TPRF E. We call the scheme with this replacement $\overline{\Pi}$. Let E_1 be the event that the adversary A outputs 1 when he is facing $\overline{\Pi}$.
We now bound $|\Pr[E_0] - \Pr[E_1]|$ with ϵ_{TPRF}.

The TPRF-adversary B. To do this we build a $((L+1)q, t) - \text{TPRF}$-adversary B against the $((L+1)q, t, \epsilon_{\text{TPRF}}) - \text{TPRF}$ E.
This TPRF adversary B faces an oracle which is either implemented with the TPRF E or a random function f.
At the start the adversary B picks a random value v^*. When A makes an encryption query (n^i, m^i) for any $i = 1, ..., q$, B, first, parses the message in l_i blocks with $|m_1^i| = ... = |m_{l_i-2}^i| = |m_{l_i}^i| = N$ and $|m_{l-1}^i| \leq N$; if the parsing is not possible he answers $\perp$ to A. Then, if $n^i = 1$, the adversary B sets $c_0^i = v^*$, otherwise he calls his oracle on input $((0,0), n^i)$ obtaining a value which adversary B sets c_0^i to.
After that for $j = 1, ..., l_i - 2$, the adversary B calls his oracle on input $((j,0), n^i)$, obtaining the value x_j^i which is XORed to the message block m_j^i obtaining c_j^i.
For the block $l_i - 1$, the adversary B calls his oracle on input $((l_i - 1, 0), n^i)$, obtaining $x_{l_i-1}^i$. Then, he takes the first $|m_{l-1}|$-bits of $x_{l_i-1}^i$ and he XORes them to m_{l_i-1} obtaining c_{l_i-1}.
For the last message block l_i, if the nonce n^i is either 1 or 2 and $m_{l-1}^i = v^*$ the TPRF adversary B calls his oracle on input $((l,1),0)$ obtaining x_l^i which he XORes to m_l^i obtaining c_l^i. Otherwise, the adversary B calls his oracle on input $((l,0), n^i)$ obtaining x_l^i which he XORes again to m_l^i obtaining c_l^i. Next adversary B computes $c^i = (c_0^i, ..., c_l^i)$ and he forwards the ciphertext c^i to the nE adversary A.
When the adversary A outputs his output bit b, B outputs the same bit $b' = b$.

Transition between Game 0 and Game 1. We observe that if the oracle facing the TPRF adversary B, is implemented with the TPRF $\mathsf{E}^{(\cdot)}(\cdot)$, the nE adversary A is playing Game 0, otherwise he is playing Game 1.
Thus $\Pr[E_0] = \Pr[\mathsf{B}^{\mathsf{E}} \Rightarrow 1]$ and $\Pr[E_1] = \Pr[\mathsf{B}^{\mathsf{E}} \Rightarrow 1]$. The adversary B makes at most $L+1$ queries to his oracle per encryption query. Since the nE adversary A asks at most q encryption queries, the TPRF adversary B makes at most $(L+1)q$ queries to his oracle. Since E is a
$((L+1)q, t, \epsilon_{\text{TPRF}})$-secure TPRF and B is a $((L+1)q, t) - \text{TPRF}$ adversary, we can bound
$|\Pr[\mathsf{B}^{\mathsf{E}} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}} \Rightarrow 1] \leq \epsilon_{\text{TPRF}}$. Thus $|\Pr[E_0] - \Pr[E_1]| \leq \epsilon_{\text{TPRF}}$.
So, $\Pr[E_0] \leq \Pr[E_1] + \epsilon_{\text{TPRF}}$.

Event C. We define the event C as the event that during Game 1 the nE adversary is able to force the encryption algorithm Enc_k to enter twice in the **if** clause boxed in Figure 5.
We assert that $\Pr[C] \leq 2^{-N}$.
To prove this, we start by observing that, in order to enter twice in that **if**, the nE adversary must have asked a query on input (n^i, m^i) with $n^i = 1$ and another query on input (n^j, m^j) with $n^j = 2$. There are no other possibilities since the nonce must not be repeated in encryption queries (see Def. 16).
There are two possibilities:

- $i < j$, that is, the nE adversary first asks to encrypt a message with nonce n^i equal to 1 and then another with nonce n^j equal to 2,

– $i > j$

Clearly $\Pr[C] \leq max(\Pr[C|i < j], \Pr[C|i > j])$. We start by computing $\Pr[C|i < j]$.
When the nE adversary A queries his oracle on input $(1, m^i)$ he has no idea of what is the value v^* since this value is picked uniformly at random and it has never been used. So the probability that the second to last block m_{l_i-1} of the message m^i is equal to v^* is $\leq 2^{-N}$(it is not equal since the block m_{l_i-1} may not be full, that is $|m_{l_i-1}| < N$). Thus $\Pr[C|i < j] \leq 2^{-N}$.
On the other hand, $\Pr[C|i > j]$ is bounded by 2^{-N} for the same reason, since when the nE adversary A calls his oracle on input $(2, m^j)$ he has no idea of the value v^*.
Thus $\Pr[C] \leq 2^{-N}$.

Game 2. We define Game 2 as Game 1 apart from the fact that if event C happens the nE adversary A outputs immediately 1. Let E_2 be the event that the nE adversary A outputs 1.
Clearly $|\Pr[E_2] - \Pr[E_1]| \leq \Pr[C] \leq 2^{-N}$.

Game 3. Game 3 is defined as Game 2 apart from the fact that we replace all c^i's with random strings of the same length. Let E_3 be the event that the nE adversary outputs 1 at the end of Game 3.

Transition from Game 2 and Game 3. We assert that $\Pr[E_2] = \Pr[E_3]$.
If event C happens the nE adversary behaves in the same way in both games. Otherwise we can observe that the random function $\mathsf{f}^{(\cdot)}(\cdot)$ is never called during the game on the same inputs. Since $\mathsf{f}^{(\cdot)}(\cdot)$ is by hypothesis a random function the XOR of its output with a message block is a random string. Moreover for the first ciphertext block c_0^i for every i we can observe that if $n^i = 1$ it is v^* which is a random value by hypothesis; otherwise it is $\mathsf{f}^{(0,0)}(n^i)$ which is a random value since f has never been computed on this input and $\mathsf{f}^{(\cdot)}(\cdot)$ is a random function. Thus all the ciphertext obtained in Game 2 are random strings, except if event C happens. Consequently $\Pr[E_3] = \Pr[E_2]$.

Thus for every $(q, t) - \mathsf{nE}$ adversary A we can bound

$$\mathsf{Adv}^{\mathsf{nE}}_{\Pi}(\mathsf{A}) = |\Pr[E_0] - \Pr[E_3]| \leq \epsilon_{\mathrm{TPRF}} + |\Pr[E_1] - \Pr[E_2]| \leq \epsilon_{\mathrm{TPRF}} + 2^{-N}$$

concluding our proof.

We have now to prove the tidiness of the scheme,

Proposition 11. *The nonce based encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ is tidy.*

Proof. A close inspection of the algorithm presented in Fig 5 proves the claims.

F.3 Security relations among A10, A11 and A12

Before to give the proofs of the Prop. 1, 2, 3, 4, we have to prove two technical lemmata. With the first, which was not formally stated in Sec. 5, but whose contents were already mentioned, we replace the PRF $\mathsf{F}^{\mathsf{IV}}_{k_M}$ and $\mathsf{F}^{\mathsf{Tag}}_{k_M}$ with two random functions, respectively f^{IV} and $\mathsf{f}^{\mathsf{Tag}}$. We do it once for all, since otherwise it would be the first step of many of the following propositions.

Replacing the Mac function with random functions

Lemma 3. *Let the* $\mathsf{vecMAC}^{\mathsf{IV}} = (\mathcal{K}_M, \mathsf{Mac}^{\mathsf{IV}}, \mathsf{Vrfy}^{\mathsf{IV}})$*, with* $\mathsf{Mac}^{\mathsf{IV}} : \mathcal{K}_M \times \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *(for A12,* $\mathsf{Mac}^{\mathsf{IV}} : \mathcal{K}_M \times \mathcal{N} \longmapsto \mathcal{IV}$*), and the* $\mathsf{vecMAC}^{\mathsf{Tag}} = (\mathcal{K}_M, \mathsf{Mac}^{\mathsf{Tag}}, \mathsf{Vrfy}^{\mathsf{Tag}})$*, with* $\mathsf{Mac}^{\mathsf{Tag}} : \mathcal{K}_M \times \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *(for A11,* $\mathsf{Mac}^{\mathsf{Tag}} : \mathcal{K}_M \times \mathcal{M} \longmapsto \mathcal{T}$*) share the same key and be derived from the same PRF* $\mathsf{Mac} : \mathcal{K}_M \times \{0,1\}^* \longmapsto \mathcal{IV} \cup \mathcal{T}$ *(see Def. 30) which is* $(2q, t, \epsilon_{PRF})-$*PRF secure. Given a tidy iv-based encryption* ivE *scheme* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$*, let* $\boldsymbol{\Pi}$ *be the generic composition of these primitives according to mode A10 (respectively A11, A12). Let* $\overline{\boldsymbol{\Pi}}$ *be the scheme obtained by* $\boldsymbol{\Pi}$ *replacing* $\mathsf{vecMAC}^{\mathsf{IV}}$ *and* $\overline{\mathsf{vecMAC}^{\mathsf{Tag}}}$ *(based on the PRFs* $\mathsf{Mac}^{\mathsf{IV}}$ *and* $\mathsf{Mac}^{\mathsf{Tag}}$ *respectively) respectively with* $\overline{\mathsf{vecMAC}^{\mathsf{IV}}}$ *and* $\overline{\mathsf{vecMAC}^{\mathsf{Tag}}}$ *(based on the random functions* f^{IV} *and* $\mathsf{f}^{\mathsf{Tag}}$ *respectively). Let* $\boldsymbol{\Pi}$ *be* $(q, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})-\mathsf{INT\text{-}CTXT1}$ *secure then* $\overline{\boldsymbol{\Pi}}$ *is* $(q, t, \overline{\epsilon_{\mathsf{INT\text{-}CTXT1}}})-\mathsf{INT\text{-}CTXT1}$ *with* $|\epsilon_{\mathsf{INT\text{-}CTXT1}} - \overline{\epsilon_{\mathsf{INT\text{-}CTXT1}}}| \leq \epsilon_{PRF}$)

The proof is completely standard.

Proof. The proof is done using a sequence of two games.

Game 0 In Game 0, the $(q, t)-\mathsf{INT\text{-}CTXT1}$-adversary A is playing the standard $\mathsf{INT\text{-}CTXT1}$ game against scheme $\boldsymbol{\Pi}$. Let $E = E_0$ be the event that A is able to produce a valid forgery in Game 0.

Game 1 In Game 1, the adversary A is playing the $\mathsf{INT\text{-}CTXT1}$-game against scheme $\overline{\boldsymbol{\Pi}}$, which is the scheme $\boldsymbol{\Pi}$ where we have replaced the pseudorandom functions $\mathsf{Mac}^{\mathsf{IV}}_{k_M}$ and $\mathsf{Mac}^{\mathsf{Tag}}_{k_M}$ with the random functions f^{IV} and $\mathsf{f}^{\mathsf{Tag}}$ respectively. Let E_1 be the event that the adversary A is able to produce a valid forgery in Game 1.

Transition between Game 0 and Game 1 We prove that

$$|\Pr[E_0] - \Pr[E_1]| \leq +\epsilon_{\mathrm{PRF}}$$

using the $(2q, t)-$PRF adversary B against the PRF Mac_{k_M} from which $\mathsf{Mac}^{\mathsf{IV}}_{k_M}(\cdot,\cdot)$ [for A12, $\mathsf{Mac}^{\mathsf{IV}}_{k_M}(\cdot)$] and $\mathsf{Mac}^{\mathsf{Tag}}_{k_M}(\cdot,\cdot)$ [for A11, $\mathsf{Mac}^{\mathsf{Tag}}_{k_M}(\cdot)$] are derived. At the start of the Game the $(2q, t)-$PRF-adversary B picks uniformly at random a key $k_E \leftarrow \mathcal{K}_E$ for the *iv*-based encryption scheme $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$. Then when A makes an encryption query $(n^i, a^i, \mathbf{m}^i)$, the adversary B simply calls his oracle, which is either implemented with the PRF $\mathsf{Mac}_{k_M}(\cdot)$ or with a

random function $\mathsf{f}(\cdot)$, on input (n^i, a^i) [for A12, on input (n^i)] to get the IV, iv^i and then B calls it again on input $(a^i, \mathbf{m}^i)$ [(for A11, on input $(\mathbf{m}^i)$] to get the tag τ^i. Then B computes $c^i \leftarrow \mathsf{Enc}_{k_E}(iv^i, \mathbf{m}^i \| \tau^i)$ and returns c^i to the INT-CTXT1-adversary A.
When A makes his decryption query (n^q, a^q, c^q), the adversary B calls his oracle on input (n^q, a^q) [for A12, n^q] to get iv^q and then he computes
$(\mathbf{m}^q \| \tau^q) \leftarrow \mathsf{Dec}_{k_E}(iv^q, c^q)$. After that, he calls his oracle on input $(a^q, \mathbf{m}^q)$ [for A11, $\mathbf{m}^q$] obtaining $\tau^{q,c}$. If $\tau^q = \tau^{q,c}$
(and $(n^q, a^q, c^q) \neq (n^i, a^i, c^i),\ \forall i = 1, ..., q-1$) he outputs 1, otherwise 0.
We observe that in both case the PRF-adversary B outputs 1, iff the adversary A is able to produce a valid forgery. Thus $\Pr[\mathsf{B}^{\mathsf{Mac}_{k_M}(\cdot)} \Rightarrow 1] = \Pr[E_0]$ and $\Pr[\mathsf{B}^{\mathsf{f}(\cdot)} \Rightarrow 1] = \Pr[E_1]$.
If the oracle is implemented with $\mathsf{Mac}_{k_M}(\cdot)$, the INT-CTXT1-adversary A is playing Game 0, otherwise the adversary A is playing Game 1. Since B asks $2q$ queries to his oracle and $\mathsf{Mac}(\cdot)$ is a $(2q, t, \epsilon_{\mathrm{PRF}}) - \mathrm{PRF}$ then

$$|\Pr[E_0] + \Pr[E_1]| = \left|\Pr[\mathsf{B}^{\mathsf{Mac}_{k_M}(\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}(\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathrm{PRF}}$$

which concludes the proof since $\Pr[E_0] = \epsilon_{\mathsf{INT\text{-}CTXT1}}$ and $\Pr[E_1] = \overline{\epsilon_{\mathsf{INT\text{-}CTXT1}}}$.

