Context-Committing Security of Leveled Leakage-Resilient AEAD

Chandranan Dhar\textsuperscript{1}, Jordan Ethan\textsuperscript{2}, Ravindra Jejurikar\textsuperscript{3}, Mustafa Khairallah\textsuperscript{4}, Eik List\textsuperscript{5} and Sougata Mandal\textsuperscript{6,7}

\textsuperscript{1} Indian Statistical Institute, Kolkata, India  
\texttt{chandranandhar(at)gmail.com}
\textsuperscript{2} CISPA Helmholtz Center for Information Security, Saarbrücken, Germany  
\texttt{jordan.ethan(at)cispa.de}
\textsuperscript{3} Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE  
\texttt{Ravindra.Jejurikar(at)tii.ae}
\textsuperscript{4} Dept. of Electrical and Information Technology, Lund University, Lund, Sweden  
\texttt{khairallah(at)ieee.org}
\textsuperscript{5} Nanyang Technological University, Singapore, Singapore  
\texttt{elist(at)posteo.de}
\textsuperscript{6} Institute for Advancing Intelligence, TCG CREST, Kolkata, India  
\texttt{sougata.mandal(at)tcgcrest.org}

\textbf{Abstract.} During recent years, research on authenticated encryption has been thriving through two highly active and practically motivated research directions: provable leakage resilience and key- or context-commitment security. However, the intersection of both fields had been overlooked until very recently. In ToSC 1/2024, Struck and Weishäupl studied generic compositions of encryption schemes and message authentication codes for building committing leakage-resilient schemes. They showed that, in general, Encrypt-then-MAC (EtM) and MAC-then-Encrypt (MtE) are not committing while Encrypt-and-MAC (EaM) is, under plausible and weak assumptions on the components. However, real-world schemes are rarely strict black-box constructions. Instead, while various leakage-resilient schemes follow blueprints inspired by generic compositions, they often tweak them for security or efficiency. In this paper, we study two blueprints, the first one based on EtM for one of the strongest possible levels of leakage resilience. The second one is a single-pass framework based on leveled implementations. We show that, with a careful selection of the underlying primitives such as with identical encryption and authentication keys and a collision-resistant PRF as the MAC, these blueprints are committing. Our results do not contradict the results by Struck and Weishäupl since we pose more, but practically-motivated, requirements on the components. We demonstrate the practical relevance of our results by showing that our results on those blueprints allow us to easily derive proofs that several state-of-the-art leakage-resilient schemes are indeed committing, including TEDT and its descendants TEDT2 and Romulus-T, as well as the single-pass scheme Triplex.

\textbf{Keywords:} Authenticated encryption · provable security · leakage resilience · committing encryption · PRF · authentication · tweakable block cipher

\section{Introduction}

Authenticated Encryption with Associated Data (AEAD) has become a fundamental component in modern security applications, providing both confidentiality and authenticity.
The development of efficient AEAD schemes has resulted in widespread constructions like AES-GCM [SCM08], Ascon [DEMS21], Decoys [JNPS21], and AES-GCM-SIV [GLL19] that address diverse security goals including but not limited to Nonce-based AEAD (nAE) [Rog04], Misuse-Resistant AEAD (MRAE) [RS06], or Deterministic AEAD (DAE) [RS06].

However, as AEAD schemes and their analyses mature, attackers continuously seek new ways to exploit their security. Additionally, new applications introduce fresh security challenges. Consequently, two areas of research have gained prominence:

1. **Leakage-resilient AEAD**: This area focuses on security notions and schemes where the adversary can observe different forms of auxiliary leakage that may depend on sensitive secret information. The objective is to construct schemes that maintain confidentiality and authenticity even in the presence of certain leakage.

2. **Context-committing AEAD**: This area addresses scenarios where the adversary has access to, and can manipulate secret keys. For example, it deals with situations where the ciphertext allows for correct decryption under multiple contexts, where a context consists of the key $K$, the nonce $N$, and associated data $A$.

