Combiners for AEAD∗

Bertram Poettering1 and Paul Rösler2

1 IBM Research – Zurich, Rüschlikon, Switzerland

2 Chair for Network and Data Security, Ruhr University Bochum, Bochum, Germany

Abstract. The Authenticated Encryption with Associated Data (AEAD) primitive, which integrates confidentiality and integrity services under a single roof, found wide-spread adoption in industry and became indispensable in practical protocol design. Recognizing this, academic research put forward a large number of candidate constructions, many of which come with provable security guarantees. Nevertheless, the recent past has shaken up with the discovery of vulnerabilities, some of them fatal, in well-regarded schemes, stemming from weak underlying primitives, flawed security arguments, implementation-level vulnerabilities, and so on. Simply reacting to such findings by replacing broken candidates by better(?) ones is in many cases unduly, costly, and sometimes just impossible. On the other hand, as attack techniques and opportunities change over time, it seems venturous to propose any specific scheme if the intended lifetime of its application is, say, twenty years.

In this work we study a workable approach towards increasing the resilience against unforeseen breaks of AEAD primitives. Precisely, we consider the ability to combine two AEAD schemes into one such that the resulting AEAD scheme is secure as long as at least one of its components is (or: as long as at most one component is broken). We propose a series of such combiners, some of which work with fully generic AEAD components while others assume specific internal structures of the latter (like an encrypt-then-MAC design). We complement our results by proving the optimality of our constructions by showing the impossibility of combiners that get along with less invocations of the component algorithms.

Keywords: Secure Combiners · Provable Security · AEAD · Encrypt-then-MAC · Ciphertext Translation · Impossibility Result

1 Introduction

AEAD. Authenticated Encryption with Associated Data (AEAD, [Rog02, McG08]) is a cryptographic primitive that gained more and more importance in the recent years. It consists of two symmetrically keyed algorithms: an encryption algorithm that is invoked by a sender and transforms a message into a ciphertext, and a decryption algorithm that is invoked by a receiver and transforms the ciphertext back to the message. The two algorithms further depend on an additional input referred to as associated data into which the sender and receiver can encode the context in which they perform their operations; equality of these contexts (i.e., associated data strings) is assumed for successful message recovery. The security typically expected of an AEAD scheme covers both confidentiality and authenticity.

COMBINERS. The idea of cryptographic combiners is to introduce redundancy in security by combining multiple constructions of the same primitive into one, to prepare for the case

∗The full version of this article [PR20] is available as article 2020/232 in the IACR eprint archive.
that one or more, but not all, of these building blocks turn out to be insecure. As long as at least one component stays secure, the combined primitive does as well.

Combiners have been studied for multiple cryptographic primitives, including one-way functions, hash functions, message authentication codes, signatures, symmetric encryption schemes, key encapsulation mechanisms, indistinguishability obfuscation [MH81, Her05, HKN+05, DK05, FL07, FL08, FLP08, FHNS16, GHP18]. Some of these works are more on the theoretical side by considering puristic feasibility results, while others aim at proposing solutions to a practical problem. For instance, while the KEM combiners of [GHP18] employ hash functions and PRFs as additional building blocks, which is in line with the practical use cases envisioned by the authors, Dodis and Katz [DK05] consider a more pure form of PKE combiner that does not add more hardness assumptions but gets along with adding only information-theoretic ingredients. While the focus of our work is on practical AEAD combiners, we achieve our goals without adding more primitives or assumptions.

1.1 Motivation for AEAD Combiners

Research in symmetric cryptography succeeded with proposing a plethora of AEAD schemes. While many of these come with formal security arguments, there remain a number of reasons why combining two AEAD schemes into one to strengthen their security might still be attractive. The arguments span over various domains and are connected to flawed security arguments, implementation issues, management practices, or simply politics.

Flawed Security Arguments. Even if a cryptographic scheme comes with a “security proof”, the unfortunate truth is that the corresponding arguments might be flawed and the scheme weak. This also holds for AEAD designs, where it seems fair to say that the high level of integration that the most efficient blockcipher-based schemes feature also makes the schemes challenging to fully comprehend and surround on a formal level. A prime example of where the security argument of an intricate AEAD scheme turned out to be fatally flawed, and this went unnoticed for a rather long period of time, is given by the recent results on OCB2 that completely broke the scheme [IIMP19]. There are several similar cases to report on, including the flawed EAX’ scheme [MLMI14], a flawed argument in the security proof of GCM [IOM12], and flaws in some of the CAESAR submissions [Nan14, BS16, SMAP16].

Untested Assumptions. Schemes might rely on relatively new and untested building blocks. For instance, the winners of the CAESAR competition, besides OCB3 which is based on plain AES, are Ascon, ACORN, AEGIS, Deoxys, and COLM, where the former two use ad-hoc constructions and the latter three build on the AES round function but in a different context than in plain AES. While no insecurities of any of these modes have been identified as of today, one could argue that the assumptions are too fresh to be fully relied upon.

Implementation-Based Attacks. Even if a construction comes with a correct formal security argument, securely implementing it might be tricky. For instance, if components of the primitive are conveniently implemented via look-up tables, cache timing side channels are hard to evade. See [Ber05] for classic practical attacks against AES implementations, and the suggestion in [KS09] for side-channel attacks against table-based implementations of GCM’s field arithmetic.

Standards. The use of a particular AEAD scheme might be required to achieve standard conformance, or to obtain a positive certification by government bodies. This might be the case even if the AEAD scheme is known to be weak, or at least its security is questionable. Examples may include cases in the payment industry where the use of 3DES still seems to be fashionable even though its blocksize is too small to achieve security in many applications [BL16], or where the use of ISO standardized AEAD schemes like the
broken OCB2 are required, etc. An AEAD combiner allows using weak yet mandated schemes without risking security.

**Political Issues.** The Snowden revelations of 2013 suggested that state agencies might engage in subverting cryptographic primitives. While the best and most clear example remains to be the Dual-EC-DRBG incident\(^1\), some actors actively avoid other NSA approved cryptosystems as well. For instance, instant messenger vendor SilentCircle switched from using the AES blockcipher to TwoFish\(^2\), and the Simon and Speck blockciphers were not adopted by the ISO for standardization\(^3\).\(^4\) Not all of these decisions are purely justifiable on an academic level, but seem partially also political in nature. The use of an AEAD combiner might contribute to satisfying the politically induced requirements of some people.

To conclude: For many popular encryption schemes, more or less compelling arguments can be found for not using them. It seems to be a matter of personal preference which of these schemes to trust or distrust. Using an AEAD combiner might help finding a common denominator among communication participants. In any case, as we argue next, it is essential that such combiners fulfill two important properties: simplicity and efficiency.

We advocate that AEAD combiners be simple. A complex combiner might lead to incomprehensible security analyses, and might be hard to implement correctly, and thus potentially introduce new security risks. In such a case it is conceivable that the combination of two secure AEAD schemes is actually insecure, with the combiner being responsible for the problems.

We further advocate that AEAD combiners be efficient. Indeed, AEAD schemes are used in almost all modern protocols, protecting billions of communications every day, and top performance is therefore a top priority. Of course a combined AEAD scheme is less efficient than its components; but the overhead should be reduced to the absolute minimum, ideally none.

All our combiners have a very clear design, come with rigorous, yet easy to verify proofs, do not require any exotic hardness assumptions of their components, and are highly efficient (in some cases we even claim optimality).

### 1.2 Approach and Results

In the course of this article we expose a number of AEAD combiners. While those of Section 3 are generic in the sense that they do not rely on any property of the component AEAD schemes that goes beyond their blackbox properties (i.e., their syntax, correctness, and security), those of Section 4 are non-generic and require a specific internal structure of at least one of their components (e.g., that it is induced by an encrypt-then-MAC design).

All our combiners take two AEAD schemes and achieve security if (at least) one of them is secure. The resulting scheme can, of course, be combined in the same way with a third AEAD scheme, a fourth, and so on.\(^5\) Conveniently, our non-generic combiners preserve the non-blackbox properties they require of their components. That is, also these combiners are smoothly amenable to a scaling process to more input schemes.

One efficiency metric for combiners is the number of internal invocations of their AEAD components. The intuitive minimum is likely four, suggested by each combined encryption operation requiring one internal invocation of each component’s encryption algorithm, and each combined decryption operation requiring one internal invocation of each component’s decryption algorithm. In Section 5 we present a result that shows that

\(^{1}\)https://en.wikipedia.org/wiki/Dual_EC_DRBG
\(^{2}\)https://silentcircle.wordpress.com/2013/09/30/mncs/
\(^{3}\)https://mobile.reuters.com/article/amp/idUSKCN1BW0GV
\(^{4}\)That also symmetric schemes can be subverted is illustrated in works like [BPR14, AP19a, AP19b].
\(^{5}\)Note that the overall combiner’s performance may depend on the order of combinations.
for generic (blackbox) AEAD schemes this minimum cannot be reached, but that at least five invocations are necessary. Five internal invocations are also sufficient: Our generic combiners are optimal in this sense, requiring two internal encryptions for a combined encryption, and two internal decryptions plus one internal encryption for a combined decryption. Also our non-generic combiners get along with five internal invocations. They outperform our generic combiners nevertheless, but according to different metrics. For instance, observing that the inner building blocks of AEAD schemes have often dedicated functions, like providing ‘passive confidentiality’ and ‘strong authentication’ in an encrypt-then-MAC design, we can employ the right building blocks for the right tasks (e.g., save on encryption if confidentiality is not a matter), ultimately making the combiner faster. Further, our non-generic combiners achieve the shortest ciphertext expansions (which is constant for all our combiners anyway).