Proof of Lemma 1 This lemma was needed to rule out the simple cases "A wins $\cap C$" and "A wins $\cap B \cap \overline{C}$".

Lemma 1. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *[for mode* $\overline{A12}$*,* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \longmapsto \mathcal{IV}$ *] and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *[for mode* $\overline{A11}$*,* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{M} \longmapsto \mathcal{T}$ *] be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-ivE*-secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE *scheme obtained composing* f^{IV}*,* $\mathsf{f}^{\mathsf{Tag}}$ *and* Π *according to mode* $\overline{A10}$ *or* $\overline{A11}$ *or* $\overline{A12}$*. Then we can bound*

$$\Pr[\mathsf{A}\ \textit{wins}\ \cap C] + \Pr[\mathsf{A}\ \textit{wins}\ \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

The proof is completely standard.

Proof. We start computing

$$\Pr[\mathsf{A}\ \text{wins}\ \cap C] = \Pr[\mathsf{A}\ \text{wins} \cap (a^q, \mathbf{m}^q) \neq (a^j, \mathbf{m}^j)\ \forall j = 1, ..., q-1]$$

$$\left[\ \text{for mode}\ \overline{A11} = \Pr[\mathsf{A}\ \text{wins} \cap \mathbf{m}^q \neq \mathbf{m}^j\ \forall j = 1, ..., q-1]\right]$$

This is bounded by $|\mathcal{T}|^{-1}$ because the probability that the tag τ^q is correct is $|\mathcal{T}|^{-1}$ since $\tau^{q,c} = \mathsf{f}^{\mathsf{Tag}}(a^q, \mathbf{m}^q)$ (for mode $\overline{A11}$, $\tau^{q,c} = \mathsf{f}^{\mathsf{Tag}}(\mathbf{m}^q)$) is picked uniformly at random after the adversary A outputs the decryption query since the tag τ^q has never been computed before.

Then we compute $\Pr[\mathsf{A}\ \text{wins}\ \cap B \cap \overline{C}] =$

$\Pr[\mathsf{A}\ \text{wins} \cap (n^q, a^q) \neq (n^i, a^i)\ \forall i = 1, ..., q-1 \cap \exists j \in \{1, ..., q-1\}\ \text{s.t.}\ (a^q, \mathbf{m}^q) = (a^j, \mathbf{m}^j)]$

$$\Big[\text{ for mode } \overline{A12}$$

$$= \Pr[\mathsf{A} \text{ wins} \cap n^q \neq n^i \ \forall i = 1, ..., q-1 \ \cap \ \exists j \in \{1, ..., q-1\} \text{ s.t. } (a^q, \mathbf{m}^q) = (a^j, \mathbf{m}^j)]\Big]$$

$$\Big[\text{ for mode } \overline{A11}$$

$$= \Pr[\mathsf{A} \text{ wins} \cap (n^q, a^q) \neq (n^i, a^i) \ \forall i = 1, ..., q-1 \ \cap \ \exists j \in \{1, ..., q-1\} \text{ s.t. } \mathbf{m}^q = \mathbf{m}^j]\Big]$$

This is bounded by $(q-1)(\epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1})$.
In fact let A be a $(q,t)-\mathsf{INT\text{-}CTXT}1$ adversary against scheme $\overline{\boldsymbol{\Pi}}$ and we suppose that event B happens and event C does not happen. Now we build, based on A, a $(q,t)-\mathsf{ivE}$ adversary B against scheme Π. The ivE-adversary B faces an oracle which is either implemented with $\mathsf{Enc}_{k_E}(\cdot,\cdot)$ or with $\$(\cdot,\cdot)$. The ivE-adversary B is constructed in this way:
First, the adversary B chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ (for mode $\overline{A12}$, $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \longmapsto \mathcal{IV}$) and $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ (for mode $\overline{A11}$, $\mathsf{f}^{\mathsf{Tag}} : \mathcal{M} \longmapsto \mathcal{T}$). Then, when the $\mathsf{INT\text{-}CTXT}1$-adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$ [for mode $\overline{A12}$, $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i)$] and $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$ [for mode $\overline{A11}$, $\tau^i = \mathsf{f}^{\mathsf{Tag}}(\mathbf{m}^i)$]. Then the ivE-adversary B queries his oracle on input $(iv^i, \mathbf{m}^i \| \tau^i)$ receiving c^i, which he forwards to the adversary A. In this way B asks at most $q-1$ oracle queries. When A makes his decryption query (n^q, a^q, c^q), B computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$ [for mode $\overline{A12}$, $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q)$]. Let $\mathcal{J}$ be the set of index $j = 1, ..., q-1$ s.t. $a^q = a^j$ (Clearly $|\mathcal{J}| \leq q-1$) [for mode $\overline{A11}$ since the AD are not used to compute the tag, every message can be picked, thus $\mathcal{J} = \{1, ..., q-1\}$]. Now adversary B, picks a random $j_g \in \mathcal{J}$ recomputes $\tau^{j_g} = \mathsf{f}^{\mathsf{Tag}}(a^{j_g}, \mathbf{m}^{j_g})$ [for mode $\overline{A11}$, $\tau^{j_g} = \mathsf{f}^{\mathsf{Tag}}(\mathbf{m}^{j_g})$] and he queries his oracle [which is either implemented with $\mathsf{Enc}(\cdot,\cdot)$ or with a random oracle $\$(\cdot,\cdot)$] on input $(iv^q, \mathbf{m}^{j_g} \| \tau^{j_g})$ obtaining the ciphertext $c^{q,c}$. Doing this, the adversary B asks his last query of the q oracle queries he has granted to. If $c^{q,c} = c^q$ he outputs 1, otherwise 0. [We observe that the ivs are picked uniformly at random form the $\mathcal{IV}$ space and the adversary B does not change any oracle query after having seen the relative iv. So, we are not obliged to pass through the $\mathsf{Enc}^{\$}_{k_E}(\cdot)$ oracle].
Since event C has happened and $\mathsf{Enc}_{k_E}(iv^q, \cdot)$ is an injective function, we obtain

$$\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \Pr[j_g = j]$$

Clearly $\Pr[j_g = j] = |\mathcal{J}|^{-1} \geq \frac{1}{q-1}$. Thus:

$$\Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \Pr[j_g = j] \geq \frac{1}{q-1} \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}]$$

Consequently

$$\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] \geq \frac{1}{q-1} \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}]$$

On the other hand

$$\Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1] = \Pr[\$(iv^q, m^{j_g} \| \tau^{j_g}) = c^q] =\leq |\mathcal{T}|^{-1} \cdot |m^j|^{-1} \leq |\mathcal{T}|^{-1}$$

But, since the ivE-scheme Π is $(q, t, \epsilon_{\mathsf{ivE}})$-secure, by definition (Def. 18), we have that

$$\left|\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathsf{ivE}}$$

Thus

$$\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] \leq \epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1}$$

then

$$\frac{1}{q-1}\Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq \Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] \leq \epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1}$$

Consequently $\Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq (q-1)(\epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1})$ which concludes the proof since

$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq |\mathcal{T}|^{-1} + (q-1)(\epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1}) = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$.

Proof of Proposition 1

We want to prove that if mode $\overline{A12}$ is INT-CTXT1-secure, then mode $\overline{A10}$ is also INT-CTXT1-secure.

Proposition 1. *Let* $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-ivE-*secure encryption scheme. Then, if mode* $\overline{A12}$ *implemented with the random function* $\mathsf{f}^{\mathsf{IV}_{12}} : \mathcal{N} \longmapsto \mathcal{IV}$ *is* $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-INT-CTXT1-*secure then mode* $\overline{A10}$ *is* $(q-1, t, q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{\mathsf{INT\text{-}CTXT1}})$-INT-CTXT1-*secure*

Proof. Let A be a $(q-1, t)$ – INT-CTXT1 adversary.
Using Lemma 1 we have that

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

So, we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
Here we reduce the INT-CTXT1 security of the scheme $\boldsymbol{\Pi}$, composed accordingly to mode $\overline{A10}$, to the INT-CTXT1 security of the scheme $\boldsymbol{\Pi'}$, composed accordingly to mode $\overline{A12}$. We do it using a sequence of two games:

Game 0 In Game 0 the (q, t) – INT-CTXT1-adversary A is playing the standard INT-CTXT1 game against scheme $\overline{\boldsymbol{\Pi}}$, with $\overline{\boldsymbol{\Pi}}$ be an $\overline{A10}$ scheme, with the condition that the adversary A's decryption query $(n^q, a^q, c^q) = \overline{\mathsf{AEnc}_{k_E}}(n^q, a^q, \mathbf{m}^q)$ respects the condition $\overline{B} \cap \overline{C}$, that is the couple (n^q, a^q) is not fresh and the couple $(a^q, \mathbf{m}^q)$ is not fresh. Let E_0 be the event that the adversary A wins this game.

Game 1 In Game 1 the (q, t) – INT-CTXT1-adversary A is playing the standard INT-CTXT1 game against scheme $\overline{\boldsymbol{\Pi'}}$, where $\overline{\boldsymbol{\Pi'}}$ is a scheme composed accordingly to mode $\overline{A12}$, with the condition that the adversary A's decryption query $(n^q, a^q, c^q) = \overline{\mathsf{AEnc}_{k_E}}(n^q, a^q, \mathbf{m}^q)$ respects the condition $\overline{B} \cap \overline{C}$, that is the couple (n^q, a^q) is not fresh and the couple $(a^q, \mathbf{m}^q)$ is not fresh. Let E_1 be the event that the adversary A wins this game.

Transition from Game 0 to Game 1 We use a $(q-1,t)-$ PRF adversary B against the oracle $\mathcal{O}$ to prove that $\Pr[E_0] = \Pr[E_1]$.
The oracle $\mathcal{O}(\cdot,\cdot)$ is either implemented with a random function $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ or with the function $\mathsf{f}'^{\mathsf{IV}_{12}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ obtained by the random function $\mathsf{f}^{\mathsf{IV}_{12}} : \mathcal{N} \longmapsto \mathcal{IV}$ simply by defining $\mathsf{f}'^{\mathsf{IV}_{12}}(n,a) := \mathsf{f}^{\mathsf{IV}_{12}}(n)\ \forall n \in \mathcal{N}, a \in \mathcal{A}$. Moreover the PRF-adversary B is not allowed to repeat the first input (n) in different oracle queries. The PRF-adversary B is built as follow:
First adversary B chooses a random function $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ and a key $k_E \in \mathcal{K}_E$ for the ivE scheme Π. Then when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B queries his oracle on input (n^i, a^i) obtaining iv^i. Then he computes $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$ and $c^i = \mathsf{Enc}_{k_E}(iv^i, m^i)$ with $m^i = \mathbf{m}^i \| \tau^i$, and he forwards c^i to adversary A. In this way B asks at most $q-1$ oracle queries. Moreover he keeps in memory the quadruple $(n^i, a^i, iv^i, \mathbf{m}^i)$.
When A makes his decryption query (n^q, a^q, c^q), (by hypothesis we have supposed that $(n^q, a^q) = (n^j, a^j)$ for a certain $j \in \{1, ..., q-1\}$) B looks up in his memory for $(n^q, a^q, \cdot, \cdot)$, he finds the corresponding j and retrieves iv^j. Then he decrypts c^q computing $c^q = (\mathbf{m}^q \| \tau^{q,c}) = \mathsf{Dec}_{k_E}(iv^j, c^q)$ and he verifies if $\tau^q = \tau^{q,c}$ $(= \mathsf{f}^{\mathsf{Tag}}(a^q, \mathbf{m}^q))$. If the equality holds (that is, the decryption query (n^q, a^q, c^q) is valid), the PRF-adversary B outputs 1, otherwise he outputs 0.
We observe that if the oracle $\mathcal{O}$ is implemented with $\mathsf{f}^{\mathsf{IV}_{10}}(\cdot,\cdot)$ the adversary A is playing Game 0, otherwise he is playing Game 1.

The security of the oracle $\mathcal{O}$ We observe that

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}_{10}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)} \Rightarrow 1]\right| = 0$$

In fact since the adversary B has not the right to repeat the first input (the nonce n) in different oracle queries he is not able to see any difference. In fact we can see $\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)$ as obtained from a random function $\mathsf{f}'^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ in this way:
When $\mathsf{f}'^{\mathsf{IV}_{12}}$ is called on input (n,a) the oracle first looks up into his list if he find a couple (n, iv) for the same n. If this is the case it outputs iv, otherwise he call the function $\mathsf{f}'^{\mathsf{IV}_{10}}$ on input (n,a) obtaining iv. Then he adds to his list the couple (n, iv) and outputs iv.
Clearly this oracle implements honestly $\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)$.
We observe that, since B is not allowed to repeat the nonce n in different oracle queries, during the previous game the oracle which implements $\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)$ never looks up into his list during AEnc queries. For the ADec query, he does not have to look up in the list for the answer since he is queried on an input (n^q, a^q) which he has already answered to. So B can be seen facing either $\mathsf{f}^{\mathsf{IV}_{10}}$ or $\mathsf{f}'^{\mathsf{IV}_{10}}$, which are both random functions from $\mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$, (clearly his behaviour is the same when he faces anyone of this two random functions, because, by definition, they are indistinguishable from each other). So

$$\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}_{10}}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)} \Rightarrow 1] = 0 = (\square)$$

$|\Pr[E_0]-\Pr[E_1]|$*:* Now we are left only with the bound of $|\Pr[E_0]-\Pr[E_1]|$. We observe that

$$\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}_{10}}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{A} \text{ wins against } \overline{A10}] = \Pr[E_0]$$

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}_{12}}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{A} \text{ wins against } \overline{A12}] = \Pr[E_1]$$

Using equation $(\square)$ we obtain that $\Pr[E_0] = \Pr[E_1]$. Thus

$$\Pr[E_0] = \Pr[\mathsf{A} \text{ wins against mode } \overline{A10} \cap \overline{B} \cap \overline{C}] \leq \Pr[\mathsf{A} \text{ wins against mode } \overline{A12}] \leq \epsilon_{\mathsf{INT\text{-}CTXT1}}$$

since the mode $\overline{A12}$ is by hypothesis $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-secure. This concludes the proof, since we have proved that:

$$\Pr[\mathsf{A} \text{ wins against mode } \overline{A10}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{\mathsf{INT\text{-}CTXT1}}$$

Proof of Proposition 2

We want to prove that if mode $\overline{A11}$ is INT-CTXT1-secure, then mode $\overline{A10}$ is also INT-CTXT1 secure.