**Leakage-resilient AEAD.** This area of research has blossomed for almost two decades. In this work, we focus on recent developments, and on the schemes discussed by Bellizia et al. in [BBC+20] in particular. Therein, the authors categorized modern leakage-resilient AEAD schemes into four grades, with a focus on so-called leveled implementations. In such schemes, a few functions are assumed to be either leak-free or heavily protected, while the rest of the construction can leak a lot of information. In this work, we will focus on two relevant types of schemes:

- **Grade-3 schemes**: These schemes usually follow the pattern of Encrypt-then-MAC (EtM), using a hash function and two calls to a heavily protected Tweakable Block Cipher (TBC) implementation. They target Ciphertext Integrity with Misuse and Decryption Leakage (CIML2) security and indistinguishability against Chosen-Ciphertext Adversaries with misuse resilience and decryption Leakage (CCAmL2) security. Examples of schemes in this category are TEDT [BGP+20] and ISAP [DEM+17].

- **Grade-2 schemes**: These schemes usually employ a single-pass AEAD scheme, a hash function, and two heavily protected TBC calls. They target CIML2 security and indistinguishability against Chosen-Ciphertext Adversaries with misuse resilience and encryption Leakage (CCAmL1) security. An example is Triplex [SPS+22].

Because they cover many practical schemes, those two grades serve as the basis for the blueprints we study in this paper.

**Context-Committing AEAD.** In recent years, a series of attacks such as the Facebook message-franking attack [DGRW18], and the partitioning-oracle attack [LGR21] have shown vulnerabilities in the usage of conventionally secure AEAD schemes. Those works shared a common root cause: the existence of ciphertexts that can be decrypted correctly under multiple keys, which was out of the scope of conventional AEAD security but is necessary for security in the respective uses in practice.

To address this gap, Bellare and Hoang introduced commitment security in [BH22], which requires each ciphertext to commit to the key (CMT-1) or to the entire context (CMT-4) that produced it. Among the notions Bellare and Hoang proposed, CMT-4 represents the strongest and therefore most desirable form for designers. It is formalized through the following game. Given an AEAD scheme $\Pi$ with an encryption function $\mathcal{E}$, an adversary has the task of providing two contexts, i.e. tuples $(K, N, A, M)$ and $(K', N', A', M')$, consisting of a key, nonce, associated data, and message each. The adversary wins the game if the
contexts differ, i.e. \((K, N, A, M) \neq (K', N', A', M')\) but they both encrypt to the same ciphertexts: \(\Pi.E(K, N, A, M) = \Pi.E(K', N', A', M')\).

**Connecting Both Areas.** At first glance, the overlap between leakage-resilient and context-committing AEAD is unclear as there has been little exploration of their potential synergies. With their recent work, Struck and Weishäupl [SW24] began to shed light on relations in investigating the generic compositions of Encryption and Message Authentication Code (MAC) schemes to develop schemes that are both leakage-resilient and committing. Their study revealed that EtM and MAC-then-Encrypt (MtE) are not committing in general. They also demonstrated that Encrypt-and-MAC (EaM) can achieve committing properties under weak assumptions on the underlying schemes. Additionally, they presented a transformation that converts an AEAD scheme into a leakage-resilient and context-committing scheme. In a separate work, Krämer, Struck and Weishäupl [KSW23] have shown that the Grade-3 scheme ISAP is committing.

**Contribution.** While black-box compositions such as EtM, EaM, or MtE are valuable for studying generic constructions and inspiring instantiations, real-world schemes often deviate from them. In particular, many leakage-resilient schemes are based on blueprints that take inspiration from generic compositions but incorporate small changes tailored to specific security goals or higher efficiency. In this paper, we explore two such blueprints. The first blueprint is based on EtM and aims to achieve the highest level of leakage resilience. The second blueprint targets leveled single-pass implementations. We demonstrate that, with a careful selection of underlying primitives, both blueprints can be committing.

While our findings on the first blueprint may seem to contradict the negative result in [SW24] on EtM, two differences in the underlying assumptions help clarify. Firstly, in [SW24], the authors considered a black-box composition where the encryption function and the MAC use independent keys, whereas we require a strict dependency between both. Secondly, our result requires a certain type of MAC in the scheme, namely a collision-resistant Pseudo-Random Function (PRF).