In Table 1 we compare our various combiners with respect to their performance and the assumptions posed on the underlying schemes. Observe that no combiner outperforms all others in all categories. Thus, which combiner to pick depends on the specific use case.

Table 1: AEAD combiners compared with respect to their underlying component schemes and their overall performance. Column ‘Structure’ describes the required construction principle of underlying scheme $\text{AE}_i$ (blackbox, encrypt-then-MAC, ciphertext translated), ‘Required Security’ lists the underlying schemes’ security guarantees (such that either of the two cells in a row must be met for a secure combination), ‘Processed Data’ adds up necessary processing of data (‘$A$’ is a unit for the length of processed associated-data strings, and ‘$M$’ is a unit for the length of encrypted messages) per combined encryption and decryption, and ‘Ctxt. Length’ adds up the combined ciphertexts’ length (depending on message length and tag length; we use symbol $\tau$ as a placeholder for the common tag length of all AEAD schemes).

<table>
<thead>
<tr>
<th>Structure</th>
<th>Required Security</th>
<th>Processed Data</th>
<th>Ctxt. Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\text{AE}_0$</td>
<td>$\text{AE}_1$</td>
<td>$\text{AE}_3$</td>
</tr>
<tr>
<td>Blackbox 1</td>
<td>BB BB</td>
<td>BB BB</td>
<td>INT, IND</td>
</tr>
<tr>
<td>Enc-then-MAC 1</td>
<td>EtM BB</td>
<td>BB BB</td>
<td>SUF, pIND</td>
</tr>
<tr>
<td>Enc-then-MAC 2</td>
<td>EtM EtM</td>
<td>BB BB</td>
<td>SUF, pIND</td>
</tr>
<tr>
<td>Ciphertext transl.</td>
<td>BB CT</td>
<td>BB BB</td>
<td>INT, IND</td>
</tr>
<tr>
<td>Blackbox 2</td>
<td>BB BB</td>
<td>BB BB</td>
<td>INT, IND</td>
</tr>
<tr>
<td>Blackbox 3</td>
<td>BB BB</td>
<td>BB BB</td>
<td>IND$^*$</td>
</tr>
</tbody>
</table>
| Impossible | BB BB | BB BB | INT, IND | INT, IND | $\Sigma \leq 4A + 4M$ |$

The intuitive minimum for the ‘Processed Data’ column is $2A + 2M$ $2A + 2M$ (as each component should process each associated data and each message at least once). Our impossibility result from Section 5 shows that this minimum is not attainable. However the table clarifies that the combiners we propose are quite close to it. Note that the shortest ciphertext length to be expected is $M + \tau$ (the message itself, plus a tag), and that one of the combiners meets this efficiency goal. (And again, the other combiners get quite close.)

1.3 Related Work

The literature on combiners is as broad as the literature on cryptography in general since, theoretically, combiners can be studied for any cryptographic primitive. We concentrate

\footnote{This result can be evaded by requiring additional (non-blackbox) properties of the component schemes. For instance, our discussion at the end of Section 3 appreciates that many practical schemes feature a specific property, tidiness, that allows for combiners that require just four invocations.}
here on work that focuses on combining symmetric encryption or message authentication codes (since both primitives are close to AEAD).

The initial motivation for combining schemes was not to rely on either of the underlying schemes’ security but to increase the (assumed) security of one specific scheme by applying it multiple times. Merkle and Hellman [MH81] analyze the security of the Data Encryption Standard (DES) when being iteratively applied on some input, and specifically compare two versus three iterations of DES.

Today’s motivation for combining schemes is to maintain security if at least one of them is secure. In this setting, Herzberg [Her05] considers different encryption and MAC combiners. He shows for randomized schemes that neither nested encryption nor certain parallel variants of encryption (where ciphertexts of the underlying schemes are encrypted iteratively or in parallel) can achieve strong confidentiality (IND-CCA security) if only one underlying scheme reaches this property. In contrast, he shows that certain nested and parallel combiners of MACs and signatures inherit unforgeability (EUF-CMA) guarantees of an underlying scheme. We note that [Her05] does not consider strong unforgeability (SUF), which is necessary for AEAD.

Zhang et al. [ZHSI04], Dodis and Katz [DK05], as well as Giacon et al. [GHP18] consider combiners for public key encryption and key encapsulation mechanisms. Their results include combiners that achieve IND-CCA security from either of the underlying schemes. Harnik et al. [HKN+05] propose combiners for one-way functions, oblivious transfer, public key encryption, as well as key exchange. In a line of work Fischlin and Lehmann [FL07, FL08], also together with Pietrzak [FLP08], analyze and propose combiners for hash functions. Finally, Fischlin et al. [FHNS16] consider combiners for obfuscation.

2 Preliminaries

We introduce general notations and the syntax and security of AEAD and MAC schemes.

**Notation.** We denote deterministic assignments with ‘←’, probabilistic assignments with ‘$\leftarrow$’, definitional assignments with ‘:=’. If variables $A, B$ represent sets we write ‘$A \leftarrow A \cup B$’ shorthand for ‘$A \leftarrow A \cup B$’. We denote with $\oplus$ the bit-wise XORing operation of two bit-strings; if the strings have different lengths, the shorter one is padded with 0 bits at the end before the operation is performed.

With ‘$a \parallel b \parallel \ldots$’ we denote the classic concatenation of strings $a, b, \ldots$ (into a single string), whereas with ‘$a \oplus b \oplus \ldots$’ we denote an injective encoding of $a, b, \ldots$ into a string such that $a, b, \ldots$ can be unambiguously recovered from the result.

We label algorithm specifications with ‘Proc’, security games with ‘Game’, and oracles that can be queried in games with ‘Oracle’. Security games are terminated via certain instructions: ‘Reward $x$’ means that the game terminates with return value 1 if condition $x$ is met (otherwise execution continues), ‘Require $x$’ means that the game terminates with value 0 if condition $x$ is not met (otherwise execution continues), and ‘Stop with $b$’ means that the game terminates with return value $b$. These terms convey an intuitive meaning, e.g., for rewarding an adversary if a winning condition is reached, or penalizing an adversary that does not follow the game rules. For a game $G$ that outputs a Boolean value when run with an adversary $A$, we write $\Pr[G(A)]$ for the probability that the game outputs 1.

**AEAD.** A scheme for providing (nonce-based) authenticated encryption with associated data (AEAD) consists of deterministic algorithms $\text{enc}, \text{dec}$ and associated spaces $K, N, AD, M, C$. The encryption algorithm $\text{enc}$ takes a key $k \in K$, a nonce $n \in N$, an associated-data string $ad \in AD$, and a message $m \in M$, and returns a ciphertext $c \in C$. The decryption algorithm $\text{dec}$ takes a key $k \in K$, a nonce $n \in N$, an associated-data string $ad \in AD$, and a ciphertext $c \in C$, and returns either a message $m \in M$ or the rejection.
We formally define only the security games and adversary advantages. The games are like IND-CCA, and that encryptions be indistinguishable in the presence of chosen-ciphertext attacks (IND-CCA), and that encryptions be indistinguishable in the presence of (passive) chosen-plaintext attacks (IND-CPA). These notions are defined via the encryption oracle Enc and the decryption oracle Dec.

**Figure 1:** AEAD games INT, IND, IND, and MAC game SUF. The condition \( n \notin N \) of lines 05, 19 checks for nonce freshness. The symbol ‘\( \diamond \)' of line 28 is used to suppress sharing the value of \( m \) with the adversary.

---

7 Among other standards, these parameter sets are mandated by RFC5116 [McG08].

8 This is a mild assumption: We are not aware of any practically relevant AEAD scheme that has non-constant expansion.

9 Our approach deliberately does not formalize of the intuitive meanings of “realistic” and “negligible”. We formally define only the security games and adversary advantages.
Message Authentication Codes. A message authentication code (MAC) for message space $M$ consists of a key space $K$ and a tag space $C$, and a deterministic algorithm $M$ that processes a key and a message into a tag:

$$K \times M \rightarrow M \rightarrow C.$$

We formalize the standard security requirement that a MAC scheme provide authenticity. This is defined via the SUF game in Figure 1. We say that a scheme provides strong unforgeability if the maximum advantage $\text{Adv}^{\text{unf}}(\mathcal{A}) := \text{Pr}[\text{SUFO}(\mathcal{A})]$ that can be attained by realistic adversaries $\mathcal{A}$ is negligible.