Before to give the proof we need a lemma, which proves the ivE-security of the ivE encryption scheme Π' described in Fig. 6 based on the ivE encryption scheme Π:

Lemma 4. *Let* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}}) - \mathsf{ivE}$ *secure* iv*-based* ivE *Encryption scheme. Let* $\mathsf{f}^{\mathsf{Enc}}(\cdot)$ *be randomly picked from the set* $\mathcal{FUNC}(\mathcal{IV}, \{0,1\}^N)$ *then the* ivE*-based Encryption scheme* $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ *described in Fig. 6 is* $(q, t, \epsilon) - \mathsf{ivE}$*-secure, where*

$$\epsilon \leq \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}$$

The proof is completely standard, since we have to consider the probability that there is a collision in the IVs during the different encryption queries.

Proof. Let A be a $(q, t) - \mathsf{ivE}$ adversary against the ivE scheme Π'.
We want to bound $|\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}} \Rightarrow 1] - \Pr[\mathsf{A}^{\$} \Rightarrow 1]|$. Let B be the event that there is a collision in the *iv*s, which are randomly picked. This probability is bounded by the well-known birthday bound (see ad example [15]), thus $\Pr[B] \leq \frac{q^2}{2|\mathcal{IV}|}$. Clearly using the Law of Total probability

$$\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1] = \Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|B] \Pr[B] + \Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|\overline{B}] \Pr[\overline{B}].$$

Now we want to bound $\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|B]$. We build a $(q, t) - \mathsf{ivE}$ adversary B against Π based on the ivE adversary A who is going against the ivE scheme Π'.The adversary B is built in this way:
At the start of the game the ivE adversary B picks at random a function $\mathsf{f}^{\mathsf{Enc}}(\cdot)$

from the set $\mathcal{FUNC}(\{0,1\}^N, \mathcal{IV})$.
When the ivE adversary A makes an encryption query on input m^i, B simply sees if m^i have to be parsed in (m_0^i, m_1^i). If it is not the case, he simply forwards m^i to his oracle, receiving c^i which he forwards to adversary A. Otherwise B parses the message m^i in (m_0^i, m_1^i) and queries his oracle on input m_1^i receiving (iv^i, c_1^i), he computes $c_0^i = \mathsf{f}^{\mathsf{Enc}}(iv^i) \oplus m_0^i$ and he forwards $c^i := (c_0^i, c_1^i)$.
At the end of the Game A outputs a bit b and B output the same bits.
We observe that, if event B does not happen, that is, if all the IVs are different, then B simulates correctly the game for the ivE adversary A since the c_0^i, when they are computed, are random values (if it is not the case, that is, there is a collision in the IVs, B is not able to correctly simulate the oracle if it is implemented with \$ for the adversary A). Thus we have proved that:

$$\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|\overline{B}] = \Pr[\mathsf{B}^{\mathsf{Enc}^{\$}(\cdot)} \Rightarrow 1|\overline{B}]$$

and

$$\Pr[\mathsf{A}^{\$(\cdot)} \Rightarrow 1|\overline{B}] = \Pr[\mathsf{B}^{\$(\cdot)} \Rightarrow 1|\overline{B}]$$

Thus

$$\Big|\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1] - \Pr[\mathsf{A}^{\$(\cdot)} \Rightarrow 1]\Big| =$$

$$\Big|\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|B]\Pr[B] + \Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}] -$$

$$\Pr[\mathsf{A}^{\$(\cdot)} \Rightarrow 1|B]\Pr[B] - \Pr[\mathsf{A}^{\$(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}]\Big| \leq$$

$$\Big|\Pr[\mathsf{A}^{\mathsf{Enc}'^{\$}(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}] - \Pr[\mathsf{A}^{\$(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}]\Big| + \frac{q^2}{2|\mathcal{IV}|} =$$

$$\Big|\Pr[\mathsf{B}^{\mathsf{Enc}^{\$}(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}] - \Pr[\mathsf{B}^{\$(\cdot)} \Rightarrow 1|\overline{B}]\Pr[\overline{B}]\Big| + \frac{q^2}{2|\mathcal{IV}|} \leq \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}$$

which concludes the proof.

The ivE scheme Π' is not efficiently implementable since it uses a random function, which cannot be efficiently computed. However, this is not a problem since it is used only for a proof.

Now we can prove the following proposition:

Proposition 2. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}_{10}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$*-secure encryption scheme. Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be a* $(0, t, \epsilon_{cr})$ *collision resistant hash function. Then, if mode* $\overline{A11}$*, implemented with the random function* $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$ *and with any* $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}) - \mathsf{ivE}$*-secure Encryption scheme, is* $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$-$\mathsf{INT\text{-}CTXT1}$*-secure then mode* $\overline{A10}$ *is* $(q-1, t, \epsilon)$-$\mathsf{INT\text{-}CTXT1}$*-secure, where*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\mathsf{INT\text{-}CTXT1}}.$$

Proof. Let A be a $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary.
Using Lemma 1 we have that

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

So, we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
Here, we reduce the $\mathsf{INT\text{-}CTXT1}$ security of the scheme $\overline{\boldsymbol{\Pi}}$, composed accordingly to mode $\overline{A10}$, to the $\mathsf{INT\text{-}CTXT1}$ security of the scheme $\overline{\boldsymbol{\Pi'}}$, composed accordingly to mode $\overline{A11}$. But, before to do it, we have to make a little change on the scheme $\overline{\boldsymbol{\Pi}}$, obtaining scheme $\overline{\boldsymbol{\Pi}_1}$ which is still composed according to the mode A10 paradigm. We explain the change and why it does not affect the $\mathsf{INT\text{-}CTXT1}$-security, using a sequence of two games:

Game 0 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}}$, implemented according to mode $\overline{A10}$. Let E_0 be the event that the adversary A wins this Game.

Game 1 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}_1}$, implemented according to mode $\overline{A10}$. The only difference is that now we have replaced $\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)$ with $\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot) := \mathsf{f}^{\mathsf{Tag}_{11}}(\mathsf{f}(\cdot)\|\cdot)$.
Let E_1 be the event that the adversary A wins this Game.

Transition between Game 0 and Game 1 We want to bound $|\Pr[E_0] - \Pr[E_1]|$.
To do this we build an adversary B who is facing an oracle $\mathcal{O}$ who is either implemented with $\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)$ or with $\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)$. The PRF-adversary B is built as follows:
First adversary B chooses a random function $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and a key $k_E \in \mathcal{K}_E$ for the ivE scheme Π. Then, when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B queries his oracle on input $(a^i, \mathbf{m}^i)$ obtaining τ^i. Then he computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$ and $c^i = \mathsf{Enc}_{k_E}(iv^i, m^i)$, with $m^i = \mathbf{m}^i\|\tau^i$, and he forwards c^i to adversary A. In this way B asks at most $q-1$ oracle queries.
When A makes his decryption query (n^q, a^q, c^q), B computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$. Then he decrypts c^q computing $c^q = (\mathbf{m}^q\|\tau^{q,c}) = \mathsf{Dec}_{k_E}(iv^q, c^q)$, he queries his oracle $\mathcal{O}$ on input $(a^q, \mathbf{m}^q)$ obtaining $\tau^{q,c}$ and he verifies if $\tau^{q,c} = \tau^q$. If the equality holds (that is, the decryption query (n^q, a^q, c^q) is valid), the PRF-adversary B outputs 1, otherwise he outputs 0.
We observe that if the oracle $\mathcal{O}$ is implemented with $\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)$ the $\mathsf{INT\text{-}CTXT1}$ adversary A is playing Game 0, otherwise he is playing Game 1.

The security of the oracle $\mathcal{O}(\cdot,\cdot)$ We observe that

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1]\right| \leq \frac{q^2}{2^{N+1}}$$

In fact, let event D be the event that there is a collision in the output of the random function $\mathsf{f}(\cdot)$. The probability of event D is bounded by $\frac{q^2}{2^{N+1}}$, due to

the well known birthday bound (see for example [15]). Using the law of total probability, we obtain that

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D] = (\circ)$$

We observe that if event D does not happen, the function $\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)$ is indistinguishable from the random function $\mathsf{f}^{\mathsf{Tag}_{10}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$, because for any new input $(a, \mathbf{m}) \in \mathcal{A} \times \mathcal{M}$ the output τ is picked uniformly at random in $\mathcal{T}$. Thus

$$(\circ) = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]$$

Thus we can bound

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1]\right| =$$

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1] - \left(\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]\right)\right|$$

$$\leq \Pr[D] \leq \frac{q^2}{2^{N+1}} = (\square)$$

$|\Pr[E_0] - \Pr[E_1]|$ We are now left to bound $|\Pr[E_0] - \Pr[E_1]|$. We observe that

$$\Pr[E_0] = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}_{10}}(\cdot,\cdot)} \Rightarrow 1]$$

$$\Pr[E_1] = \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}_{11}}(\cdot),\cdot)} \Rightarrow 1]$$

thus ,using $(\square)$ we obtain:

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{q^2}{2^N}$$

which immediately gives:

$$\left|\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] - \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}_1}]\right| \leq \frac{q^2}{2^{N+1}}$$

and

$$\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] \leq \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}_1}] + \frac{q^2}{2^{N+1}}$$

Now we build the scheme $\overline{\boldsymbol{\Pi}}'$ which is obtained according to the mode $\overline{A11}$ composing the $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{IV}}}$ (based on the random function $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$) and $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{Tag}_{11}}}$ (based on the random function $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$) and the iv-based encryption ivE scheme Π', where Π' is based on Π. Scheme Π' treats differently the first block, which is encrypted in $\mathsf{f}^{\mathsf{Enc}}(iv) \oplus m_1^i$. This can only be problems iff the IVs of different encryption queries are repeated. This probability is bounded by the birthday bound [see [15]]). The complete description of this scheme can be found in Fig. 6. (We use in the following c_0^i to encrypt

$\mathsf{f}(a^i)$ and makes the message depending on the AD). We have proved that Π' is $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|})$ secure (Lemma 4).
Now we uses a INT-CTXT1-adversary A against scheme $\overline{\boldsymbol{\Pi}_1}$ (type $\overline{A10}$) to build a INT-CTXT1-adversary C against scheme $\overline{\boldsymbol{\Pi}'}$ (type $\overline{A11}$).
The INT-CTXT1-adversary C has access to the oracle $\mathsf{AEnc}'(\cdot,\cdot,\cdot)$ which is implemented according to scheme $\overline{\boldsymbol{\Pi}'}$.
First the adversary C picks uniformly at random a function $\mathsf{f} : \mathcal{A} \longmapsto \{0,1\}^N$, from
$\mathcal{FUNC}(\mathcal{A}, \{0,1\}^N)$. Then when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, C computes $\mathsf{f}(a^i)$ and asks an encryption query on input $(n^i, a^i, \mathbf{m}'^i)$ with $\mathbf{m}'^i := \mathsf{f}(a^i)\|m^i$ obtaining $c^i = (c_0^i, c_1^i)$. Then he forwards c_1^i to adversary A. When the adversary A asks his decryption query (n^q, a^q, c^q) with $(n^q, a^q) = (n^j, a^j)$ for a certain $j \in \{1, ..., q-1\}$ (this j is unique since n is a nonce), the adversary C simply asks to his decryption query $(n^q, a^q, (c_0^j, c^q))$. We observe that $c_0^j = \mathsf{f}^{\mathsf{Enc}}(iv^j) \oplus \mathsf{f}(a^j) = \mathsf{f}^{\mathsf{Enc}}(iv^q) \oplus \mathsf{f}(a^q)$ since $iv^j = iv^q$ and $a^j = a^q$. Now if the decryption query made by A is valid, this decryption query is valid since the tag in the first case is computed as $\mathsf{f}'^{\mathsf{Tag}_{11}}(a^q, \mathbf{m}^q)$, where $\mathbf{m}^q$ is the decryption of c^q, while in the second case it is computed as $\mathsf{f}^{\mathsf{Tag}_{11}}(\mathsf{f}(a^q)\|\mathbf{m}^q)$. Since $\overline{\boldsymbol{\Pi}'}$ is an $\overline{A11}$ authenticated encryption scheme which is $(q, t, \epsilon_{\text{INT-CTXT1}}) - \text{INT-CTXT1}$ secure, since Π' is $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}) - \mathsf{ivE}$ secure due to Lemma 4, then, the probability that the INT-CTXT1 adversary C forges is bounded by $\epsilon_{\text{INT-CTXT1}}$. Thus, the probability that the INT-CTXT1 adversary A forges scheme $\overline{\boldsymbol{\Pi}_1}$ is bounded by $\epsilon_{\text{INT-CTXT1}}$.
Thus

$$\Pr[\mathsf{A} \text{ forges against } \overline{\boldsymbol{\Pi}}|\overline{B} \cap \overline{C}] \leq \frac{q^2}{2^{N+1}} + \epsilon_{\text{INT-CTXT1}}$$

Consequently we obtain that $\overline{\boldsymbol{\Pi}}$ is $(q, t, \epsilon) - \text{INT-CTXT1}$ secure with

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \frac{q^2}{2^{N+1}} + \epsilon_{\text{INT-CTXT1}}$$

Proof of Proposition 3

We want to prove that if mode $\overline{A10}$ is INT-CTXT1 secure than mode $\overline{A12}$ is also INT-CTXT1 secure.