Those additional requirements are not impractical. Our result on EtM generalizes [FOR17, Theorem 3] and [GLR17, Theorem 3], where the authors demonstrated similar restrictions on keys and MACs. The results on both blueprints allow us to easily derive that several leakage-resilient schemes are committing, including TEDT and its descendants TEDT2 and Romulus-T, as well as the single-pass scheme Triplex.

For schemes that follow our blueprints, showing their commitment security reduces to showing the collision resistance of their building blocks. For this purpose, we study the collision resistance of several leakage-resilient MACs used in EtM-based schemes, including Hash-then-BC (HBC), Hash-then-TBC (HTBC), and LRMAC1. For single-pass schemes, we examine instead the collision resistance of more components, including their functions for Key Derivation (KDF), Encryption (Enc), and Tag Generation (TGF).

Our analysis poses a few cryptographic assumptions on the used components. For keyed primitives, we operate in the ideal-cipher model, which is unavoidable in the chosen-key setting of committing security. For hash functions and compression functions, we require either collision and everywhere-preimage resistance, or collision resistance only. For LRMAC1, which requires only collision resistance, this matches the assumption on the hash function in the original MAC proof. For HBC, we require collision and everywhere-preimage resistance, which is still more concrete than the random-oracle model used in the original proof. For HTBC, we require collision and everywhere-preimage resistance, while the MAC proof requires collision and range-oriented preimage resistance. While our assumptions are slightly stronger, they are close to practice, as everywhere-preimage resistance can be seen as a worst-case analysis of range-oriented preimage resistance and is therefore, expected to lead to a similar bound for any secure standard hash function.
2 Preliminaries

In this section, we define some necessary security notions of functions in general and hash functions in particular, e.g., collision resistance, preimage resistance, and right collision resistance. Thereupon, we recall the definitions for the primitives we need for authenticated encryption.

General Notation. For a set $\mathcal{X}$, we write $X \overset{\$}{\leftarrow} \mathcal{X}$ to denote that a value $X$ is sampled uniformly at random from $\mathcal{X}$ and independent from other values. An adversary $A$ is a computationally bounded algorithm that shall win a security game against a challenger. We call $A$ $t$-bounded if it runs in time at most $t$. We indicate that $A$ outputs $X$ by $A \Rightarrow X$. W.l.o.g., we assume that adversaries never ask pointless queries, i.e., queries to which they can compute the answers themselves. In the following, we will introduce standard primitives and security notions. Throughout this section, we will denote non-empty sets and spaces by calligraphic uppercase variables and use $K$ (or $K_h$), $\mathcal{M}$, $\mathcal{C}$, $\mathcal{X}$, as spaces for keys, plaintexts, ciphertexts, and hash values, respectively.

2.1 Security Notions for Keyed Hash Functions

Collision Resistance (CR). Let $H : \mathcal{K}_h \times \mathcal{M} \rightarrow \mathcal{X}$ be a hash function and $K_h \overset{\$}{\leftarrow} \mathcal{K}_h$. $H$ is called $(\epsilon_{cr}, t)$-collision-resistant (CR) if for every $t$-bounded adversary $A$, the probability that $A(K_h)$ outputs a pair of distinct values $(M_0, M_1) \in \mathcal{M}^2$, such that $M_0 \neq M_1$ and $H_{K_h}(M_0) = H_{K_h}(M_1)$ is bounded by $\epsilon_{cr}$:

$$\Pr \left[ K_h \overset{\$}{\leftarrow} \mathcal{K}_h, A(K_h) \Rightarrow (M_0, M_1) \in \mathcal{M}^2 \text{ s.t. } M_0 \neq M_1, H_{K_h}(M_0) = H_{K_h}(M_1) \right] \leq \epsilon_{cr}.$$ 