3 Blackbox Combiners for AEAD

We present an AEAD combiner that is fully black-box, meaning that it works generically for any two component AEADs. Clearly, any such combiner invokes each component scheme at least once: The combined encryption will invoke each component’s encryption algorithm, and the combined decryption will invoke each component’s decryption algorithm. We refer to such combiners as two-enc-two-dec combiners. The combiner we present here requires more invocations, as its decryption algorithm makes three invocations of component algorithms. This is only seemingly suboptimal, as in Section 5 we prove that generically secure two-enc-two-dec combiners actually do not exist. Indeed, the three-invocation combiner from the current section can be seen as tightly complementing the impossibility result.

Actually, it may even be surprising that AEAD combiners that leverage on the security of just one component, while requiring effectively nothing of the other, can exist in the first place. Consider that, during encryption, one component will be invoked first and transform some message into some ciphertext, and then the second component will be invoked on input a message that may depend on the first ciphertext, and output its own ciphertext; the combined ciphertext will be a function of the former two and is required to be INT-secure, i.e., none of its parts may be malleable. While this intuitively requires that the two components protect their ciphertexts mutually (the one scheme protects the other’s ciphertext, and vice versa), in practice one component has to be invoked last, so its output cannot be integrity protected by the other.

Our combiner uses an intriguing technique to side-step this seeming contradiction. Its code is specified in Figure 2. (We silently assume sufficiently compatible nonce spaces, associated data spaces, message spaces, and ciphertext spaces.) The combined encryption is simply a nested encryption of the two component algorithms, using the same nonce and associated data for both (lines 01,02). Note that this is already sufficient to achieve confidentiality (against passive adversaries), if at least one of the components provides confidentiality. The combined decryption first recovers the message by reversing the nesting (lines 05–08). The integrity protection of the outer ciphertext (i.e., the component ciphertext not protected by the other component) is accomplished by re-computing and confirming it (lines 09–10). Note that this approach only works because AEAD encryption is deterministic. (We generalize this re-encryption technique in Section 4.3, where we show that it can be used to turn every INT-PTXT secure scheme into an INT-CTXT secure one.)

We show that if either of the two component schemes is a secure AEAD scheme, then so is the combined scheme. For the following formal statement we assume $N \subseteq N_0 \cap N_1$, $AD \subseteq AD_0 \cap AD_1$, $M \subseteq M_0$, and $C_0 \subseteq M_1$, where $N_i$, $AD_i$, $M_i$, $C_i$ are the spaces of nonces, associated data, messages, and ciphertexts of scheme $\text{AE}_i$, and, without indices, of combiner $\text{CB}$.

**Theorem 1.** For all pairs of correct AEAD schemes $\text{AE}_0$ with constant expansion and $\text{AE}_1$, all indices $i \in \{0, 1\}$, and all adversaries $\mathcal{A}$ against the combined scheme $\text{CB}(\text{AE}_0, \text{AE}_1)$
as defined in Figure 2, there exists an adversary $B^\text{ind}_1$ such that $\text{Adv}^\text{int}_{\text{CB}(AE_0, AE_1)}(A) \leq \text{Adv}^\text{int}_{AE_0, AE_1}(B^\text{int}_1)$, an adversary $B^\text{ind}_0$ such that $\text{Adv}^\text{ind}_{\text{CB}(AE_0, AE_1)}(A) \leq \text{Adv}^\text{ind}_{AE_0, AE_1}(B^\text{ind}_0)$, and an adversary $B^\text{ind}_1$ such that $\text{Adv}^\text{ind}_{\text{CB}(AE_0, AE_1)}(A) \leq \text{Adv}^\text{int}_{AE_1}(B^\text{int}_1) + \text{Adv}^\text{ind}_{AE_1}(B^\text{ind}_1)$. The running time of the adversaries $B$ is about that of $A$.

Proof. From an adversary $A$ against INT security of the combined scheme $\text{CB}(AE_0, AE_1)$ we construct an adversary $B^\text{int}_0$ against the AEAD security of scheme $AE_i$ as follows: $B^\text{int}_0$ entirely simulates scheme $AE_j, j \in \{0, 1\}$ \{i\} itself and derives the encryptions and decryptions under scheme $AE_i$ by forwarding the inputs to the encryption and decryption oracles respectively of game INT against scheme $AE_i$.

Adversary $B^\text{int}_1$, obtaining a forgery for a combined ciphertext $c$ in the decryption oracle, can immediately forward this forgery $c$ to the decryption oracle of the INT game against scheme $AE_1$: note that set $Q$ in the combined INT game (against which $A$ plays) directly complies with set $Q$ in the INT game against scheme $AE_1$ (against which $B^\text{int}_1$ plays). Observe that the re-encryption in combined decryption does not need to be simulated in a reduction to $AE_1$'s INT security as the adversary either provides a forgery (which is directly reduced with the simulation of line 05), or a ciphertext that has been obtained from the combined encryption oracle (for which no integrity verification is necessary), or a ciphertext that decrypts to ‘⊥’ in the first place.

Adversary $B^\text{int}_0$ can compute all algorithms of $AE_1$ directly and use the oracles from the INT game against scheme $AE_0$ to simulate $AE_0$. For a ciphertext $c$, queried to the combined decryption oracle, that has not been an output under the same nonce and associated data of the combined encryption oracle, $B^\text{int}_0$ first decrypts $c$ to obtain $c_0$. If $c_0$ was never derived as part of a combined encryption query under the same nonce and associated data, its decryption either fails or it represents a forgery against INT security of scheme $AE_0$ (such that the reduction is successful in this case). If $c_0$ was, however, derived as part of such a previous combined encryption query, then $c_0' \neq c$ would have been the resulting ciphertext under scheme $AE_1$ (as computed in lines 09–10). Consequently, the combined decryption rejects this ciphertext (as line 10 would output ⊥). Thereby, the only way, adversary $A$ produces a valid forgery, can be reduced to INT security of scheme $AE_0$ such that $\text{Adv}^\text{int}_{\text{CB}(AE_0, AE_1)}(A) \leq \text{Adv}^\text{int}_{AE_0}(B^\text{int}_0)$ for both $i \in \{0, 1\}$.

Reducing successful adversaries against confidentiality to $AE_0$'s IND security is trivial: $B^\text{ind}_0$ derives $c_0$ from the encryption oracle in the IND game against scheme $AE_0$ by querying both messages $m^0$ and $m^1$ under $(n, ad)$, and encrypts $c_0$ under $AE_1$ itself with $(k_1, n, ad)$. The decryption oracle in the IND game against the combiner can accordingly be simulated by actually computing decryptions under scheme $AE_1$ and deriving decryptions under

\[
\begin{array}{cc}
\text{Proc } \text{enc}(k, n, ad, m) & \text{Proc } \text{dec}(k, n, ad, c) \\
00 (k_0, k_1) \leftarrow k & 04 (k_0, k_1) \leftarrow k \\
01 c_0 \leftarrow \text{enc}_0(k_0, n, ad, m) & 05 c_0 \leftarrow \text{dec}_1(k_1, n, ad, c) \\
02 c_1 \leftarrow \text{enc}_1(k_1, n, ad, c_0) & 06 \text{If } c_0 = \bot: \text{Return } \bot \\
03 \text{Return } c_1 & 07 m \leftarrow \text{dec}_0(k_0, n, ad, c_0) \\
& 08 \text{If } m = \bot: \text{Return } \bot \\
& 09 c'_1 \leftarrow \text{enc}_1(k_1, n, ad, c_0) \\
& 10 \text{If } c'_1 \neq c: \text{Return } \bot \\
& 11 \text{Return } m
\end{array}
\]
scheme $\text{AE}_0$ from the IND game against $\text{AE}_0$. A successful guess $b'$ for the challenge bit $b$ by adversary $\mathcal{A}$ is thereby immediately a successful guess for $\mathcal{B}_1^{\text{ind}}$ as well. Hence, we have $\text{Adv}^{\text{ind}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(\mathcal{A}) \leq \text{Adv}^{\text{ind}}_{\text{AE}_1}(\mathcal{B}_1^{\text{ind}})$.