Proposition 3. *Let* $\mathsf{f}^{\mathsf{IV}_{12}} : \mathcal{N} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-ivE*-secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE*-scheme obtained composing these components according to mode* $\overline{A12}$*. Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be* $(0, t, \epsilon_{cr})$.
Then, if mode $\overline{A10}$*, implemented with the random function* $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and with any* $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}) - \mathsf{ivE}$*-secure Encryption scheme, is* $(q, t, \epsilon_{\text{INT-CTXT1}})$-INT-CTXT1*-secure then mode* $\overline{A12}$ *is* $(q-1, t, \epsilon)$-INT-CTXT1*-secure with*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\text{INT-CTXT1}}.$$

Proof. Let A be a $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary.
Using Lemma 1 we have that

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

So, we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
Here, we reduce the $\mathsf{INT\text{-}CTXT1}$ security of the scheme $\overline{\boldsymbol{\Pi}}$, composed accordingly to mode $\overline{A12}$, to the $\mathsf{INT\text{-}CTXT1}$ security of the scheme $\overline{\boldsymbol{\Pi}}_{10}$, composed accordingly to mode $\overline{A10}$. But, before to do it, we have to do a little change on scheme $\overline{\boldsymbol{\Pi}}$, obtaining scheme $\overline{\boldsymbol{\Pi}'}$, which is still composed according to mode $\overline{A12}$. We explain the change and why it does not affect the $\mathsf{INT\text{-}CTXT1}$ security using a sequence of two games:

Game 0 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}}$, implemented according to mode $\overline{A12}$. Let E_0 be the event that the adversary A wins this Game.

Game 1 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}'}$, implemented according to mode $\overline{A12}$. The only difference is that now we have replaced $\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)$ with $\mathsf{f}'^{\mathsf{Tag}}(a,\mathbf{m}) := \mathsf{f}^{\mathsf{Tag}}(a_f, \mathsf{f}(a)\|\mathbf{m})$ where $a_f \in \mathcal{A}$ is a fixed AD.
Let E_1 be the event that the adversary A wins this Game.

Transition between Game 0 and Game 1 We want to bound $|\Pr[E_0] - \Pr[E_1]|$.
To do this we build a $(q,t)-\mathrm{PRF}$ adversary B who is facing an oracle $\mathcal{O}$ who is either implemented with $\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)$ or with $\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)$. The PRF-adversary B is built as follows:
First adversary B chooses a random function $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \longmapsto \mathcal{IV}$ and a key $k_E \in \mathcal{K}_E$ for Π. Then, when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B queries his oracle on input $(a^i, \mathbf{m}^i)$ obtaining τ^i. Then, he computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i)$ and $c^i = \mathsf{Enc}_{k_E}(iv^i, m^i)$ with $m^i := \mathbf{m}^i\|\tau^i$ and he forwards c^i to adversary A. In this way B asks at most $q-1$ oracle queries.
When A makes his decryption query (n^q, a^q, c^q), B computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q)$. Then, he decrypts c^q computing $c^q = (\mathbf{m}^q\|\tau^{q,c}) = \mathsf{Dec}_{k_E}(iv^q, c^q)$, he queries his oracle $\mathcal{O}$ on input $(a^q, \mathbf{m}^q)$ obtaining $\tau^{q,c}$ and he verifies if $\tau^{q,c} = \tau^q$. If the equality holds (that is, the decryption query (n^q, a^q, c^q) is valid), the PRF-adversary B outputs 1, otherwise he outputs 0.
We observe that if the oracle $\mathcal{O}$ is implemented with $\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)$ the $\mathsf{INT\text{-}CTXT1}$ adversary A is playing Game 0, otherwise he is playing Game 1.

The security of the oracle $\mathcal{O}(\cdot,\cdot)$ We observe that

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1]\right| \leq \frac{q^2}{2^{N+1}}$$

In fact, let event D be the event that there is a collision in the output of the random function $\mathsf{f}(\cdot)$. The probability of event D is bounded by $\frac{q^2}{2^{N+1}}$, due to

the well known birthday bound (see for example [15]). Using the law of total probability, we obtain that

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1] =$$

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D] = (\circ)$$

We observe that if event D does not happen, the function $\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)$ is indistinguishable from the random function $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$, because for any new input $(a, \mathbf{m}) \in \mathcal{A} \times \mathcal{M}$ the output τ is picked uniformly at random in $\mathcal{T}$. Thus

$$(\circ) = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]$$

Thus we can bound

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1]\right| =$$

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1] - \left(\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]\right)\right|$$

$$\leq \Pr[D] \leq \frac{q^2}{2^{N+1}} = (\square)$$

$|\Pr[E_0] - \Pr[E_1]|$ We are now left to bound $|\Pr[E_0] - \Pr[E_1]|$. We observe that

$$\Pr[E_0] = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1]$$

$$\Pr[E_1] = \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{Tag}}(\cdot,\cdot)} \Rightarrow 1]$$

thus ,using $(\square)$ we obtain:

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{q^2}{2^{N+1}}$$

which immediately gives:

$$\left|\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] - \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}'}]\right| \leq \frac{q^2}{2^{N+1}}$$

and

$$\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] \leq \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}'}] + \frac{q^2}{2^{N+1}}$$

Now we build the scheme $\overline{\boldsymbol{\Pi}_{10}}$ which is obtained according to the scheme $\overline{A10}$ composing the $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{IV}}}$ (based on the random function $\mathsf{f}^{\mathsf{IV}_{10}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$) and $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{Tag}}}$ (based on the random function $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$) and the IV-based ivE encryption scheme Π' based on the ivE Encryption scheme Π, used already in the proof of Prop. 2 and described in Fig. 6.
Now we uses a $\mathsf{INT\text{-}CTXT1}$-adversary A against scheme $\overline{\boldsymbol{\Pi}'}$ (mode $\overline{A12}$) to build

a INT-CTXT1-adversary C against scheme $\overline{\boldsymbol{\Pi}_{10}}$ (mode $\overline{A10}$).

The INT-CTXT1-adversary C has access to the oracle $\overline{\mathsf{AEnc}_{10}}(\cdot,\cdot,\cdot)$ which is implemented according to scheme $\overline{\boldsymbol{\Pi}_{10}}$. First the adversary C picks a random function $\mathsf{f} : \mathcal{A} \longmapsto \{0,1\}^N$, from the family $\mathcal{FUNC}(\mathcal{A},\{0,1\}^N)$. Then he picks an associated data $a_f \in \mathcal{A}$.
When the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, C computes $\mathsf{f}(a^i)$ and asks an encryption query on input $(n^i, a_f, \mathbf{m}'^i)$ where $\mathbf{m}'^i := \mathsf{f}(a^i)\|\mathbf{m}^i$ obtaining $c^i = (c_0^i, c_1^i)$. Then he forwards c_1^i to adversary A. When the adversary A asks his decryption query (n^q, a^q, c^q) with $(n^q, a^q) = (n^j, a^j)$ for a certain $j \in \{1, ..., q-1\}$ (this j is unique since n is a nonce), the adversary C simply asks to his decryption query $(n^q, a_f, (c_0^j, c^q))$. We observe that $c_0^j = \mathsf{f}^{\mathsf{Enc}}(iv^j) \oplus \mathsf{f}(a^j) = \mathsf{f}^{\mathsf{Enc}}(iv^q) \oplus \mathsf{f}(a^q)$ since $iv^j = iv^q$ and $a^j = a^q$. Now if the decryption query made by A is valid, the decryption query made by B is valid since the tag in the first case is computed as $\mathsf{f}^{\mathsf{Tag}}(a_f, \mathsf{f}(a^q)\|\mathbf{m}^q)$, where $\mathbf{m}^q$ is the decryption of c^q, while in the second case it is computed as $f^{\mathsf{Tag}}(a_f, \mathbf{m}'^q)$ with $\mathbf{m}'^q = \mathsf{f}(a^q)\|\mathbf{m}^q$. Since $\overline{\boldsymbol{\Pi}_{10}}$ is an $\overline{A10}$ authenticated encryption scheme which is $(q, t, \epsilon_{\text{INT-CTXT1}})$-secure, since Π' is $(q, t, \epsilon_{\mathsf{ivE}} + \frac{q^2}{2|\mathcal{IV}|}) - \mathsf{ivE}$ secure due to Lemma 4, then the probability that the INT-CTXT1 adversary C forges is bounded by $\epsilon_{\text{INT-CTXT1}}$. Thus the probability that the INT-CTXT1 adversary A forges scheme $\overline{\boldsymbol{\Pi}'}$ is bounded by $\epsilon_{\text{INT-CTXT1}}$.
Thus

$$\Pr[\mathsf{A} \text{ forges against } \overline{\boldsymbol{\Pi}} | \overline{B} \cap \overline{C}] \leq \frac{q^2}{2^{N+1}} + \epsilon_{\text{INT-CTXT1}}$$

Consequently we obtain that $\overline{\boldsymbol{\Pi}}$ is $(q, t, \epsilon) - \text{INT-CTXT1}$ secure with

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \frac{q^2}{2^{N+1}} + \epsilon_{\text{INT-CTXT1}}$$

Proof of Proposition 4

We want to prove that if mode $\overline{A10}$ is INT-CTXT1 secure than mode $\overline{A11}$ is also INT-CTXT1 secure.

Proposition 4. *Let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions and let* $\Pi = (\mathcal{K}_E, \mathsf{Enc}, \mathsf{Dec})$ *be a* $(q, t, \epsilon_{\mathsf{ivE}})$-ivE-*secure encryption scheme. Let* $\overline{\boldsymbol{\Pi}}$ *be the* nAE *scheme obtained composing these components according to mode* $\overline{A11}$. *Let* $\mathsf{H} : \mathcal{A} \longmapsto \{0,1\}^N$ *be a* $(0, t, \epsilon_{cr})$-*collision resistant hash function.*
Then, if mode $\overline{A10}$, *implemented with the random function* $\mathsf{f}^{\mathsf{Tag}_{10}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$, *is* $(q, t, \epsilon_{\text{INT-CTXT1}})$-INT-CTXT1-*secure then mode* $\overline{A11}$ *is* $(q-1, t, \epsilon')$-INT-CTXT1-*secure with*

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \epsilon_{cr} + \epsilon_{\text{INT-CTXT1}}.$$

Proof. Let A be a $(q-1, t) - \text{INT-CTXT1}$ adversary.
Using Lemma 1 we have that

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

So, we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
Here, we reduce the INT-CTXT1 security of the scheme $\overline{\boldsymbol{\Pi}}$, composed accordingly to mode $\overline{A11}$, to the INT-CTXT1 security of the scheme $\overline{\boldsymbol{\Pi}}_{10}$, composed accordingly to mode $\overline{A10}$. But, before to do it, we have to do a little change on scheme $\overline{\boldsymbol{\Pi}}$, obtaining scheme $\overline{\boldsymbol{\Pi}'}$, which is still composed according to mode $\overline{A11}$. We explain the change and why it does not affect the INT-CTXT1 security using a sequence of two games:

Game 0 It is the standard INT-CTXT1 game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}}$, implemented according to mode $\overline{A11}$. Let E_0 be the event that the adversary A wins this Game.

Game 1 It is the standard INT-CTXT1 game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}'}$, implemented according to mode $\overline{A11}$. The only difference is that now we have replaced $\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)$ with $\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot) := \mathsf{f}^{\mathsf{IV}}(\cdot\|\mathsf{f}(\cdot))$.
Let E_1 be the event that the adversary A wins this Game.

Transition between Game 0 and Game 1 We want to bound $|\Pr[E_0] - \Pr[E_1]|$. To do this we build a $(q,t)-$PRF) adversary B who is facing an oracle $\mathcal{O}$ who is either implemented with $\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)$ or with $\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)$. The PRF-adversary B is built as follows:
First adversary B chooses a random function $\mathsf{f}^{\mathsf{Tag}_{11}} : \mathcal{M} \longmapsto \mathcal{T}$ and a key $k_E \in \mathcal{K}_E$ for Π. Then, when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B queries his oracle on input (n^i, a^i) obtaining iv^i. Then he computes $\tau^i = \mathsf{f}^{\mathsf{Tag}_{11}}(\mathbf{m}^i)$ and $c^i = \mathsf{Enc}_{k_E}(iv^i, m^i)$ with $m^i := \mathbf{m}^i\|\tau^i$ and he forwards c^i to adversary A. In this way B asks at most $q-1$ oracle queries.
When A makes his decryption query (n^q, a^q, c^q), B calls his oracle $\mathcal{O}$ on input (n^q, a^q) obtaining iv^q. Then he decrypts c^q computing $c^q = (\mathbf{m}^q\|\tau^{q,c}) = \mathsf{Dec}_{k_E}(iv^q, c^q)$, he computes $\tau^{q,c} = \mathsf{f}^{\mathsf{Tag}_{11}}(\mathbf{m}^q)$ and he verifies if $\tau^{q,c} = \tau^q$. If the equality holds (that is, the decryption query (n^q, a^q, c^q) is valid), the PRF-adversary B outputs 1, otherwise he outputs 0.
We observe that if the oracle $\mathcal{O}$ is implemented with $\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)$ the INT-CTXT1 adversary A is playing Game 0, otherwise he is playing Game 1.

The security of the oracle $\mathcal{O}(\cdot,\cdot)$ We observe that

$$\left|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot} \Rightarrow 1]\right| \leq \frac{q^2}{2^{N+1}}$$

In fact, let event D be the event that there is a collision in the output of the random function $\mathsf{f}(\cdot)$. The probability of event D is bounded by $\frac{q^2}{2^{N+1}}$, due to the well known birthday bound (see for example [15]). Using the law of total probability, we obtain that

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1] =$$

$$\Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D] = (\circ)$$

We observe that if event D does not happen, the function $\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)$ is indistinguishable from the random function $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$, because for any new input $(n, a) \in \mathcal{N} \times \mathcal{A}$ the output iv is picked uniformly at random in $\mathcal{IV}$. Thus

$$(\circ) = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]$$

Thus we can bound

$$\Big|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1]\Big| =$$

$$\Big|\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1] - \Big(\Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|\overline{D}]\Pr[\overline{D}] + \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1|D]\Pr[D]\Big)\Big|$$

$$\leq \Pr[B] \leq \frac{q^2}{2^{N+1}} = (\square)$$

$|\Pr[E_0] - \Pr[E_1]| \leq \frac{q^2}{2^{N+1}}$ We are now left to bound $|\Pr[E_0] - \Pr[E_1]|$. We observe that

$$\Pr[E_0] = \Pr[\mathsf{B}^{\mathsf{f}^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1]$$

$$\Pr[E_1] = \Pr[\mathsf{B}^{\mathsf{f}'^{\mathsf{IV}}(\cdot,\cdot)} \Rightarrow 1]$$

thus, using $(\square)$ we obtain:

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{q^2}{2^{N+1}}$$

which immediately gives:

$$\Big|\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] - \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}'}]\Big| \leq \frac{q^2}{2^{N+1}}$$

and

$$\Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}}] \leq \Pr[\mathsf{A} \text{ wins against scheme } \overline{\boldsymbol{\Pi}'}] + \frac{q^2}{2^{N+1}}$$

Now we build the scheme $\overline{\boldsymbol{\Pi}_{10}}$ which is obtained according to the scheme $\overline{A10}$ composing the $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{IV}}}$ (based on the random function $\mathsf{f}'^{\mathsf{IV}} : \mathcal{N}' \times \mathcal{A} \longmapsto \mathcal{IV}$) with $\mathcal{N}' := \mathcal{N} \times \{0,1\}^N$, and $\mathsf{vecMAC}\ \overline{\mathsf{MAC}^{\mathsf{Tag}}}$ (based on the random function $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$) and the iv-based encryption scheme Π.