Right Collision Resistance (RCR). Let $\mathcal{X}_l \times \mathcal{X}_r$ be nonempty sets of spaces $\mathcal{X}_l$ and $\mathcal{X}_r$. Let $H : \mathcal{K}_h \times \mathcal{M} \rightarrow \mathcal{X}_l \times \mathcal{X}_r$ be a hash function and $K_h \overset{\$}{\leftarrow} \mathcal{K}_h$. $H$ is called $(\epsilon_{rcr}, t)$-right collision-resistant (RCR) if for every $t$-bounded adversary $A$, the probability that $A(K_h)$ outputs a pair of distinct values $(M_0, M_1) \in \mathcal{M}^2$, such that $(X_0, Y_0) = H_{K_h}(M_0), (X_1, Y_1) = H_{K_h}(M_1), Y_0 = Y_1$, and $M_0 \neq M_1$, is bounded by $\epsilon_{rcr}$:

$$\Pr \left[ K_h \overset{\$}{\leftarrow} \mathcal{K}_h, A(K_h) \Rightarrow (M_0, M_1) \in \mathcal{M}^2 \text{ s.t. } M_0 \neq M_1, (X_0, Y_0) = H_{K_h}(M_0), (X_1, Y_1) = H_{K_h}(M_1), Y_0 = Y_1 \right] \leq \epsilon_{rcr}.$$ 

We can define Left Collision Resistance (LCR) analogously. In the following, we extend the definition to a hash function with multiple inputs, where the collision resistance property holds for a subset of the inputs.

Collision Resistance on a Subset of the Inputs (Partial CR). Let $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n$ denote nonempty sets or spaces and define $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2 \times \cdots \times \mathcal{M}_n$. Let $H : \mathcal{K}_h \times \mathcal{M} \rightarrow \mathcal{X}$ be a hash-function and $K_h \overset{\$}{\leftarrow} \mathcal{K}_h$. For a positive integer $i \in \{1, \ldots, n\}$, $H$ is called $(\epsilon_{cr}, t)$-($\mathcal{M}_1, \ldots, \mathcal{M}_i, \ldots, \mathcal{M}_n$)-collision-resistant, if the probability of finding a hash collision on two distinct messages $M = (M_1, \ldots, M_n), M' = (M'_1, \ldots, M'_n) \in \mathcal{M}^2$ s.t. $(M_1, \ldots, M_i) \neq (M'_1, \ldots, M'_i)$ is bounded by $\epsilon_{cr}$:

$$\Pr \left[ K_h \overset{\$}{\leftarrow} \mathcal{K}_h, A(K_h) \Rightarrow (M_1, \ldots, M_n), (M'_1, \ldots, M'_n) \in \mathcal{M}^2, \right.$$

$$\left. \text{s.t. } (M_1, \ldots, M_i) \neq (M'_1, \ldots, M'_i), H_{K_h}(M_1, \ldots, M_n) = H_{K_h}(M'_1, \ldots, M'_n) \right] \leq \epsilon_{cr}.$$
Note that if $i < n$, then $(M_{i+1}, \ldots, M_n)$ and $(M'_{i+1}, \ldots, M'_n)$ may or may not be equal. If $i = n$, the definition is equivalent to standard collision resistance. In general, a function can be collision-resistant on any subset of the inputs, and the inputs are explicitly given in the collision-resistance property. We will call a hash function “partial right collision-resistant” (partial RCR) if it achieves right collision resistance on a subset of inputs.

**Everywhere Preimage Resistance.** Let $H : K_h \times M \to X$ be a hash function and $K_h \leftarrow \$ K_h$. $H$ is called $(\epsilon_{\text{epre}}, t)$-everywhere-preimage-resistant ($\text{epre}$) if for every $t$-bounded adversary $A$,

$$\max_{X \in X} \left\{ \Pr \left[ K_h \leftarrow \$ K_h, A(K_h) \Rightarrow M, \text{ s.t. } H_{K_h}(M) = X \right] \right\} \leq \epsilon_{\text{epre}}.$$

### 2.2 Primitives

**Tweakable Block Cipher (TBC).** A TBC is a mapping $\tilde{E} : K \times T_w \times \{0,1\}^n \to \{0,1\}^n$ such that for any choice of $K \in K$ and $T_w \in T_w$, $\tilde{E}(K, T_w, \cdot)$ is a permutation over $\{0,1\}^n$. If $T_w = \emptyset$, then $E : K \times \{0,1\}^n \to \{0,1\}^n$ is a Block Cipher (BC). We will sometimes write $\tilde{E}_K(X)$ and $E_K(X)$ for $\tilde{E}(K, T, X)$ and $E(K, X)$, respectively. In this paper, we will analyze constructions in the ideal-cipher model, where $\tilde{E}$ or $E$ will be selected randomly from the set of all possible cipher families with the same domain and range.