For the reduction to scheme $\text{AE}_1$, we proceed in one game hop: in game $G_1$ we abort on decryptions (in the IND game’s decryption oracle against the combiner) that output a message (i.e., not $\perp$). An adversary, detecting this game hop, breaks INT security (see above for the reduction). As a result, we have $\text{Adv}^{\text{ind}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(\mathcal{A}) \leq \text{Adv}^{\text{int}}_{\text{AE}_1}(\mathcal{B}_1^{\text{int}}) + \text{Adv}^{G_1}$. In game $G_1$ we can assume that none of the ciphertexts, given to the combiner’s decryption oracle, result in a valid message (hence the decryption oracle does not need to be simulated anymore). From game $G_1$, we can directly reduce to the IND security of scheme $\text{AE}_1$. $\mathcal{B}_1^{\text{ind}}$ encrypts both messages $m^0$ and $m^1$ under $(k_0, n, ad)$ itself and then queries the encryption oracle of the IND game against scheme $\text{AE}_1$ for both resulting ciphertexts $c_0^1$ and $c_0^0$ as input messages (where $|c_0^1| = |c_0^0|$). The guessed bit $b'$ is therefore valid in case of a successful adversary $\mathcal{A}$, resulting in $\text{Adv}^{\text{ind}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(\mathcal{A}) \leq \text{Adv}^{\text{int}}_{\text{AE}_1}(\mathcal{B}_1^{\text{int}}) + \text{Adv}^{\text{ind}}_{\text{AE}_1}(\mathcal{B}_1^{\text{ind}})$.

Note that our combiner inherits the security guarantees of its underlying secure scheme. As a result, it can be applied recursively to combine more than two AEAD schemes (such that only one of them needs to remain secure). Also it is notable that for the combiner’s IND and INT security it suffices to have scheme $\text{AE}_0$ only IND secure and scheme $\text{AE}_1$ only INT secure.\footnote{The simulation of the re-encryption in the combiner’s decryption is the problematic part because of which we first reduce to IND security. We cannot use the encryption oracle in the IND game against $\text{AE}_1$ to simulate this re-encryption because either the respective nonce was used in a combined encryption query before (not allowing us to query encryption under the same nonce again), or the adversary wants to query a combined encryption under the same nonce in the future (which it then cannot do as our simulation exhausted this nonce already). For nonce misuse-resilient schemes (for which the security experiment allows for multiple encryptions under the same nonce, as long as e.g., associated data changes), this issue is resolved.}

In the full version \cite{PoetteringRoesler20} we present two further blackbox combiners that have different performance properties (i.e., slightly better in some dimensions while worse in other dimensions). We provide these combiners for didactic reasons since we believe the underlying concepts support the understanding of AEAD combiners in general.

**Remarks on Tidy Encryption Schemes** The tidiness property \cite{NRS14} of an AEAD scheme requires that different ciphertexts decrypt to different messages. Equivalently, it is required that any ciphertext that validly decrypts to a message is also the result of an encryption of that message (under the same key, nonce, and associated data). Given a candidate AEAD scheme it is typically straightforward to decide from its specification whether it is tidy or not, and in fact most modern AEAD schemes turn out to have this property. (This includes EtM constructions as well as highly integrated modes like OCB. We note however that tidiness is neither a necessary nor a sufficient condition for attaining INT or IND security.) For tidy schemes, the decrypt-then-encrypt-then-compare component of our blackbox combiner collapses to a simple decryption. As a consequence, securely combining two AEAD schemes, one of which is guaranteed to be tidy, can be done in a particularly efficient way. (The combiner would be just like the one of Figure 2, but with lines 09,10 removed.) We caution however that blindly relying on this simpler and more efficient combiner in practice, even if all component schemes are evidently tidy according to their specification, might lead to fatal results. This is because ‘tidiness by specification’ means
little if ‘tidiness of implementation’ is what ultimately counts. We note that it is fairly easy to (mis)implement a theoretically tidy scheme in a practically untidy way: The decryption process of most current AEAD schemes concludes with a step where some authentication value is computed from the results of the plaintext recovery and compared with a tag positioned at the end of the ciphertext. It seems conceivable that a flawed implementation would compare these two values in an incomplete way, e.g., by comparing the values except for their last bits. Such an implementation would still be formally correct, and could also provide a very fair level of authenticity and confidentiality, yet it would be untidy. As we believe that effectively assessing the practical tidiness of schemes implemented as closed-source software or in silicon is unrealistically costly, and even in the case of open-source software may represent a considerable challenge, we ultimately only recommend using our generic combiner (or one of the combiners from Section 4).

We finally note that a combination based on a tidy scheme allows for a circumvention of our performance bound from Section 5 since then only one algorithm invocation per scheme and operation is necessary. Our impossibility result is based on combining a secure AEAD scheme with an insecure untidy scheme, and crucially exploits the untidiness of the latter.

4 Non-Blackbox Combiners for AEAD

In the previous section we proposed an AEAD combiner that used its component AEAD schemes fully generically, i.e., we assumed no property of the latter other than correctness and security. In this section we study more efficient AEAD combiners, at the expense of having to require specific structures of at least one component. Concretely, we propose two classes of improved combiners. The first class applies in cases where at least one of the AEAD components is induced by the encrypt-then-MAC paradigm, and the second class can be used if the AEAD component is constructed from an AE scheme and a PRF using ciphertext translation.\(^\text{12}\)

4.1 EtM-Structured AEAD

In practice, authenticated encryption is often achieved from an encryption scheme and a message authentication code (MAC) using the encrypt-then-MAC (EtM) paradigm, either explicitly or implicitly. The idea is that first the message is encrypted using some passively secure encryption scheme, and then the ciphertext is integrity-protected using the MAC, providing INT security and lifting IND-CPA to IND-CCA security. Many real-world protocols such as TLS [Gut14] and SSH [SSH, ADHP16] can be used with such an AEAD construction. Further, many direct AEAD constructions make use of this design principle as well, though rather implicitly. Examples for the latter include the GCM [MV04] and CWC [KVW04] modes of operation.

We propose two EtM based combiners: One that combines a generic AEAD scheme with an EtM-structured one, and a second that combines two EtM-structured AEAD schemes. By explicitly considering the design principle of the component schemes, the combiners can distribute the processing overhead between encryption and decryption more evenly compared to the blackbox combiner of Section 3. The second combiner has also particularly short ciphertexts.

We say that an AEAD scheme is EtM-structured if its key space and its ciphertext space have the form \( K = K' \times K'' \) and \( C = C' \times C'' \) for some sets \( K', K'', C', C'' \), and there

\(^{12}\text{With ‘ciphertext translation’ [Rog02] we refer to a technique that transforms an AE scheme into an AEAD scheme by XOR-ing the PRF evaluation of the associated data into the ciphertext. This is, for instance, used in EAX and OCB.}\)
exist three algorithms
\[ \mathcal{K}' \times \mathcal{N} \times \mathcal{M} \to \mathcal{E} \to \mathcal{C}' \quad \mathcal{K}' \times \mathcal{N} \times \mathcal{C}' \to \mathcal{D} \to \mathcal{M} \cup \{\bot\} \quad \mathcal{K}'' \times \mathcal{M}' \to \mathcal{M} \to \mathcal{C}'' \],
where we write \( \mathcal{M}' = \mathcal{N} \times \mathcal{AD} \times \mathcal{C}' \), such that the code in Figure 3 implements algorithms \( \text{enc} \) and \( \text{dec} \). Note how algorithms \( \mathcal{E} \) and \( \mathcal{D} \) stand for the encryption and decryption algorithms, respectively, while \( \mathcal{M} \) implements the MAC. An EtM-structured AEAD scheme is secure if algorithms \((E, D)\) provide indistinguishability against passive adversaries (according to game \(\text{pIND}^{13}\)) and algorithm \(M\) is a strongly unforgeable MAC (according to game \(\text{SUF}\)).

### EtM with Blackbox Combiner

We specify our first EtM combiner in Figure 4. It intertwines an EtM-structured AEAD scheme \(\mathcal{A}\mathcal{E}_0\) implemented by algorithms \((\mathcal{E}_0, \mathcal{D}_0, \mathcal{M}_0)\) with a blackbox AEAD scheme \(\mathcal{A}\mathcal{E}_1 = (\text{enc}_1, \text{dec}_1)\). For combined encryption, the ciphertext of the message encryption under the EtM-scheme (line 01) is fed into the blackbox encryption algorithm (line 02). The resulting ciphertext is then MACed together with the associated data (line 03). The combined decryption first verifies the MAC (lines 08–09) and then, if verification succeeds, reverses the nested encryption by decrypting under both schemes (lines 10–12).

Confidentiality is protected by the combiner due to the nested encryption, and integrity is maintained since either the MAC is secure and \(c\) thus protected directly, or \(c_1\) is integrity protected by \(\text{enc}_1\) such that the MAC reduces to being just a deterministic computation on it (which cannot be manipulated).

### Figure 3: EtM construction.

![EtM construction](image)

### Figure 4: EtM combiner. **Associated cost:** enc: \(M + (A + M) + (A + M) = 2A + 3M\); dec: \((A + M) + (A + M) + M = 2A + 3M\). **Ciphertext length:** \(M + \tau + \tau\).