Now we uses a $\mathsf{INT\text{-}CTXT1}$-adversary A against scheme $\overline{\boldsymbol{\Pi}'}$ (mode $\overline{A12}$) to build a
$\mathsf{INT\text{-}CTXT1}$-adversary C against scheme $\overline{\boldsymbol{\Pi}_{10}}$ (mode $\overline{A10}$).

The $\mathsf{INT\text{-}CTXT1}$-adversary C has access to the oracle $\overline{\mathsf{AEnc}_{10}}(\cdot,\cdot,\cdot)$ which is implemented according to scheme $\overline{\boldsymbol{\Pi}_{10}}$. First the adversary C picks a random

function $\mathsf{f} : \mathcal{A} \longmapsto \{0,1\}^N$, from the family $\mathcal{FUNC}(\mathcal{A}, \{0,1\}^N)$. Then he picks an associated data $a_f \in \mathcal{A}$.
When the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, C computes $\mathsf{f}(a^i)$ and asks an encryption query on input $(n'^i, a_f, \mathbf{m}^i)$ with and $n'^i := n^i \| \mathsf{f}(a^i)$ obtaining c^i which he forwards to adversary A. When the adversary A asks his decryption query (n^q, a^q, c^q) with $(n^q, a^q) = (n^j, a^j)$ for a certain $j \in \{1, ..., q-1\}$ (this j is unique since n is a nonce), the adversary C simply asks to his decryption query $(n^q \| \mathsf{f}(a^q), a_f, c^q))$. Now if the decryption query made by A is valid, this decryption query is valid since for A the iv should be computed as $\mathsf{f}'^{\mathsf{IV}}(n^q \| \mathsf{f}(a^q))$, while in the second case it is computed as $\mathsf{f}^{\mathsf{IV}}(n'^q, a_f)$ with $n'q = n^q \| \mathsf{f}(a^q)$. Since a_f is constant in all the queries made by C we can ignore it. Moreover for A the tag should be computed as $\mathsf{f}^{\mathsf{Tag}_{11}}(\mathbf{m}^q)$ while for C it should be computed as $\mathsf{f}^{\mathsf{Tag}_{10}}(a_f, \mathbf{m}^q)$, but again, since a_f is constant in all the queries made by C, we can ignore it and the tag is correct in both cases. The nAE scheme $\overline{\boldsymbol{\Pi}_1 0}$ is by hypothesis $(q-1, t, \epsilon_{\mathsf{INT\text{-}CTXT1}})$, thus the probability that the INT-CTXT1 adversary A forges scheme $\overline{\boldsymbol{\Pi}'}$ is bounded by $\epsilon_{\mathsf{INT\text{-}CTXT1}}$.
Thus

$$\Pr[\mathsf{A} \text{ forges against } \overline{\boldsymbol{\Pi}} | \overline{B} \cap \overline{C}] \leq \frac{q^2}{2^{N+1}} + \epsilon_{\mathsf{INT\text{-}CTXT1}}$$

Consequently we obtain that $\overline{\boldsymbol{\Pi}}$ is $(q, t, \epsilon) - \mathsf{INT\text{-}CTXT1}$ secure with

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + \frac{q^2}{2^{N+1}} + \epsilon_{\mathsf{INT\text{-}CTXT1}}$$

F.4 Proofs for secure variants of modes A10, A11 and A12

Proof of Proposition 5

We want to prove that mode $\overline{A10}$ is INT-CTXT1-secure if the ivE Encryption scheme Π is misuse resistant.

Proposition 5. *Let the* ivE *scheme* Π *be a* $(q, t, \epsilon_{\mathsf{mrE}})$*-misuse resistant* mrE *and* $(q, t, \epsilon_{\mathsf{ivE}}) - \mathsf{ivE}$ *secure, let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions. Then, the scheme* $\overline{\boldsymbol{\Pi}}$ *obtained composing these components according to mode* $\overline{A10}$*, is* $(q-1, t, (q-1)|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + (q-1)\epsilon_{\mathsf{mrE}}) -$ INT-CTXT1*-secure.*

Proof. Let A be a $(q-1, t) - \mathsf{INT\text{-}CTXT1}$ adversary.
Using Lemma 1 we have that

$$\Pr[\mathsf{A} \text{ wins } \cap C] + \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}}$$

So, we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
In this case, we can reduce the $(q, t) - \mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to a $(q, t) - \mathsf{mrE}$ adversary B against Π, which is $(q, t, \epsilon_{\mathsf{mrE}}) - \mathsf{mrE}$-secure, by hypothesis. The $(q, t) - \mathsf{mrE}$ adversary B is built in this way:
First adversary B chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and

$\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$. Then when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$ and $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$. Then the adversary B queries his oracle (which is either implemented with $\mathsf{Enc}(\cdot,\cdot)$ or with a random function $\$(\cdot,\cdot)$ on input (iv^i, m^i), with $m^i = \mathbf{m}^i \| \tau^i$) receiving c^i, which he forwards to adversary A. When A makes his decryption query (n^q, a^q, c^q), B computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$. Let $\mathcal{J}$ be the set of index $i = 1, ..., q-1$ s.t. $a^q = a^j$. Clearly $|\mathcal{J}| \leq q-2$. Then the adversary B picks an index $j \leftarrow \mathcal{J}$ uniformly at random and queries his oracle on input (iv^q, m^q) with $m^q := \mathbf{m}^j \| \tau^j$ obtaining c^j. If $c^j = c^q$ he outputs 1, otherwise 0.

$$\Pr[\mathsf{B}^{\mathsf{Enc}(\cdot,\cdot)} \Rightarrow 1] =$$

$$\Pr[j \text{ correct }] \Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}] = \frac{1}{|\mathcal{J}|} \Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$$

$$\Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1] = \Pr[\$(iv^q, m^j) = c^q] = |\mathsf{Enc}(iv^q, m^j)|^{-1}$$

$$\leq |\mathcal{T}|^{-1} \cdot |m^j|^{-1} \leq |\mathcal{T}|^{-1}$$

Since Enc is $(q, t, \epsilon_{\mathsf{mrE}}) - \mathsf{mrE}$-secure ivE Encryption scheme and B is a $(q, t) - \mathsf{mrE}$ adversary

$$\Pr[\mathsf{B}^{\mathsf{Enc}(\cdot,\cdot)} \Rightarrow 1] \leq \Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1] + \epsilon_{\mathsf{mrE}}$$

Thus

$$\frac{1}{|\mathcal{J}|} \Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}] \leq |\mathsf{Enc}(iv^q, m^j)|^{-1} + \epsilon_{\mathsf{mrE}}$$

Consequently

$$\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}] \leq \left(|\mathsf{Enc}(iv^q, m^j)|^{-1} + \epsilon_{\mathsf{mrE}}\right) |\mathcal{J}| \leq (q-1) \left(|\mathcal{T}|^{-1} + \epsilon_{\mathsf{mrE}}\right)$$

Consequently we obtain that the nAE scheme $\overline{\boldsymbol{\Pi}}$ is $(q-1, t, \epsilon) - \mathsf{INT\text{-}CTXT1}$ secure, with

$$\epsilon = q|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + (q-1)\left(|\mathcal{T}|^{-1} + \epsilon_{\mathsf{mrE}}\right) = (2q-1)|\mathcal{T}|^{-1} + (q-1)\epsilon_{\mathsf{ivE}} + (q-1)\epsilon_{\mathsf{mrE}}.$$

Better bound for the INT-CTXT1-security of mode $\overline{A10}$ using a misuse resistant ivE scheme

We can have a better bound if we decide to give the mrE adversary B more encryption queries.

Proposition 12. *Let the* ivE *scheme* π *be a* $(2q-2, t, \epsilon_{\mathsf{mrE}})$*-misuse resistant* mrE *scheme, let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions. Then the scheme* $\overline{\boldsymbol{\Pi}}$*, obtained composing these components according to mode* $\overline{A10}$ *is* $(q-1, t, \frac{2q-1}{|\mathcal{T}|} + 2\epsilon_{\mathsf{mrE}}) - \mathsf{INT\text{-}CTXT1}$*-secure.*

Proof. To have a better bound we cannot use Lemma 1, but we have to redo its proof.
Let A be a $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary.
We start computing

$$\Pr[\mathsf{A} \text{ wins } \cap C] = \Pr[\mathsf{A} \text{ wins} \cap (a^q, \mathbf{m}^q) \neq (a^j, \mathbf{m}^j)\ \forall j = 1, ..., q-1]$$

This is bounded by $|\mathcal{T}|^{-1}$ because the probability that the tag τ^q is correct is $|\mathcal{T}|^{-1}$ since $\tau^{q,c} = \mathsf{f}^{\mathsf{Tag}}(a^q, \mathbf{m}^q)$ is picked uniformly at random after the adversary A outputs the decryption query since the tag τ^q has never been computed before, as in Lemma 1.

Then we compute $\Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] =$

$$\Pr[\mathsf{A} \text{ wins} \cap (n^q, a^q) \neq (n^i, a^i)\ \forall i = 1, ..., q-1 \cap \exists j \in \{1, ..., q-1\} \text{ s.t. } (a^q, \mathbf{m}^q) = (a^j, \mathbf{m}^j)]$$

In fact let A be a $(q,t)-\mathsf{INT\text{-}CTXT1}$ adversary against scheme $\overline{\boldsymbol{\Pi}}$ and we suppose that event B happens and event C does not happen. Now we build, based on A, a $(2q-2,t)-\mathsf{mrE}$ adversary B against scheme Π. The mrE-adversary B faces an oracle which is either implemented with $\mathsf{Enc}_{k_E}(\cdot,\cdot)$ or with $\$(\cdot,\cdot)$. The ivE-adversary B is constructed in this way:
First the adversary B chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$. Then, when the $\mathsf{INT\text{-}CTXT1}$-adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary B computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$ and $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$. Then the ivE-adversary B queries his oracle on input $(iv^i, \mathbf{m}^i \| \tau^i)$ receiving c^i, which he forwards to the adversary A. In this way B asks at most $q-1$ oracle queries.
When A makes his decryption query (n^q, a^q, c^q), B computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$. Let $\mathcal{J}$ be the set of index $j = 1, ..., q-1$ s.t. $a^q = a^j$ (Clearly $|\mathcal{J}| \leq q-1$). Now adversary B, asks for every $j \in \mathcal{J}$ B recomputes $\tau^j = \mathsf{f}^{\mathsf{Tag}}(a^j, \mathbf{m}^j)$ and he queries his oracle [which is either implemented with $\mathsf{Enc}(\cdot,\cdot)$ or with a random oracle $\$(\cdot,\cdot)$] on input $(iv^q, \mathbf{m}^j \| \tau^j)$ obtaining the ciphertext $c^{q,j,c}$. Doing this, the adversary B asks his last $q-1$ queries of the $2q-2$ oracle queries he has granted to. If $\exists j \in \mathcal{J}$ s.t. $c^{q,j,c} = c^q$ he outputs 1, otherwise 0.
Since event C has happened and $\mathsf{Enc}_{k_E}(iv^q, \cdot)$ is an injective function, we obtain

$$\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}]$$

On the other hand

$$\Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1] = \Pr[\exists j \in \mathcal{J}\ s.t.\ (iv^q, m^j \| \tau^j) = c^q] \leq$$

$$1 - \left(1 - |\mathcal{T}|^{-1} \cdot |m^j|^{-1}\right)^{q-1} \leq 1 - \left(1 - |\mathcal{T}|^{-1}\right)^{q-1} \leq \frac{q-1}{|\mathcal{T}|}$$

But, since the ivE-scheme Π is $(q, t, \epsilon_{\mathsf{mrE}})$-secure, by definition (Def. 20), we have that

$$\left|\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1]\right| \leq \epsilon_{\mathsf{mrE}}$$

Thus

$$\Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] \leq \epsilon_{\mathsf{mrE}} + \frac{q-1}{|\mathcal{T}|}$$

then

$$\Pr[\mathsf{A} \text{ wins } \cap B \cap \overline{C}] \leq \Pr[\mathsf{B}^{\mathsf{Enc}_{k_E}(\cdot,\cdot)} \Rightarrow 1] \leq \epsilon_{\mathsf{mrE}} + \frac{q-1}{|\mathcal{T}|}$$

Now we only have to compute $\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$.
In this case, we can reduce the $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to a $(2q-2,t)-\mathsf{mrE}$ adversary C against Π, which is $(2q-2,t,\epsilon_{\mathsf{mrE}})-\mathsf{mrE}$-secure, by hypothesis. The $(2q-2,t)-\mathsf{mrE}$ adversary C is built in this way:
First adversary C chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$. Then when the adversary A asks an encryption query on input $(n^i, a^i, \mathbf{m}^i)$, the adversary C computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$ and $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$. Then the adversary C queries his oracle (which is either implemented with $\mathsf{Enc}(\cdot,\cdot)$ or with a random function $\$(\cdot,\cdot)$ on input (iv^i, m^i), with $m^i = \mathbf{m}^i \| \tau^i$) receiving c^i, which he forwards to adversary A. When A makes his decryption query (n^q, a^q, c^q), C computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$. Then the adversary C for every $j \in \mathcal{J}$ queries his oracle on input (iv^q, m^q) with $m^q := \mathbf{m}^j \| \tau^j$ obtaining $c^{q,j}$. If $c^{q,j} = c^q$ he outputs 1, otherwise 0. In this way C asks at most $q-1$ queries not surpassing his total of $2q-2$ oracle queries he is allowed to.