**Pseudo-random Function (PRF) and Pseudo-Random Number Generator (PRNG).**

A PRF is a deterministic mapping $F : K \times X \to Y$. Let $\text{Func}(X, Y)$ be the set of all functions with domain $X$ and range $Y$. In the PRF game, a challenger samples $K \leftarrow \$ K$ and $\rho \leftarrow \text{Func}(X, Y)$ and provides an adversary $A$ with access to either $F_K$ or $\rho$. The PRF advantage of $A$ on $F_K$ is defined as

$$\text{Adv}_{F_K}^\text{PRF}(A) = |\Pr[A^{F_K} \Rightarrow 1] - \Pr[A^{\rho} \Rightarrow 1]|.$$

We call $F$ an $(\epsilon_{\text{PRF}}, t)$-secure PRF if for all $t$-bounded adversaries $A$, $\text{Adv}_{F_K}^\text{PRF}(A) \leq \epsilon_{\text{PRF}}$.

A PRNG is a deterministic mapping $G : \{0,1\}^k \times N \to Y$ with $Y \subseteq \{0,1\}^*$ that takes an input $K \in \{0,1\}^k$ and a positive integer $\ell$ as inputs and outputs $Y \in \{0,1\}^{k+\ell}$. In the PRNG game, a challenger samples $K \leftarrow \$ K$ and $\rho \leftarrow \text{Func}(K \times N, Y)$, and, on input of a length $\ell$, outputs either $G(K, \ell)$ or $\rho(K, \ell)$. Then, the PRNG advantage of an adversary $A$ against $G$ is defined as

$$\text{Adv}_{G}^\text{PRNG}(A) = |\Pr[A^{G} \Rightarrow 1] - \Pr[A^{\rho} \Rightarrow 1]|.$$

We call $G$ an $(\epsilon_{\text{PRNG}}, t)$-secure PRNG if for all $t$-bounded adversaries $A$, it holds that $\text{Adv}_{G}^\text{PRNG}(A) \leq \epsilon_{\text{PRNG}}$. Later, we will use a generalization with multiple output-length parameters $\ell_1, \ell_2$ where $Y = \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2}$ and so on.

**Hash-function-based Message Authentication Codes (MACs).** Let $\text{MAC} : K_h \times K \times M \to T$ be a keyed function that transforms an input $M \in M$ to a tag $T \in T$. Let $\text{Ver}_{\text{MAC}} : K_h \times K \times M \times T \to \{\bot, \top\}$ be the verification function that takes a message $M \in M$ and a would-be tag $T \in T$ and returns $\top$ if $\text{MAC}_{s,K} (M) = T$ and $\bot$ otherwise. In other contexts, security notions such as unforgeability and/or pseudo-randomness are needed, but in the context of this paper, we are interested only in collision resistance, which we define for hash-function-based MACs as follows.
Collision Resistance for Hash-function-based MACs. Let $K_h \leftarrow K_h$. A MAC is called $(\epsilon_{\text{maccr}}, t)$-collision-resistant (MAC-CR) if for every $t$-bounded adversary $A$, the probability that $\mathcal{A}(K_1)$ outputs a pair of distinct inputs $(K_0, M_0), (K_1, M_1) \in (K \times M)^2$, such that $	ext{MAC}_{K_0, K_1}(M_0) = \text{MAC}_{K_0, K_1}(M_1)$ and $(K_0, M_0) \neq (K_1, M_1)$, is bounded by $\epsilon_{\text{maccr}}$:

$$
\Pr \left[ K_h \leftarrow K_h, \mathcal{A}(K_h) \Rightarrow ((K_0, M_0), (K_1, M_1)) \in (K \times M)^2 \\
\text{s. t. } (K_0, M_0) \neq (K_1, M_1), \text{MAC}_{K_0, K_1}(M_0) = \text{MAC}_{K_0, K_1}(M_1) \right] \leq \epsilon_{\text{maccr}}.
$$

In all collision games in the remainder, we will drop the hash key $K_h$ that is released to the adversary and assume that it is given to the adversary at the beginning of the game.