Our EtM combiner is INT and IND secure for an EtM-structured scheme \(\mathcal{A}\mathcal{E}_0\) and a blackbox AEAD scheme \(\mathcal{A}\mathcal{E}_1\) if \(\mathcal{A}\mathcal{E}_0\)'s algorithms provide SUF and pIND security respectively, or \(\mathcal{A}\mathcal{E}_1\) is a secure AEAD scheme. For the following formal statement we assume \(\mathcal{N} \subseteq \mathcal{N}_0 \cap \mathcal{N}_1, \mathcal{AD} \subseteq \mathcal{A}\mathcal{D}_0 \cap \mathcal{A}\mathcal{D}_1, \mathcal{M} \subseteq \mathcal{M}_0, \mathcal{C}_0 \subseteq \mathcal{M}_1, \text{and } \mathcal{N} \times \mathcal{AD} \times \mathcal{C}_1 \subseteq \mathcal{M}_0\), where

\[\text{Note that } (E, D) \text{ have no associated-data input. Oracle Enc thus ignores the } ad \text{ input in game pIND against these algorithms.}\]
The running time of the adversaries that 132 Combiners for AEAD

For all pairs of correct AEAD schemes $\text{AE}_0$, implemented by $(E_0, D_0, M_0)$ with constant expansion, and $\text{AE}_1$, all indices $i \in \{0, 1\}$, and all adversaries $A$ against the combined scheme $CB(\text{AE}_0, \text{AE}_1)$ from Figure 4, there exists an adversary $B_i^{\text{INT}}$ such that $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{int}}(A) \leq \text{Adv}_{M_0}^{\text{ind}}(B_0^{\text{ind}})$, an adversary $B_1^{\text{INT}}$ such that $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{int}}(A) \leq \text{Adv}_{AE_i}^{\text{int}}(B_1^{\text{int}})$, an adversary $B_0^{\text{IND}}$ such that $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{M_0}^{\text{adv}}(B_0^{\text{adv}}) + \text{Adv}_{AE_i}^{\text{adv}}(B_0^{\text{adv}})$, and an adversary $B_1^{\text{IND}}$ such that $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{AE_1}^{\text{ind}}(B_1^{\text{ind}})$. The running time of the adversaries $B$ is about that of $A$.

Proof. We split our proof into reductions to integrity of each scheme and reductions to confidentiality of each scheme.

The reduction from INT security of the combiner to SUF security of scheme $\text{AE}_0$’s MAC is straightforward. All encryption and decryption queries of an adversary $A$ against the combiner are simulated by reduction $B_i^{\text{INT}}$ by directly computing all algorithms except for the MAC $M_0$. MAC computations are instead derived from the SUF game such that lines 08–09 are obtained from oracle $Vfy$ (cf. Figure 1). In case adversary $A$ queries the decryption oracle on a ciphertext that it did not obtain from the encryption oracle under the same pair $(n, ad)$, then the MAC verification either fails (such that it is neither a forgery in game INT nor in game SUF) or succeeds such that the forgery in the INT game is directly forwarded as a forgery in the SUF game. Thus, we have $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{int}}(A) \leq \text{Adv}_{M_0}^{\text{adv}}(B_0^{\text{adv}})$.

Adversary $B_1^{\text{INT}}$, reducing INT security of the combiner to INT security of scheme $\text{AE}_1$, computes all algorithms of scheme $\text{AE}_1$ directly and derives all computations under $\text{AE}_0$ from the INT game, against which it plays. A ciphertext $c = c_1 || t$, provided to the combined decryption oracle, that differs from all ciphertexts under the same pair $(n, ad)$, output by the combined encryption oracle, can differ in the ciphertext part $c_1$ and in the tag part $t$. If it only differs in the tag part, then the tag verification will fail as there only exists one valid tag per tuple $(n, ad, c_1)$ (as MAC computation is deterministic). If it differs in the ciphertext part, then either decryption under $dec_1$ outputs $\bot$ or $A$ broke INT security of scheme $\text{AE}_1$ such that $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{int}}(A) \leq \text{Adv}_{AE_1}^{\text{adv}}(B_1^{\text{adv}})$.

For the reduction of confidentiality from the combiner to the EtM-structured scheme, we proceed in a (short) sequence of games. In the first game, we output $\bot$ on any combined decryption query. An adversary, distinguishing this game from the original IND game against the combiner, breaks the SUF security of MAC $M_0$ as shown above. Due to this game hop, adversary $B_0^{\text{IND}}$, reducing successful IND adversaries $A$ from this game to the pIND security of scheme $\text{AE}_0$’s algorithms, does not need to simulate the combined decryption oracle anymore. The simulation of the combined encryption oracle is conducted by querying the encryption oracle of scheme $\text{AE}_0$’s MAC against algorithm $E_0$ of scheme $\text{AE}_0$ for both messages $m_0$ and $m_1$ that are input to the combined encryption oracle. The remaining computations are conducted directly by reduction $B_0^{\text{IND}}$. As distinguishing between combined encryptions of $m_0$ and $m_1$ distinguishes encryptions of $m_0$ and $m_1$ under the EtM-structured scheme, we have $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{AE_0}^{\text{adv}}(B_0^{\text{adv}}) + \text{Adv}_{AE_1}^{\text{adv}}(B_0^{\text{adv}})$.

The reduction $B_1^{\text{IND}}$, reducing IND security of the combiner to IND security of scheme $\text{AE}_1$, computes all algorithm invocations except for $enc_1$ and $dec_1$ directly. Computations of $enc_1$ and $dec_1$ are obtained from the IND game against scheme $\text{AE}_1$. In order to embed the challenge, reduction $B_1^{\text{IND}}$ computes algorithm $E_0$ twice during combined encryption: once under each message $m_0$ and $m_1$. Then it queries the two resulting equally long ciphertexts as challenge messages to oracle $Enc$ in game IND against scheme $\text{AE}_1$. The resulting ciphertext $c_1$ is MACed by $B_1^{\text{IND}}$ to obtain $c = c_1 || t$. An adversary $A$, successfully guessing bit $b$ in the IND game against the combiner, thereby successfully guesses bit $b$ in the IND game against scheme $\text{AE}_1$. Consequently we have $\text{Adv}_{CB(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{AE_1}^{\text{ind}}(B_1^{\text{ind}})$.
which completes the proof.\hfill \Box

**EtM with EtM Combiner** We now consider a combiner that takes two EtM-structured schemes $\text{AEA}_0$ and $\text{AEA}_1$ implemented by algorithms $(E_0, D_0, M_0)$ and $(E_1, D_1, M_1)$, respectively, and produces an AEAD scheme that is EtM-structured as well. As many real-world protocols are based on EtM-structured AEAD schemes, when aiming to combine these schemes with others there is a wide range of options to choose from. This combiner features the shortest ciphertext length among the ones considered in this article. Last not least, since the combined scheme is again EtM-structured, it can straight-forwardly be combined with further EtM-structured schemes.

We specify our combiner in Figure 5, where we make the algorithms $(E, D, M)$ of the EtM-structured result explicit. To obtain the full AEAD scheme from this, apply the procedures from Figure 3. The following description refers to the latter.

The combined encryption encrypts the message in a nested form under both schemes (see lines 01–02) and then computes MACs over the final ciphertext under both MAC algorithms (see lines 10–11). The resulting MAC tags are then XORed and appended to the final encryption ciphertext. For combined decryption, first the MAC computations are repeated and compared with the provided XOR of MAC tags in the input ciphertext (compare with Figure 3 lines 07–08). Finally, the nested encryption is reversed (lines 05–07 in Figure 5). Note that in most practical cases the ciphertext output by $E$ has the same length as the input message. If we further assume that both component schemes use the same tag length, the overall combined ciphertext has the length of the message plus this tag length.

Confidentiality is again achieved by the nested encryption, and integrity is protected under each MAC. If one MAC is secure, the other MAC can be seen as a function, deterministically computed on integrity protected input, whose output is added only for transportation.

<table>
<thead>
<tr>
<th>$\text{Proc } E(ke, n, m)$</th>
<th>$\text{Proc } D(ke, n, c)$</th>
<th>$\text{Proc } M(km, m)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$00 \ (ke_0, ke_1) \leftarrow ke$</td>
<td>$04 \ (ke_0, ke_1) \leftarrow ke$</td>
<td>$09 \ (k_0, k_1) \leftarrow k$</td>
</tr>
<tr>
<td>$01 \ c_0 \leftarrow E_0(ke_0, n, m)$</td>
<td>$05 \ c_0 \leftarrow D_1(ke_1, n, c)$</td>
<td>$10 \ t_0 \leftarrow M_0(k_0, m)$</td>
</tr>
<tr>
<td>$02 \ c \leftarrow E_1(ke_1, n, c_0)$</td>
<td>$06 \ \text{If } c_0 = \perp: \text{Return } \perp$</td>
<td>$11 \ t_1 \leftarrow M_1(k_1, m)$</td>
</tr>
<tr>
<td>$03 \ \text{Return } c$</td>
<td>$07 \ m \leftarrow D_0(ke_0, n, c_0)$</td>
<td>$12 \ \text{tag } \leftarrow t_0 \oplus t_1$</td>
</tr>
<tr>
<td>$08 \ \text{Return } m$</td>
<td>$13 \ \text{Return } \text{tag}$</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5:** EtM-EtM combiner. **Associated cost:** enc: $M + M + (A + M) + (A + M) = 2A + 4M$; dec: $(A + M) + (A + M) + M + M = 2A + 4M$. **Ciphertext length:** $M + \tau$.