$$\Pr[\mathsf{C}^{\mathsf{Enc}(\cdot,\cdot)} \Rightarrow 1] = \Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}]$$

$$\Pr[\mathsf{C}^{\$(\cdot,\cdot)} \Rightarrow 1] = \Pr[\exists j \in \mathcal{J} \text{ s.t. } \$(iv^q, m^j) = c^q] = \left(|\mathsf{Enc}(iv^q, m^j)|^{-1}\right)^{q-1} \leq \frac{q-1}{|\mathcal{T}|}$$

Since Enc is $(q,t,\epsilon_{\mathsf{mrE}})-\mathsf{mrE}$-secure ivE Encryption scheme and B is a $(q,t)-\mathsf{mrE}$ adversary

$$\Pr[\mathsf{B}^{\mathsf{Enc}(\cdot,\cdot)} \Rightarrow 1] \leq \Pr[\mathsf{B}^{\$(\cdot,\cdot)} \Rightarrow 1] + \epsilon_{\mathsf{mrE}}$$

Thus

$$\Pr[\mathsf{A} \text{ wins } \cap \overline{B} \cap \overline{C}] \leq \frac{q-1}{|\mathcal{T}|} + \epsilon_{\mathsf{mrE}}$$

Consequently we obtain that the nAE scheme $\overline{\boldsymbol{\Pi}}$ is $(q-1,t,\epsilon) - \mathsf{INT\text{-}CTXT1}$ secure, with

$$\epsilon = \frac{1}{|\mathcal{T}|} + \epsilon_{\mathsf{mrE}} + \frac{q-1}{|\mathcal{T}|} + \frac{q-1}{|\mathcal{T}|} + \epsilon_{\mathsf{mrE}} = \frac{2q-1}{|\mathcal{T}|} + 2\epsilon_{\mathsf{mrE}}.$$

Proof of Prop. 6

We want to prove the $\mathsf{INT\text{-}CTXT1}$ security of mode $\overline{A10}$ if the ivE-scheme is "message-malleable".

Proposition 6. *Let the* ivE *scheme* Π *be* $(q,t,\epsilon_{\mathsf{ivE}})$-$\mathsf{ivE}$-*secure,* $(q-1,t,\epsilon_{\mathsf{mCPA}})$-$\mathsf{mCPA}$-*secure and "message-malleable", let* $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ *and* $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ *be two random functions. Then, the scheme* $\overline{\boldsymbol{\Pi}}$ *obtained composing these components according to mode* $\overline{A10}$*, is* $(q,t,(q-1)\epsilon_{\mathsf{ivE}} + q|\mathcal{T}|^{-1} + 8\epsilon_{\mathsf{mCPA}}) - \mathsf{INT\text{-}CTXT1}$*-secure.*

Proof. Let A be a $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary.
Let event B (that is, (n^q, a^q) is fresh) and C (that is, $(a^q, \mathbf{m}^q)$ as in Lemma 1.
Using the proof of Lemma 1 we can prove that $\Pr[\mathsf{A} \text{ wins } |B] \leq (q-1)(\epsilon_{\mathsf{ivE}} + |\mathcal{T}|^{-1})$.
Now, we can reduce the $(q,t)-\mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to two $(q-1,t)-\mathsf{mCPA}$ adversary B and C against Π, which is $(q,t,\epsilon_{\mathsf{mCPA}})-\mathsf{mCPA}$-secure, by hypothesis. To do this, we need two Games:

Game 0 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}}$ implemented according to mode $\overline{A1\$0}$. Let E_0 be the event that the adversary A wins this game. Let B_0 the event B in Game 0.

Game 1 It is the standard $\mathsf{INT\text{-}CTXT1}$ game where the adversary A faces scheme $\overline{\boldsymbol{\Pi}}'$ which is a variant of scheme $\overline{\boldsymbol{\Pi}}$: instead of computing $c^i \leftarrow \mathsf{Enc}(iv^i, m^i \| \tau^i)$, $\overline{\mathsf{AEnc}}$ picks uniformly at random in the set $\mathcal{T}$ a value r^i and then it computes $c \leftarrow \mathsf{Enc}(iv^i, m^i \| r^i)$; on the other hand $\overline{\mathsf{Dec}}$ is not changed (this implies that $\overline{\mathsf{Dec}}$ is not able to decrypt correctly, with overwhelming probability the encryptions $\overline{\mathsf{AEnc}}$ makes). Let E_1 be the event that the adversary A wins this game. Let B_1 the event B in Game 1.

Now want to bound $|\Pr[\overline{B}_0] - \Pr[\overline{B_1}]|$, then we can use this result to bound $|\Pr[\mathsf{A} \text{ wins } |\overline{B}_0] - \Pr[\mathsf{A} \text{ wins } |\overline{B}_1]|$.
We bound the equality $|\Pr[\overline{B}_0] - \Pr[\overline{B}_1]|$ (r. $|\Pr[E_0 \cap \overline{B}_0] - \Pr[E_1 \cap \overline{B}_1]|$) using an mCPA adversaries B (r. C), reducing the $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to a $(q-1,t)-\mathsf{mCPA}$ adversary B (r. C) using the fact Π which is $(q-1,t,\epsilon_{\mathsf{mCPA}})-\mathsf{mCPA}$-secure.
In Table 2 we give the choice of the output bit b' of adversaries B and C, and the security results we obtain thanks to them:

Adversary	Choice of b'	Results
B	0 if event B happens 1 otherwise	$\Pr[\overline{B}_0] \leq \Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}}$
C	0 if event B does happen 1 if event B and E do not happen 0 if event B does not happen and E do happen	$\Pr[E_0 \cap \overline{B}_0] \leq \Pr[E_1 \cap \overline{B}_1] + 8\epsilon_{\mathsf{mCPA}}$

Table 2. Choice of the output bit b' by the mCPA adversaries in Prop. 6

The mCPA*-adversary* B*:* To prove that $\Pr[\overline{B}_0] \leq \Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}}$ we reduce the $(q-1,t)-\mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to a $(q-1,t)-\mathsf{mCPA}$ adversary B against Π.
To start the reduction, first adversary B chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$. When adversary A makes an encryption query $(n^i, a^i, \mathbf{m}^i)$ for any $i = 1, .., q-1$, adversary B computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$, $\tau^i = \mathsf{f}^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$ and picks a random value $r^i \leftarrow \mathcal{T}$ (if $r^i = \tau^i$ there is no problem). Then B queries his oracle $\mathsf{Enc}_k^b(\cdot,\cdot,\cdot)$ on input (iv^i, m_0^i, m_1^i) with $m_0^i :=$

$\mathbf{m}^i \| \tau^i$ and $m_1^i := \mathbf{m}^i \| r^i$) and receives c^i which he forwards to adversary A. When A makes his decryption query (n^q, a^q, c^q), the adversary B first outputs $b = 0$ if event B happens, that is (n^q, a^q) is fresh [i.e. $\exists j \in \{1, ..., q-1\} s.t. (n^q, a^q) = (n^j, a^j)$]; otherwise, he outputs 1. Clearly

$$\begin{aligned}
\Pr[b' = b] =& \Pr[B|b = 0] \Pr[b = 0] + \Pr[\overline{B}|b = 1] \Pr[b = 1] \\
\text{observe that } \Pr[b = 0] = \Pr[b = 1] =& \frac{1}{2} \text{ because } b \text{ is randomly picked} \\
=& \frac{1}{2} \left(\Pr[B_0] + \Pr[\overline{B_1}] \right) \\
=& \frac{1}{2} \left(1 - \Pr[\overline{B}_0] + \Pr[\overline{B}_1] \right)
\end{aligned}$$

Since Π is a $(q, t, \epsilon_{\mathsf{mCPA}})-\mathsf{mCPA}$ secure $\Pr[b = b'] \leq \frac{1}{2} + \epsilon_{\mathsf{mCPA}}$. Thus $\Pr[\overline{B}_0] \leq \Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}}$.

The mCPA*-adversary* C*:* Now to prove that $\Pr[E_0 \cap \overline{B}_0] \leq \Pr[E_1 \cap \overline{B}_1] \leq 6\epsilon_{\mathsf{mCPA}}$ we reduce the $(q-1, t)-\mathsf{INT\text{-}CTXT1}$ adversary A against $\overline{\boldsymbol{\Pi}}$ to a $(q-1, t)-\mathsf{mCPA}$ adversary C against Π.
To start the reduction, first adversary C chooses two random functions $\mathsf{f}^{\mathsf{IV}} : \mathcal{N} \times \mathcal{A} \longmapsto \mathcal{IV}$ and $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$. When adversary A makes an encryption query $(n^i, a^i, \mathbf{m}^i)$ for any $i = 1, .., q-1$, adversary C computes $iv^i = \mathsf{f}^{\mathsf{IV}}(n^i, a^i)$, $\mathsf{f}^i = \rho^{\mathsf{Tag}}(a^i, \mathbf{m}^i)$ and picks a random value $r^i \leftarrow \mathcal{T}$ (if $r^i = \tau^i$ there is no problem). Then C queries his oracle $\mathsf{Enc}_k^b(\cdot, \cdot, \cdot)$ on input (iv^i, m_0^i, m_1^i) with $m_0^i := \mathbf{m}^i \| \tau^i$ and $m_1^i := \mathbf{m}^i \| r^i$ and receives c^i which he forwards to adversary A. When A makes his decryption query (n^q, a^q, c^q), the adversary C first computes $iv^q = \mathsf{f}^{\mathsf{IV}}(n^q, a^q)$. If event B has not happened C outputs 0. Otherwise, since event $\overline{B}$ has happened, $iv^q = iv^j$ for a certain $i = 1, ..., q-1$ (due to event $\overline{B}$ $(n^q, a^q) = (n^j, a^j)$ for a certain $j = 1, ..., q-1$). Using the fact that Π is nonce-message-malleable, adversary C is able to answer correctly to the decryption query of A. In fact he computes $\mathbf{m}^q$ and τ^q by simply parsing $m^q = (\mathbf{m}^q \| \tau^q) \leftarrow \mathsf{Dec}(iv^q, c^q)$ [if the decryption gives $\perp$ C simply outputs 1]. Then he can compute $\tau^{q,c} = \mathsf{f}^{\mathsf{Tag}}(a^q, \mathbf{m}^q)$ and then verify if $\tau^{q,c} = \tau^q$.
The mCPA adversary C outputs $b' = 0$ if $\tau^{q,c} = \tau^q$ (that is, the ciphertext provided by the $\mathsf{INT\text{-}CTXT1}$ adversary A is valid), 1 otherwise. Thus, using also the results
$\Pr[\overline{B}_0] \leq \Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}}$ due to adversary B. First, let us suppose that $\Pr[B_0],\ \Pr[B_1] \neq$

1:

$$\Pr[b' = b] = \Pr[B_0]\Pr[b = 0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\Pr[b = 0] + \Pr[\overline{E}|\overline{B}_1]\Pr[\overline{B}_1]\Pr[b = 1]$$

observe that $\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2}$ because b is randomly picked

$$\begin{aligned}
&= \frac{1}{2}\left(\Pr[B_0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] + \Pr[\overline{E}|\overline{B}_1]\Pr[\overline{B}_1]\right) \\
&= \frac{1}{2}\left(1 - \Pr[\overline{B}_0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] + \Pr[\overline{E}|\overline{B}_1]\Pr[\overline{B}_1]\right) \\
&= \frac{1}{2}\left(1 - \Pr[\overline{B}_0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] + \left(1 - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_1]\right) \\
&= \frac{1}{2}\left(1 - \Pr[\overline{B}_0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] + \Pr[\overline{B}_1] - \Pr[E|\overline{B}_1]\Pr[\overline{B}_1]\right) \\
&= \frac{1}{2}\left(1 - \Pr[\overline{B}_0] + \Pr[\overline{B}_1] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] - \Pr[E|\overline{B}_1]\Pr[\overline{B}_1]\right) \\
&= \frac{1}{2}\left(1 - \Pr[\overline{B}_0] + \Pr[\overline{B}_1] + \right. \\
&\quad \left.\left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0] - \Pr[E|\overline{B}_1]\left(\Pr[\overline{B}_1] - \Pr[\overline{B}_0]\right)\right) = (\circ)
\end{aligned}$$

Using the fact that $|\Pr[\overline{B}_0] - \Pr[\overline{B}_1]| \leq 2\epsilon_{\mathsf{mCPA}}$, due to B, we have:

$$\begin{aligned}
&\frac{1}{2}\left(1 - 2\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0] - \Pr[\overline{E}|\overline{B}_1]2\epsilon_{\mathsf{mCPA}}\right) \leq (\circ) \\
&\quad \leq \frac{1}{2}\left(1 + 2\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0] + \Pr[\overline{E}|\overline{B}_1]2\epsilon_{\mathsf{mCPA}}\right)
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{2}\left(1 - 2\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0] - 2\epsilon_{\mathsf{mCPA}}\right) \leq (\circ) \\
&\quad \leq \frac{1}{2}\left(1 + 2\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0] + 2\epsilon_{\mathsf{mCPA}}\right)
\end{aligned}$$

Since C is a $(q,t) - \mathsf{mCPA}$ against the scheme Π which is $(q,t,\epsilon_{\mathsf{mCPA}}) - \mathsf{mCPA}$-secure we obtain:

$$\frac{1}{2}\left(1 - 4\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0]\right) \leq \frac{1}{2} + \epsilon_{\mathsf{mCPA}}$$

and

$$\frac{1}{2}\left(1 + 4\epsilon_{\mathsf{mCPA}} + \left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)\Pr[\overline{B}_0]\right) \leq \frac{1}{2} + \epsilon_{\mathsf{mCPA}}$$

thus

$$\frac{\Pr[B_0]\left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)}{2} \leq 3\epsilon_{\mathsf{mCPA}}$$

and

$$\frac{\Pr[\overline{B}_0]\left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right)}{2} \leq -\epsilon_{\mathsf{mCPA}}$$

thus

$$\Pr[\overline{B}_0]\left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right) \leq 6\epsilon_{\mathsf{mCPA}}$$

and

$$\Pr[\overline{B}_0]\left(\Pr[E|\overline{B}_0] - \Pr[E|\overline{B}_1]\right) \leq -2\epsilon_{\mathsf{mCPA}}$$