If either of the underlying MtE-structured schemes provides SUF and pIND security for its respective algorithms, then the combiner from Figure 5 achieves the same security properties. Moreover, it suffices if one scheme has a secure MAC and the other scheme’s encryption provides confidentiality against passive adversaries to obtain a secure combination. For the formal statement we assume $N \subseteq N_0 \cap N_1, M \subseteq M_0, C_0 \subseteq M_1$, and $N \times AD \times C_1 \subseteq M_1$ where $N_0, AD, M_1, C_0$ are the spaces of nonces, associated data, messages, and ciphertexts of scheme $\text{AEA}_i$ and, without indices, of combiner $CB$, and

**Theorem 3.** For all pairs of correct AEAD schemes $\text{AEA}_0$ with constant expansion and $\text{AEA}_1$ implemented by $(E_i, D_i, M_i)$, all indices $i \in \{0, 1\}$, and all adversaries $A$ against the combined scheme $CB(\text{AEA}_0, \text{AEA}_1)$ as depicted in Figure 5, there exists an adversary $B_{\text{sup}}^{A_i}$ such that $\text{Adv}_{CB(M_0, M_1)}^{\text{sup}}(A) \leq \text{Adv}_{M_i}^{\text{sup}}(B_{\text{sup}}^{A_i})$, and an adversary $B_i^{\text{ind}}$ such that $\text{Adv}_{CB(\text{AEA}_0, \text{AEA}_1)}(A) \leq \text{Adv}_{\text{AEA}_i}^{\text{ind}}(B_i^{\text{ind}})$. The running time of the adversaries $B_i$ is about that of $A$.
Parts of this statement have been proven before when pure symmetric encryption was considered (e.g., by Herzberg [Her05]) but we are not aware of SUF secure MAC combiners in the literature. For completeness we give a full proof.

Proof. Reduction $B_{\text{utf}}$, playing the SUF game against the MAC of scheme $\text{AE}_i$, while simulating the SUF game for adversary $A$ against the combined MAC $M$, computes algorithm $M_j$, $j \in \{0,1\} \setminus \{i\}$ directly. In order to obtain MAC tags $t_i$ for $A$’s queries to oracle $\text{Tag}$, it queries the Tag oracle in the SUF game against MAC $M_i$. For the simulation of oracle $\text{Vfy}$ towards $A$ on input $(m, t)$, $B_{\text{utf}}$ first computes $t_j$ under $M_j$ directly and then queries oracle $\text{Vfy}$ for input $(m, t \oplus t_j)$. The result of this query is forwarded to adversary $A$. For a forgery against the combined MAC, input $(m, t)$ to the combined Vfy oracle must not have been an input-output pair of a combined Tag oracle query before. If only the tag input $t$ to a combined $\text{Vfy}$ oracle query differs from previous queries to the combined Tag oracle, then, by the determinism of both algorithms $M_i$ and $M_j$, this query is answered with $\perp$. If, on a new message input (i.e., not yet queried to combined $\text{Tag}$) to the combined $\text{Vfy}$ oracle, the tag verification succeeds (such that this is a valid forgery against the combined MAC), then $(m, t \oplus t_j)$ is a valid forgery against algorithm $M_i$ (since $1$. $m$ was not queried before and $2$. $t \oplus t_j$ must be the MAC under $M_i$ for $m$). Consequently, we have $\text{Adv}_{\text{CB}(M_0, M_1)}(B_{\text{utf}}) \leq \text{Adv}_{\text{AE}_i}(B_{\text{utf}})$. Reducing pIND security from the combiner to each scheme $\text{AE}_i$ works by simulating the combined encryption as follows (remember that the combined decryption does not need to be simulated in game pIND): Reduction $B_{\text{pind}}^0$ derives ciphertext $c_0$ for a combined encryption query under input $(m^0, m^1)$ by querying the encryption oracle in game pIND against scheme $\text{AE}_0$ under the same input. Encryptions under scheme $\text{AE}_0$ are thereby directly computed. For reducing to pIND security of scheme $\text{AE}_1$, reduction $B_{\text{pind}}^1$ computes two equally long ciphertexts $c_0^1, c_1^1$ by encrypting each combined encryption oracle input $m^0$ and $m^1$ with algorithm $E_0$. These ciphertexts are then forwarded to the encryption oracle in game pIND against scheme $\text{AE}_1$, which outputs the combined ciphertext $c$. In either of both reductions, the challenge bit $b$ in the combined pIND game equals the challenge bit in the pIND game against which $B_{\text{pind}}^b$ plays, such that a successful adversary $A$ breaks both underlying schemes’ pIND security with $\text{Adv}_{\text{pind}}^{\text{CB}(\text{AE}_0, \text{AE}_1)}(A) \leq \text{Adv}_{\text{AE}_i}^{\text{pind}}(B_{\text{pind}}^b)$. This completes the proof. 

4.2 Ciphertext Translation based AEAD

We consider the combination of AEAD schemes where at least one was obtained via ciphertext translation [Rog02]. As in Section 4.1 this results in particularly efficient combiners.

The term ‘ciphertext translation’ refers to a technique that transforms an AE scheme into an AEAD scheme by XORing a PRF value derived from the associated data into the ciphertext. That is, encryption and integrity protection of the message are conducted independently of the associated data. Examples where this technique is used include EAX [BRW04] and the OCB family (OCB3 [KR11] and the insecure OCB2 [Rog04, IIMP19]).

We say that an AEAD scheme is ciphertext translated if there exist three algorithms $\mathcal{K} \times \mathcal{N} \times \mathcal{M} \rightarrow \mathcal{E} \rightarrow \mathcal{C}$ $\mathcal{K} \times \mathcal{N} \times \mathcal{C} \rightarrow \mathcal{D} \rightarrow \mathcal{M} \cup \{\perp\}$ $\mathcal{K} \times \mathcal{N} \times \mathcal{AD} \rightarrow \mathcal{F} \rightarrow \mathcal{C}$, such that the code in Figure 6 implements algorithms enc and dec. (Note that function $F$ sees the nonce, but this is actually optional.)

Security-wise, our results assume of a ciphertext translated AEAD scheme that it offers INT and IND security for the composed algorithms (enc, dec). That is, our consideration of ciphertext translated schemes is only restrictive regarding their syntax but not regarding security.
The idea behind our combiner of a ciphertext translated AEAD scheme $\text{AE}_1$, implemented by algorithms $(E_1, D_1, F_1)$, with a blackbox AEAD scheme $\text{AE}_0 = (\text{enc}_0, \text{dec}_0)$ is very close to our blackbox combiner from Section 3. However, by treating ciphertext translation explicitly, the combiner can save one operation in decryption and hence reach better efficiency.

We specify our ciphertext translation based combiner in Figure 7. It nests the blackbox AEAD encryption into the ciphertext translated AEAD encryption for combined encryption (lines 01–03) and reverses this operation for combined decryption (lines 06–10). To protect the integrity of the ciphertext, the re-encryption technique from Section 3 is applied: The outer encryption (of the ciphertext translated scheme) is re-computed to verify that, if the ciphertext translated scheme provides no ciphertext integrity, the input ciphertext $c_1$ would have been the result of an honest encryption under $(k_1, n, c_0)$ (lines 11–12). Since the computation of function $F$ is independent of the input ciphertext $c$, it does not need to be re-computed and compared in order to verify integrity.

**Figure 6:** Ciphertext translated AEAD construction.

**Figure 7:** Ciphertext translation based combiner from blackbox AEAD scheme $\text{AE}_0$ and ciphertext translated AEAD scheme $\text{AE}_1$. **Associated cost:** $\text{enc}(A + M) + (A + M) = 2A + 2M$; $\text{dec}(A + M) + (A + M) + M = 2A + 3M$. **Ciphertext length:** $M + \tau + \tau$.

The ciphertext translation based combiner reaches INT and IND security if either of the underlying schemes provides these properties. For the formal statement we assume $\mathcal{N} \subseteq \mathcal{N}_0 \cap \mathcal{N}_1$, $\mathcal{AD} \subseteq \mathcal{AD}_0 \cap \mathcal{AD}_1$, $\mathcal{M} \subseteq \mathcal{M}_0$, and $\mathcal{C}_i \subseteq \mathcal{M}_i$, where $\mathcal{N}_1$, $\mathcal{AD}_1$, $\mathcal{M}_i$, $\mathcal{C}_i$ are the spaces of nonces, associated data, messages, and ciphertexts of scheme $\text{AE}_i$ and, without indices, of combiner CB.

**Theorem 4.** For all pairs of correct AEAD schemes $\text{AE}_0$ with constant expansion and $\text{AE}_1$, implemented by $(E_1, D_1, F_1)$, all indices $i \in \{0, 1\}$, and all adversaries $A$ against the combined scheme CB($\text{AE}_0$, $\text{AE}_1$) as depicted in Figure 7, there exists an adversary $B^{\text{int}}$ such that $\text{Adv}_{\text{CB}(\text{AE}_0, \text{AE}_1)}^{\text{int}}(A) \leq \text{Adv}_{\text{AE}_1}^{\text{int}}(B^{\text{int}})$, an adversary $B_0$ such that $\text{Adv}_{\text{CB}(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{\text{AE}_0}^{\text{ind}}(B_0)$, and an adversary $B_1$ such that $\text{Adv}_{\text{CB}(\text{AE}_0, \text{AE}_1)}^{\text{ind}}(A) \leq \text{Adv}_{\text{AE}_1}^{\text{ind}}(B_1) + \text{Adv}_{\text{AE}_1}^{\text{ind}}(B_1)$. The running time of the adversaries $B$ is about that of $A$.

**Proof.** The proof proceeds in two steps: first we slightly change the combiner by adding a redundant computation. Then we apply Theorem 1 since adding the redundant computation makes our combiner here equivalent with the blackbox combiner from Section 3.
In our first game, we add the computation $c' \leftarrow c'_1 \oplus F_1(k_1, n, ad)$ to the code from Figure 7 between lines 11 and 12, and call this addition ‘line 11.5’ hereafter. Additionally, we change the first part of line 12 from “If $c'_1 \neq c_1$: …” to “If $c' \neq c$: …”. These two changes are fully oblivious to the adversary since, by line 06, $c_1$ and $c$ are in the exact same relation as $c'_1$ and $c'$ (according to our changes). Consequently, no adversary can detect this game hop.

Now observe that, due to our changes, all computations of encryptions and decryptions under scheme $\text{AE}_1$ can be merged (disregarding the ciphertext translation idea) to blackbox algorithms ($\text{enc}_1, \text{dec}_1$). By reversing the explicit consideration from Figure 6, lines 02–03 and lines 11–11.5 are replaced by blackbox $\text{enc}_1$ respectively and lines 06–07 are replaced by blackbox $\text{dec}_1$. The resulting scheme is exactly the same as the blackbox combiner from Figure 2. As a result, INT and IND security in this game follow from the proof of Theorem 1.

Consequently, we obtain $\text{Adv}^{\text{ind}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(A) \leq \text{Adv}^{\text{ind}}_{\text{AE}_1}(B^{0}_{1}), \quad \text{Adv}^{\text{ind}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(A) \leq \text{Adv}^{\text{int}}_{\text{AE}_1}(B^{1}_{1})$, and $\text{Adv}^{\text{int}}_{\text{CB}(\text{AE}_0, \text{AE}_1)}(A) \leq \text{Adv}^{\text{int}}_{\text{AE}_0}(B^{1}_{1})$ for both $i \in \{0, 1\}$ which concludes our proof.

4.3 Deriving INT-CTXT from INT-PTXT

So far, all of our combiners use the idea of verifying the integrity of ciphertexts by partially re-computing them. This technique can be generalized by considering INT-PTXT and INT-CTXT security, where the latter is defined by our INT game and a formal definition of INT-PTXT security is obtained by changing lines 07 and 12 of game INT in Figure 1 such that tuples $(n, ad, m)$ are considered in the comparison instead. Abstractly, every nonce based scheme that is INT-PTXT secure can efficiently be turned into a scheme that is INT-CTXT secure by verifying the respective ciphertext via re-computation. This additional computation induces tidiness of the AEAD scheme (see Section 3) such that manipulations of ciphertexts must result in manipulations of plaintexts.

Jost et al. [JBB18] prove that INT-PTXT and INT-CTXT security are equivalent for schemes that are also IND secure. Our technique is actually independent of any confidentiality requirements. We are not aware that this result has been stated in the literature before and thus provide a formal proof.

Lemma 1. For all adversaries $A$ and all nonce-based AEAD schemes $\text{AE} = (\text{enc}, \text{dec})$ it holds for nonce-based AEAD scheme $\text{AE}' = (\text{enc}, \text{dec}')$ with

\[ \text{dec}'(k, n, ad, c): m \leftarrow \text{dec}(k, n, ad, c); \text{If } c = \text{enc}(k, n, ad, m): \text{Return } m; \text{Else: Return } \bot \]

that there exists an adversary $B$ such that $\text{Adv}^{\text{int}-\text{ctxt}}_{\text{AE}'}(A) \leq \text{Adv}^{\text{int}-\text{ptxt}}_{\text{AE}}(B)$.

Proof. Obviously all queries of an adversary $A$ in the INT-CTXT game can be answered by an adversary $B$ against the INT-PTXT game by simply relaying the algorithm invocations. If an adversary $A$ provides a ciphertext to the decryption oracle of the INT-CTXT game, simulated by adversary $B$, that was not output by an earlier query to the encryption oracle of the INT-CTXT game, then this ciphertext 1. either results in a decryption failure under algorithm $\text{dec}$ (such that it is no forgery in either game), 2. decrypts via $\text{dec}$ to a message which was queried under the same pair of nonce and associated data to the encryption oracle before (which is not a forgery in the INT-PTXT game but probably in the INT-CTXT game), or 3. decrypts to a message that has not been queried to the encryption oracle before under the same pair of nonce and associated data (resulting in a valid forgery against INT-PTXT security). Case 3. can obviously be reduced to INT-PTXT security. In case 2., the adversary (by definition of the cases) produced a new ciphertext $c'$ for a message $m$ that was queried to the encryption oracle, outputting ciphertext $c$, such that $c \neq c'$. Since the consistency check via re-computation will again produce ciphertext $c$
from message $m$, the output of $\text{dec}'$ will be $\bot$ such that ciphertext $c'$ cannot be a forgery in either security game. Consequently, $A$ can only win the INT-CTXT game against scheme $\text{AE}'$ if it produces an INT-PTXT forgery for scheme $\text{AE}$. This completes the proof.

As a consequence of this result, it actually suffices for our re-computation based combiners that the outer AEAD scheme (i.e., the one invoked secondly during combined encryption) reaches only INT-PTXT security in order to achieve INT security for the combined scheme.

Note finally that our result is independent of the associated data. It thus also applies to pure authenticated encryption.

5 On the Impossibility of Two-Invocation Combiners

We proposed explicit AEAD combiners in Sections 3 and 4. The constructions, though efficient, require more than the intuitively minimal number of invocations of the components’ encryption and decryption algorithms. Concretely, while combiners in general will not do without invoking for each encryption operation at least once the encryption algorithm of each component, and for each decryption operation at least once the decryption algorithm of each component, it is a priori unclear why a combiner would necessarily need more than these. In this section we give a negative result, showing that no generic AEAD combiner that reaches the intuitive minimum can exist.

We note that our impossibility result holds for the combination of generic AEAD schemes, i.e., that fulfill the set of properties formalized in Section 2. If one demands further properties (that is, if one makes the primitive stronger) the result may not hold any more. For instance, in Section 4 we demonstrate that zero-overhead combiners exist for EtM schemes, and in Section 3 we do the same for schemes the tidiness of which can be effectively confirmed.

We say that an AEAD combiner $\text{CB}$ is two-enc-two-dec if for any AEAD schemes $\text{AE}_0 = (\text{enc}_0, \text{dec}_0)$ and $\text{AE}_1 = (\text{enc}_1, \text{dec}_1)$ the algorithms $\text{enc}$ and $\text{dec}$ of $\text{CB}(\text{AE}_0, \text{AE}_1)$ both internally make precisely two algorithm invocations: $\text{enc}$ invokes $\text{enc}_0$ and $\text{enc}_1$ one time each, and $\text{dec}$ invokes $\text{dec}_0$ and $\text{dec}_1$ one time each. The order in which $\text{enc}$ and $\text{dec}$ invoke their algorithms determines two classes of two-enc-two-dec combiners: If the first invocations made by $\text{enc}$ and $\text{dec}$ are both of algorithms of the same component (i.e., both $\text{enc}$ and $\text{dec}$ invoke $\text{AE}_0$ first, or both $\text{enc}$ and $\text{dec}$ invoke $\text{AE}_1$ first), we say the combiner is synchronized. Otherwise, if the first invocations are of algorithms of different components (i.e., $\text{enc}$ invokes $\text{AE}_0$ first and $\text{dec}$ invokes $\text{AE}_1$ first, or the other way round), we say the combiner is reversed. The algorithms specified in Figure 8 characterize synchronized and reversed two-enc-two-dec combiners: A combiner $\text{CB}$ is of the synchronized type if there exist algorithms $\alpha, \beta, \gamma, \phi, \pi, \rho$ such that $\text{CB}$’s algorithms coincide with $\text{enc}^S$ and $\text{dec}^S$, and it is of the reversed type if algorithms $\alpha, \beta, \gamma, \phi, \pi, \rho$ exist such that the combiner’s algorithms coincide with $\text{enc}^R$ and $\text{dec}^R$.