Thus:

$$\Pr[E \cap \overline{B_0}] = \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] \leq \Pr[E|\overline{B}_1]\Pr[\overline{B}_0] + 6\epsilon_{\mathsf{mCPA}}$$

$$= \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] - \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + \Pr[E|\overline{B}_1]\Pr[\overline{B}_0] + 6\epsilon_{\mathsf{mCPA}}$$

$$= \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + \Pr[E|\overline{B}_1]\left(\Pr[\overline{B}_0] - \Pr[\overline{B}_1]\right) + 6\epsilon_{\mathsf{mCPA}}$$

$$\leq \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}} + 6\epsilon_{\mathsf{mCPA}} = \Pr[E \cap \overline{B}_1] + 8\epsilon_{\mathsf{mCPA}}$$

From the other inequality we obtain

$$\Pr[E \cap \overline{B_0}] = \Pr[E|\overline{B}_0]\Pr[\overline{B}_0] \leq \Pr[E|\overline{B}_1]\Pr[\overline{B}_0] - 2\epsilon_{\mathsf{mCPA}}$$

$$= \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] - \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + \Pr[E|\overline{B}_1]\Pr[\overline{B}_0] - 2\epsilon_{\mathsf{mCPA}}$$

$$= \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + \Pr[E|\overline{B}_1]\left(\Pr[\overline{B}_0] - \Pr[\overline{B}_1]\right) - 2\epsilon_{\mathsf{mCPA}}$$

$$\leq \Pr[E|\overline{B}_1]\Pr[\overline{B}_1] + 2\epsilon_{\mathsf{mCPA}} - 2\epsilon_{\mathsf{mCPA}} = \Pr[E \cap \overline{B}_1]$$

Instead if $\Pr[B_0] = 1$, then $\Pr[\overline{B}_0] = 0$, thus, $\Pr[E_0|\overline{B_0}]$ cannot be defined. But, clearly $\Pr[E_0 \cap \overline{B}_0] = 0$. On the other end, if $\Pr[B_1] = 1$, then $\Pr[\overline{B}_1] = 0$, thus, $\Pr[\overline{E}_1|\overline{B_1}]$ cannot be defined. But, if $\Pr[B_0] \neq 1$ (thus $\Pr[\overline{B}_0] \neq 0$), we obtain

$$\Pr[b' = b] = \Pr[B_0]\Pr[b = 0] + \Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\Pr[b = 0] + \Pr[\overline{E} \cap \overline{B}_1]\Pr[b = 1]$$

thus, since by hypothesis $\Pr[\overline{B}_1] = 0$

$$= \Pr[B_0]\Pr[b = 0] + \Pr[E|\overline{B}_0]\Pr[b = 0]$$

since b is randomly picked $\Pr[b=0]=\Pr[b=1]=\frac{1}{2}$, thus

$$=\frac{1}{2}\left(\Pr[B_0]+\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\right)=(\star)$$

Since, by hypothesis, $\Pr[B_1]=1$, and since, due to the mCPA adversary B we have proved that $|\Pr[B_0]-\Pr[B_1]|\leq 2\epsilon_{\mathsf{mCPA}}$, we obtain:

$$\frac{1}{2}\left(1-2\epsilon_{\mathsf{mCPA}}+\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\right)\leq(\star)\leq\frac{1}{2}\left(1+\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\right)$$

Since C is a $(q,t)-\mathsf{mCPA}$ against the scheme Π which is $(q,t,\epsilon_{\mathsf{mCPA}})-\mathsf{mCPA}$-secure we obtain:

$$\frac{1}{2}\left(1-2\epsilon_{\mathsf{mCPA}}+\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\right)\leq\frac{1}{2}+\epsilon_{\mathsf{mCPA}}$$

and

$$\frac{1}{2}\left(1+\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\right)\leq\frac{1}{2}+\epsilon_{\mathsf{mCPA}}$$

Thus

$$\frac{\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]}{2}\leq\epsilon_{\mathsf{mCPA}}+\epsilon_{\mathsf{mCPA}}$$

and

$$\frac{\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]}{2}\leq\epsilon_{\mathsf{mCPA}}$$

Consequently:

$$\Pr[E\cap\overline{B}_0]=\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\leq 8\epsilon_{\mathsf{mCPA}}=\Pr[E\cap\overline{B}_1]+8\epsilon_{\mathsf{mCPA}}$$

and

$$\Pr[E\cap\overline{B}_0]=\Pr[E|\overline{B}_0]\Pr[\overline{B}_0]\leq 2\epsilon_{\mathsf{mCPA}}=\Pr[E\cap\overline{B}_1]+4\epsilon_{\mathsf{mCPA}}$$

Thus we have proved the bound:

$$\Pr[E\cap\overline{B_0}]\leq\Pr[E\cap\overline{B}_1]+8\epsilon_{\mathsf{mCPA}}$$

$\Pr[E_1|B_1]=\frac{1}{2}$*:* Eventually, we compute $\Pr[E_1|B_1]$. Since $\tau^{q,c}=\mathsf{f}^{\mathsf{Tag}}(a^q,\mathbf{m}^q)$ is completely random and it has never been computed before, because in Game 1 the function $\mathsf{f}^{\mathsf{Tag}}$ is never used for encryption queries, the probability it is equal to τ^q is equal to $|\mathcal{T}|^{-1}$. Thus $\Pr[E_1\cap\overline{B}_1]\leq|\mathcal{T}|^{-1}$ (the inequality is due to the the fact that $\mathsf{Dec}(iv^q,c^q)\neq\perp$ it is not granted). So we have proved the proposition, since $\Pr[E_0\cap\overline{B}_0]\leq\Pr[E_1\cap\overline{B}_1]$ thanks to adversary C. Thus:

$$\Pr[E_0]=\Pr[E_0\cap B_0]+\Pr[E_0\cap\overline{B}_0]\leq(q-1)(\epsilon_{\mathsf{ivE}}+|\mathcal{T}|^{-1})+|\mathcal{T}|^{-1}+8\epsilon_{\mathsf{mCPA}}=$$

$$(q-1)\epsilon_{\mathsf{ivE}}+q|\mathcal{T}|^{-1}+8\epsilon_{\mathsf{mCPA}}$$

Message-malleability for N4

Proposition 13. *Let the* nE *scheme Π be $(q, t, \epsilon_{\mathsf{nE}})$-*nE*-secure, $(q-1, t, \epsilon_{\mathsf{mCPA}})$-*mCPA*-secure and "message-malleable", let $\mathsf{f}^{\mathsf{Tag}} : \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{T}$ be a random function. Then, the scheme $\overline{\boldsymbol{\Pi}}$ obtained composing these components according to mode N4, is $(q, t, (q-1)\epsilon_{\mathsf{nE}} + q|\mathcal{T}|^{-1} + 8\epsilon_{\mathsf{mCPA}})$ − INT-CTXT1-secure.*

Proof. The proof is similar to the proof of Prop. 14 with some easy adjustments.

F.5 Proof of insecure variants of mode A10, A11, and A12

Stateful

Proof of ivE*-security* Now we have to prove that Π is ivE secure.

Proposition 14. *Let* $\mathsf{E} : \mathcal{K} \times \mathcal{TW} \times \{0,1\}^N \longmapsto \{0,1\}^N$*, where* $\mathcal{TW} = \{0, 1, ..., L\} \times \{0, 1\}$*, be a TPRP* $((L+2)q, t, \epsilon_{TPRF}) - TPRF$ *secure. Then Π is* $(q, t, \epsilon_{TPRP} + 2^{-N})$ *if every message has at most L blocks.*

The proof is similar to the proof of Prop. 10.

Proof. Let A be a $(q, t) -$ ivE adversary who asks messages which have at most L message blocks.
We remind that, due to our hypothesis, the ivE adversary A is able to set the state of Enc at the start of the Game. He sets the state to ctr^* as he wishes.
By definition of ivE-security (Def. 18), we have to bound

$$\mathsf{Adv}^{\mathsf{ivE}}_{\Pi}(\mathsf{A}) := \left| \Pr\left[\mathsf{A}^{\mathsf{Enc}^{\$}_k(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{A}^{\$(\cdot)} \Rightarrow 1\right] \right|$$

for every $(q, t) -$ ivE-adversary.
We will do it using a sequence of games.
First we observe that the length $|\mathsf{Enc}_k(n, m)|$ is equal to $|m| + 2N$ $\forall (k, iv, m) \in \mathcal{K} \times \mathcal{IV} \times \mathcal{M}$, so the length of the ciphertext does not give any information about its inputs apart from the length $|m|$.

Game 0. The first game, Game 0, is the game where the ivE adversary A is facing Π. At the end of the game, the ivE adversary outputs a bit b.
Let E_0 be the event that the bit output at the end of Game 0 by the ivE adversary A is 1.

Game 1. First we replace the TPRP E with a tweakable random function f with the same signature of the TPRP E. We call the scheme with this replacement $\overline{\Pi}$. Let E_1 be the event that the adversary A outputs 1 when he is facing $\overline{\Pi}$.
We now bound $|\Pr[E_0] - \Pr[E_1]|$ with ϵ_{TPRF}.

The TPRF-adversary B. To do this we build a $((L+1)q, t)-$ TPRF-adversary B against the $((L+1)q, t, \epsilon_{\text{TPRF}})-$ TPRF E.
This TPRF adversary B faces an oracle which is either implemented with the TPRF E or a random function f. At the start the adversary B picks a random value v^* and set the state $ctr = ctr^*$ to the value the nE adversary A wants. When A makes an encryption query (m^i) for any $i = 1, ..., q$, B first parses the message in l_i blocks with $|m_1^i| = ... = |m_{l_i-2}^i| = |m_{l_i}^i| = N$, then he picks a random $iv^i \leftarrow \mathcal{IV}$ and the actual state ctr. Then to compute c_{-1}^i he calls his oracle on input $((0,1), ctr)$ and he set c_{-1}^i to this value. Next, if $ctr = 1$, the adversary B sets $c_0^i = v^*$, otherwise he calls his oracle on input $((0,0), iv^i)$ obtaining a value which adversary B sets c_0^i to.
Next for $j = 1, ..., l_i - 2$, the adversary B calls his oracle on input $((j,0), iv^i)$, obtaining the values x_j^i which is XORed to the message block m_j^i obtaining c_j^i.
For the block $l_i - 1$, the adversary B calls his oracle on input $((l_i - 1, 0), iv^i)$, obtaining $x_{l_i-1}^i$. Then he takes the first $|m_{l-1}|$-bits of $x_{l_i-1}^i$ and he XORes them to m_{l_i-1} obtaining c_{l_i-1}.
For the last message block l_i, if the state ctr is either 1 or 2 and $m_l^i = v^*$ the TPRF adversary B calls his oracle on input $((l,1),0)$ obtaining x_l^i which he XORes to m_l^i obtaining c_l^i. Otherwise, the adversary B calls his oracle on input $((l,0), iv^i))$ obtaining x_l^i which he XORes again to m_l^i obtaining c_l^i. After that the adversary B increases the state ctr of 1. Then, adversary B computes $c^i = (c_{-1}^i, c_0^i, ..., c_l^i)$, updates the state (doing $ctr++$), and he forwards the iv iv^i and the ciphertext c^i to the ivE adversary A.
When the adversary A outputs his output bit b, B outputs the same bit $b' = b$.

Transition between Game 0 and Game 1. We observe that if the oracle facing the TPRF adversary B, is implemented with the pseudorandom function $\mathsf{E}(\cdot)$, the ivE adversary A is playing Game 0 because the oracle $\mathsf{Enc}_k(\cdot,\cdot)$ is simulated correctly. Otherwise, he is playing Game 1.
Thus $\Pr[E_0] = \Pr[\mathsf{B}^{\mathsf{E}} \Rightarrow 1]$ and $\Pr[E_1] = \Pr[\mathsf{B}^{\mathsf{f}} \Rightarrow 1]$. The adversary B makes at most $L+2$ queries to his oracle per encryption query. Since the ivE adversary A asks at most q encryption query, the TPRF adversary B makes at most $(L+2)q$ queries to his oracle. Since E is
$((L+12)q, t, \epsilon_{\text{TPRF}})$-secure-TPRF and B is a $((L+2)q, t)-$TPRF adversary, we can bound $|\Pr[\mathsf{B}^{\mathsf{E}} \Rightarrow 1] - \Pr[\mathsf{B}^{\mathsf{f}} \Rightarrow 1] \leq \epsilon_{\text{TPRF}}$. Thus $|\Pr[E_0] - \Pr[E_1]| \leq \epsilon_{\text{TPRF}}|$.
So, $\Pr[E_0] \leq \Pr[E_1] + \epsilon_{\text{TPRF}}$.

Event C. We define the event C as the event that during Game 1 the ivE adversary is able to force the encryption algorithm Enc_k to enter twice in the **if** clause boxed in Figure 5.
We assert that $\Pr[C] \leq 2^{-N}$.
To prove this we start by observing that, in order to enter twice in that **if**, the ivE adversary must have asked the first two queries on input (m^1, m^2) with $m_{l^1-1}^1 = v^*$ and $m_{l^2-1}^2 = v^*$. There are no other possibilities since when the state $ctr > 2$ it is not possible to enter in the **if** clause box. Moreover it should be noted that there cannot be two encryptions with the same state ctr (as long

the ciphertext is not $\perp$. This latter case clearly does not create any security problem).
When the ivE adversary A queries his oracle on input (m^1) he has no idea of what is the value v^* since this value is picked uniformly at random and it has never been used. So the probability that the second to last block m_{l_1-1} of the message m asked to be encrypted when the state is $ctr = 1$, is equal to v^* is 2^{-N}. Thus $\Pr[C] \leq 2^{-N}$.

Game 2. We define Game 2 as Game 1 apart from the fact that if event C happens the ivE adversary A outputs immediately 1. Let E_2 be the event that the ivE adversary A outputs 1.
Clearly $|\Pr[E_2] - \Pr[E_1]| \leq \Pr[C] \leq 2^{-N}$.