We now formulate our result, stating that secure two-enc-two-dec combiners do not exist:

**Theorem 5.** No secure two-enc-two-dec AEAD combiner exists (neither synchronized nor reversed). More precisely, for any $x \in \{S,R\}$ and any set of algorithms $\alpha, \beta, \gamma, \phi, \pi, \rho$ for Figure 8 there exists a pair $(\text{AE}_0, \text{AE}_1)$ of AEAD schemes, one of which secure, and an adversary $A$ that breaks the combined scheme $\text{CB}^x(\text{AE}_0, \text{AE}_1) = (\text{enc}^x, \text{dec}^x)$ with high probability.

The theorem follows as a corollary from Lemmas 2 and 3, which handle the synchronized and reversed case separately.
Lemma 2 (Synchronized case). For any algorithms \( \alpha, \beta, \gamma, \varphi, \pi, \rho \) there exist a secure AEAD scheme \( \text{AE}_0 \), an (insecure) AEAD scheme \( \text{AE}_1 \), and an adversary \( \mathcal{A} \), such that \( \mathcal{A} \) breaks the integrity of the combined scheme \( \text{CB}^S(\text{AE}_0, \text{AE}_1) \) with high probability.

Proof. Let \( \text{AE}, \text{AE}' \) be secure AEAD schemes, and derive the schemes \( \text{AE}^{00}, \text{AE}^{11}, \text{AE}^{07}, \text{AE}^{17} \) from \( \text{AE}' \) as specified in Figure 9. Note that \( \text{AE}^{00} \) and \( \text{AE}^{11} \) provide authenticity, while ciphertexts of \( \text{AE}^{07} \) and \( \text{AE}^{17} \) are forgeable by flipping a single bit.

Figure 9: Schemes \( \text{AE}^{00}, \text{AE}^{11}, \text{AE}^{07}, \text{AE}^{17} \), all parameterized with a secure AEAD scheme \( \text{enc}', \text{dec}' \).

For arbitrarily picked \( (n, ad, m) \), consider an encryption \( c \leftarrow \text{CB}.\text{enc}(n, ad, m) \) followed by a decryption \( m \leftarrow \text{CB}.\text{dec}(n, ad, c) \), where the combiner \( \text{CB} := \text{CB}^S(\text{AE}_0, \text{AE}_1) \) is operated with components \( \text{AE}_0 = \text{AE} \) and either (a) \( \text{AE}_1 = \text{AE}^{00} \) or (b) \( \text{AE}_1 = \text{AE}^{11} \). As the difference between the two cases becomes visible to \( \text{CB}.\text{enc} \) not before line 04 of Figure 8, the values of \( n_0, ad_0, m_0, c_0 \) from line 02 are independent of the case. Further, the values \( n_0, ad_0, c_0, m_0 \) from line 09 will coincide with those of line 02, as otherwise the
the integrity of the combined scheme and of the combiner as hard as for any outside adversary. Consequently, crafting a different valid ciphertext is for the combiner as hard as for any outside adversary.

Lemma 3 (Reversed case). For any algorithms $\alpha, \beta, \gamma, \varphi, \pi, \rho$ there exist a secure AEAD scheme $\mathcal{AE}_0$, an (insecure) AEAD scheme $\mathcal{AE}_1$, and an adversary $A$, such that $A$ breaks the integrity of the combined scheme $CB^R(\mathcal{AE}_0, \mathcal{AE}_1)$ with high probability.

Proof. Let $\mathcal{AE}$ be a secure AEAD scheme and $M$ a strongly unforgeable MAC, and derive the schemes $\mathcal{AE}^{mt00}, \mathcal{AE}^{mt11}, \mathcal{AE}^{mt07}, \mathcal{AE}^{mt17}$ from $M$ as specified in Figure 10. Note that $\mathcal{AE}^{mt00}$ and $\mathcal{AE}^{mt11}$ provide authenticity, while ciphertexts of $\mathcal{AE}^{mt07}$ and $\mathcal{AE}^{mt17}$ are forgeable by flipping the last bit of any authentic ciphertext.

Figure 10: Schemes $\mathcal{AE}^{mt00}, \mathcal{AE}^{mt11}, \mathcal{AE}^{mt07}, \mathcal{AE}^{mt17}$, all parameterized with a strongly unforgeable MAC scheme $M$. Note that algorithms $\text{dec}^{mt07}$ and $\text{dec}^{mt17}$ are identical.

For arbitrarily picked $(n, ad, m)$, consider an encryption $c \leftarrow CB.\text{enc}(n, ad, m)$ followed by a decryption $m \leftarrow CB.\text{dec}(n, ad, c)$, where the combiner $CB := CB^R(\mathcal{AE}_0, \mathcal{AE}_1)$ is operated with components $\mathcal{AE}_0 = \mathcal{AE}$ and either (a) $\mathcal{AE}_1 = \mathcal{AE}^{mt00}$ or (b) $\mathcal{AE}_1 = \mathcal{AE}^{mt11}$.

\footnote{We note that neither of the combiner's algorithms has access to either of the schemes' symmetric key. Furthermore, the combiner has no state that stores information (e.g., ciphertexts) beyond one execution of combined encryption or decryption respectively. Consequently, crafting a different valid ciphertext is for the combiner as hard as for any outside adversary.}
The values \( n_0, ad_0, c_0, m_0 \) from line 28 in Figure 8 will coincide with those of line 18, as otherwise the combiner would, with noticeable probability, either abort in line 29 or present a forgery for \( AE_0 \), contradicting either the correctness of \( CB \) or the unforgeability of \( AE_0 \). Similarly the values \( n_1, ad_1, c_1, m_1 \) from line 25 will coincide with those of line 20, as otherwise the combiner would, with noticeable probability, either abort in line 26 or present a forgery for \( AE_1 \), contradicting either the correctness of \( CB \) or the unforgeability of \( AE_1 \). We show that values \( st_1, c_1 \) from line 21 are publicly recoverable: Recover \( st_0, c_1 \) from \( \varphi, n, ad, c \) as in line 24, recover \( m_1 \) from \( c_1 \) by exploiting that \( AE_1 \)-ciphertexts encode the message in the clear, recover \( c_0 \) from \( \pi, st_0, m_1 \) as in line 27, recover \( st_0 \) from \( \alpha, n, ad, m \) as in line 17, finally recover \( st_1 \) from \( \beta, st_0, c_0 \) as in line 19.

Consider the adversary that poses an encryption query \( Enc(n, ad, m) \), recovers \( st_1, c_1 \) as just described, derives \( c_1' \) from \( c_1 \) by flipping its last bit, then computes \( c_1' \leftarrow \gamma(st_1, c_1') \) as in line 21, and finally poses a decryption query \( Dec(n, ad, c) \).

Consider finally the two additional cases \((a') AE_1 = AE_{mt0} \) and \((b') AE_1 = AE_{mt1} \), i.e., the instantiation of the \( AE_1 \) component almost as above, the difference being that the decryption algorithms tolerate bit flips. As the invocation of \( \beta \) in line 19 is independent of the case we are in (hence \( st_1 \) is independent of the cases), the above observation that the values \( n_1, ad_1 \) from lines 20 and 25 are identical continues to hold in all of these cases. If \( c_1 \) was generated in case \((a') \), \( c_1' \) looks for \( \gamma \) as in cases \((b) \) or \((b') \) and thus \( c_1' \) looks for algorithms \( \varphi, \pi, \) and \( \rho \) as in cases \((b) \) or \((b') \) as well (and vice versa if \( c_1 \) was generated in case \((b') \)). Observing that the decryption algorithms \( dec_{mt0} \) and \( dec_{mt1} \) coincide, the value \( m_1 \) recovered in line 25 in the Dec query of adversary \( \mathcal{A} \) is independent of the case, in particular will be processed as in \((a) \) and \((b) \) and thus accepted. That is, adversary \( \mathcal{A} \) delivered a successful forgery \( c_1' \).

\[ \square \]

**Acknowledgments**

We thank Jeroen Pijnenburg for early discussions on the topic and the reviewers of ToSC for their helpful suggestions for improving this article. The research of Poettering was supported by the European Union’s Horizon 2020 project FutureTPM (779391) and the research of Rösler was supported by the research training group “Human Centered Systems Security” sponsored by the state of North Rhine-Westphalia, Germany.

**References**


Combiners for AEAD