Game 3. Game 3 is defined as Game 2 apart from the fact that we replace all c^i's with random strings of the same length. Let E_3 be the event that the ivE adversary outputs 1 at the end of Game 3.

Transition from Game 2 and Game 3. We assert that $\Pr[E_2] = \Pr[E_3]$.
If event C happens the ivE adversary behaves in the same way in both games. Otherwise we can observe that $\mathsf{f}(\cdot,\cdot)$ is never called during the game on the same inputs. Since $\mathsf{f}(\cdot,\cdot)$ is by hypothesis a random function the XOR of its output with a message block is a random string. Moreover for the first ciphertext block c^i_{-1} for every i we can observe that it is $\mathsf{E}^{0,1}_k(ctr)$, whose inputs are always different. For the second block for the message encrypted when the state ctr is equal to 1, it is v^* which is a random value by hypothesis, otherwise it is $\mathsf{f}((0,0), iv^i)$ which is a random value since f has never been computed on this input and $\mathsf{f}(\cdot,\cdot)$ is a random function. Thus all the ciphertext obtained in Game 2 are random strings, except if event C happens. Consequently $\Pr[E_3] = \Pr[E_2]$.

Thus for every $(q,t) - \mathsf{ivE}$ adversary A we can bound

$$\mathsf{Adv}^{\mathsf{ivE}}_{\Pi}(\mathsf{A}) = |\Pr[E_0] - \Pr[E_3]| \leq \epsilon_{\mathrm{TPRF}} + |\Pr[E_1] - \Pr[E_2]| \leq \epsilon_{\mathrm{TPRF}} + 2^{-N},$$

thus concluding our proof.

The tidiness of the stateful ivE scheme Π follows from a close inspection of the algorithm.

G Message-malleable schemes

In this section we want to show three examples of message malleable schemes, two fixed length and one with various length. For simplicity, we give only the encryption algorithms, since the decryption algorithm is straightforward.

G.1 Fixed length scheme

We give the examples of two common schemes: CTR and OFB. Although they are ivE-secure for any message length they are message-malleable only if they are employed to encrypt fixed length messages. Moreover, as we show, they provide examples of schemes which are ivE-secure but not nE secure (for any message length). They are all based on a PRF $\mathsf{E} : \mathcal{K} \times \mathcal{IV} \longmapsto \{0,1\}^N$. The key of the schemes is the key k of the PRF.

CTR (counter) The description of the ivE encryption scheme CTR can be found in Fig. 2.

The ivE-security of the scheme is well-known (see for example [15]).

The CTR scheme is not nE-secure. In fact let (iv, c_1, c_2, c_3) be the encryption of the message (m_1, m_2, m_3) for a random iv, then if we want to encrypt the message $m' = (m_2, m_3)$ with $iv' := iv + 1$ we obtain $c' = (c_2, c_3)$.

The CTR scheme is clearly "message-malleable". In fact, given two messages m and m' where $|m| = |m'|$, let $c \leftarrow \mathsf{Enc}_k(iv, m)$ then $c' \leftarrow \mathsf{Enc}_k(iv, m')$ with $c \oplus m \oplus m'$ where
$c \oplus m \oplus m' := (c_1 \oplus m_1 \oplus m'_1, ..., c_l \oplus m_l \oplus m'_l)$

The ivE-scheme CTR

$\mathsf{Enc}_k(iv, m)$:
- Parse $m = (m_1, ..., m_l)$ with $|m_1| = ... = |m_{l-1}| = N$ and $|m_l| \leq N$.
- $ctr = iv$
- **For** $i = 1, ..., l-1$
  - $z_i = \mathsf{E}_k(ctr)$
  - $c_i = z_i \oplus m_i$
  - $ctr++$
- $len = |m_l|$
- $z_l = \mathsf{E}_k(ctr)$
- $c_l = \pi_{len}(z_l) \oplus m_l$
- **Return** $c = (c_1, ..., c_l)$

Fig. 2. The ivE-scheme CTR (counter), which is iv-secure, not nE secure and "message malleable" for fixed length message.

OFB (Output Feedback) The description of the ivE encryption scheme OFB can be found in Fig. 3.

The ivE-security of the scheme is well-known (see for example [15]).

The OFB scheme is not nE-secure. In fact let (iv, c_1, c_2, c_3) be the encryption of the message (m_1, m_2, m_3) for a random iv, then if we want to encrypt a message $m' = (m_2, m_3)$ with $iv' := z_1 := c_1 \oplus m_1$ we obtain $c' = (c_2, c_3)$.

The OFB scheme is clearly "message-malleable". In fact, given two messages m and m' where $|m| = |m'|$, let $c \leftarrow \mathsf{Enc}_k(iv, m)$ then $c' \leftarrow \mathsf{Enc}_k(iv, m')$ with $c \oplus m \oplus m'$ where
$c \oplus m \oplus m' := (c_1 \oplus m_1 \oplus m'_1, ..., c_l \oplus m_l \oplus m'_l)$

The ivE-scheme OFB
$\mathsf{Enc}_k(iv, m)$:
– Parse $m = (m_1, ..., m_l)$ with $\|m_1\| = ... = \|m_{l-1}\| = N$ and $\|m_l\| \leq N$.
– $z_0 = iv$
– **For** $i = 1, ..., l-1$
• $z_i = \mathsf{E}_k(z_{i-1})$
• $c_i = z_i \oplus m_i$
– $len = \|m_l\|$
– $z_l = \mathsf{E}_k(z_{l-1})$
– $c_l = \pi_{len}(z_l) \oplus m_l$
– **Return** $c = (c_1, ..., c_l)$

Fig. 3. The ivE-scheme OFB (Output feedback), which is iv-secure, not nE secure and "message malleable" for fixed length message.

G.2 Various length scheme

It is more difficult to find an example of "message-malleable" encryption scheme in the literature. We give it using a variant of the ivE scheme which Pereira et al. [29] presented at CCS 2015 in the context of leakage-resilient cryptography. Here it is not the place to discuss about leakage, we only want to discuss one feature of this scheme: the use of the rekeying, that is, there is a master key used once in the leakfree [that is, a heavy protected against side-channel attacks primitive, which is very slow](PRF) component E^* per encryption which generates many ephemeral keys which are used only twice in the PRF E (less protected, but much faster), in order to achieve leakage resistance (and it used to obtain AE by Berti et al. [10], [9].
The key k is the key of the leak free PRF E^*. Two public constants p_A and p_B are used. The difference with regard to [29] is the fact that we give the last ephemeral key k_{l+1} and the bits of z_l that we do not use to encrypt m_l. The details are in Fig. 4.

The ivE (in reality the nE) security is proved by their authors. The change we did do not affect the security.

The "message-malleability" comes from the fact that given an ephemeral key we are able to compute all the following ephemeral keys.

But by now we are only able to have forward malleability for messages m' that are longer or as long as the given message m (in reality also for all messages m' s.t. $\lfloor \frac{|m'|+1}{N} \rfloor \geq \lfloor \frac{|m|+1}{N} \rfloor$), since we are not able to recompute to the previous ephemeral keys. We can solve it allowing the messages to be padded, that is message may be encrypted after having padded a 1 and as many 0 as we wants. In the decryption the padding is removed. In this way we can make a message m' to be longer using many 0s in the padding.

The ivE-scheme PVS-modified
$\mathsf{Enc}_k(iv, m)$: – Parse $m = (m_1, ..., m_l)$ with $\|m_1\| = ... = \|m_{l-1}\| = N$ and $\|m_l\| \leq N$. – $k_1 = \mathsf{E}^*_k(iv)$ – **for** $i = 1, ..., l-1$ • $z_i = \mathsf{E}_{k_i}(p_A)$ • $c_i = z_i \oplus m_i$ • $k_{i+1} = \mathsf{E}_{k_i}(p_B)$ – $len = \|m_l\|$ – $z_l = \mathsf{E}_{k_l}(p_A)$ – $c_l = \pi_{len}(z_l) \oplus m_l$ – $c'_l = z_l \oplus \pi_{len} \| 0*$ – $k_{l+1} = \mathsf{E}_{k_l}(p_B)$ – **return** $c = (c_1, ..., c_l, c'_l, k_{l+1})$

Fig. 4. The ivE-scheme PVS-modified, which is *iv*-secure, nE secure and "message malleable" for various length message.

H Example of an mrE scheme not mrAE

Let $\mathcal{PERP}^{\mathcal{K}\times\mathcal{N}\times\mathcal{A}}(\mathcal{M}) := \{\mathsf{f} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \longmapsto \mathcal{M}$ s.t. $\forall k \in \mathcal{K}, n \in \mathcal{N}, a \in \mathcal{A}$ $\mathsf{f}_k(n, a)(\cdot)$ is a permutation$\}$. Let $f \leftarrow \mathcal{PERP}^{\mathcal{K}\times\mathcal{N}\times\mathcal{A}}(\mathcal{M})$.
We define the nAE encryption scheme $\boldsymbol{\Pi} = (\boldsymbol{\mathcal{K}}, \mathsf{AEnc}, \mathsf{ADec})$ as follow:

– $\boldsymbol{\mathcal{K}} = \mathcal{K}$
– $\mathsf{AEnc}_k(n, a, m) := \mathsf{F}_k(n, a, m)$
– $\mathsf{ADec}_k(n, a, c) := \mathsf{F}^{-1}_k(n, a, c)$

This scheme is clearly $\mathsf{nAE} - \mathsf{E}$-secure, since for every fresh triple (n, a, m) the encryption $c = \mathsf{f}_k(n, a, m)$ is fresh. On the other hand, since $\mathsf{f}^{n,a}_k(\cdot)$ is a permutation, then $\forall (n, a, c) \in \mathcal{N} \times \mathcal{A} \times \mathcal{M}$, there exists $m = \mathsf{ADec}_k(n, a, c)$ with $m \neq \perp$.

I Algorithms

Fig. 5. The nE-scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ used in Sec. 4 - Full description. Its nE security is proved in Prop. 10

The ivE-scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$

Gen
- $k \leftarrow \mathcal{K}_E$
- $\mathsf{f}^{\mathsf{Enc}} \leftarrow \mathcal{FUNC}\left(\mathcal{IV}, \{0,1\}^N\right)$

$\mathsf{Enc}'_{(k,\mathsf{f}^{\mathsf{Enc}})}(iv, m)$
- **if** $|m| \leq N$
  - $m_1 = m$
- **else**
  - Parse $m = (m_0, m_1)$ with $|m_0| = N$
- **if** $\exists m_0$
  - $c_0 = \mathsf{f}^{\mathsf{Enc}}(iv) \oplus m_0$
- $c_1 = \mathsf{Enc}_k(iv, m_1)$
- **if** $\exists c_0$
  - **return** $c = (c_0, c_1)$
- **else**
  - **return** $c = c_1$

$\mathsf{Dec}'_{(k,\mathsf{f}^{\mathsf{Enc}})}(iv, c)$
- **if** $|c| \leq N$
  - $c_1 = c$
- **else**
  - Parse $c = (c_0, c_1)$ with $|c_0| = N$
- **if** $\exists c_0$
  - $m_0 = \mathsf{f}^{\mathsf{Enc}}(iv) \oplus c_0$
- $(m_1) = \mathsf{Dec}_k(iv, c_1)$
- **return** $m = (m_0, m_1)$

Fig. 6. The ivE-scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$, based on the ivE scheme Π. used in the proof of Prop. 2 and 3 - Full description. Its ivE-security is proved in Lemma 4.

The stateful ivE-scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

Gen
- $k \leftarrow \mathcal{K}$
- $v^* \leftarrow \{0,1\}^I V$
- $ctr = 1$

$\mathsf{Enc}_{k,v^*}(iv, m)$
- Parse $m = (m_1, ..., m_l)$ with $|m_1| = ... = |m_{l-2}| = |m_l| = N$ and $|m_{l-1}| \leq N$
- **if** $l > L$
  - **return** $\perp$
- $c_{-1} = \mathsf{E}^{0,1}(ctr)$ — **Block**$_{-1}$
- **if** $ctr = 1$
  - $c_0 = v^*$
- **else**
  - $c_0 = \mathsf{E}_k^{0,0}(iv)$

  } **Block**$_0$

- **for** $i = 1, ..., l-2$
  - $c_i = \mathsf{E}_k^{i,0}(iv) \oplus m_i$
- $len = |m_{l-1}|$
- $c_{l-1} = \pi_{len}[\mathsf{E}_k^{l-1,0}(iv)] \oplus m_{l-1}$

  } **Block**$_1$**,...,** **Block**$_{l-1}$
- **if** $(ctr = 1 \vee ctr = 2) \wedge m_{l-1} = v^*$
  - $c_l = \mathsf{E}_k^{l,1}(0) \oplus m_l$
- **else**
  - $c_l = \mathsf{E}_k^{l,0}(iv) \oplus m_l$

  } **Block**$_l$

- $ctr++$
- **return** c $[= (c_0, ..., c_l)]$

$\mathsf{Dec}_{k,v^*}(iv, c)$
- Parse $c = (c_{-1}, ..., c_l)$ with $|c_{-1}| = ... = |c_{l-2}| = |c_l| = N$ and $|c_{l-1}| \leq N$
- **if** $l > L$
  - **Return** $\perp$
- $ctr = \left(\mathsf{E}_k^{0,1}\right)^{-1}(c_{-1})$
- **if** $ctr = 1$
  - **if** $c_0 \neq v^*$
    - **return** $\perp$
- **else**
  - **if** $c_0 \neq \mathsf{E}_k^{0,0}(iv)$
    - **return** $\perp$
- **for** $i = 1, ..., l-2$
  - $m_i = \mathsf{E}_k^{i,0}(iv) \oplus c_i$
- $len = |c_{l-1}|$
- $m_{l-1} = \pi_{len}[\mathsf{E}_k^{l-1,0}(iv)] \oplus c_{l-1}$
- **if** $(ctr = 1 \vee ctr = 2) \wedge m_{l-1} = v^*$
  - $m_l = \mathsf{E}_k^{l,1}(0) \oplus c_l$
- **else**
  - $m_l = \mathsf{E}_k^{l,0}(iv) \oplus c_l$
- **return** m $[= (m_1, ..., m_l)]$

Fig. 7. The stateful ivE-scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ used in Sec. 7.2 - Full description.