Authenticated Encryption. A nonce-based Authenticated Encryption scheme supporting Associated Data (nAEAD) is a pair of functions $\Pi = (\mathcal{E}, \mathcal{D})$ with associated sets $K, N, A, M, C$, denoting the key space, nonce space, associated data space, message space, and ciphertext space, respectively. The elements of $\mathcal{C}$ comprise of a pair $(C, T)$, with $T \in \{0, 1\}^\sigma$. The encryption algorithm and decryption algorithms $\mathcal{E}$ and $\mathcal{D}$ are deterministic functions input and $D : K \times N \times A \times C \rightarrow M \cup \{\bot\}$, where the special symbol $\bot$ indicates that $(C, T)$ was deemed invalid. We sometimes write $\mathcal{E}_{K, A}^N(M)$ and $\mathcal{D}_{K, A}^N(C, T)$ to denote $\mathcal{E}(K, N, A, M)$ and $D(K, N, A, (C, T))$. For all correct schemes, encryption is injective from $M$ to $\mathcal{C}$ under fixed $K, N, A$. The scheme is correct if $\mathcal{D}_{K, A}^N(\mathcal{E}_{K, A}^N(M)) = M$ for all $K, N, A, M$ and tidy if $M = \mathcal{D}_{K, A}^N(C, T)$ and $M \neq \bot$, then $\mathcal{E}_{K, A}^N(M) = (C, T)$ for all $K, N, A, C, T$. All AEAD schemes considered in this work are assumed to be correct and tidy.

CMT-4 Security. The two prevalent notions of committing security in the literature are

- CMT-1 security: A commitment to only the key $K$.
- CMT-4 security: A commitment to the complete context $(K, N, A, M)$.

Since we consider only CMT-4 security, we define it more formally here. Note that Bellare and Hoang [BH22] demonstrated that incorporating the message $M$ into the context is unnecessary, as committing to $(K, N, A)$ is equivalent to committing to $(K, N, A, M)$.

In the CMT-4 game against an AEAD scheme $\Pi$, an adversary $\mathcal{A}$ outputs $(K_1, N_1, A_1, M_1)$ and $(K_2, N_2, A_2, M_2); \mathcal{A}$ wins if and only if $(K_1, N_1, A_1, M_1) \neq (K_2, N_2, A_2, M_2)$ and $\Pi.\text{Enc}(K_1, N_1, A_1, M_1) = \Pi.\text{Enc}(K_2, N_2, A_2, M_2)$. We write $\text{Adv}_{\text{CMT4}}(\mathcal{A})$ to denote the probability that $\mathcal{A}$ wins the CMT-4 game where $\mathcal{A}$ has access to the ideal primitives and hash keys used by $\Pi$.

3 Blueprints for Leakage Resilience and their Motivation as Committing Schemes

In this section, we describe a paradigm for designing leakage-resilient schemes based on so-called leveled implementations. In this paradigm, different parts of the scheme have different assumptions on how they are implemented and the associated leakage functions. Since our focus is on the relation to context commitment, we study only integrity and Ciphertext Integrity with Misuse and Leakage with decryption leakage (CIML2). We will also consider a widespread leakage model wherein the adversary can receive unlimited leakage, most of the scheme is unprotected, and only the protected parts are assumed to be leak-free.
3.1 The EtM-based Blueprint

The first blueprint we look at is based on EtM but tailored to leakage resilience. It is close to the FGHF′ construction by Degabriele et al. [DJS19], which itself is an instance of N2 [NRS14]. In the following, let \( K_e, K_m, N, A, M, C, IV, FV, \) and \( T \) be nonempty sets or spaces for encryption keys, MAC keys, nonces, associated data, plaintexts, ciphertexts, initial values, forward values, and tags, respectively. A leveled leakage-resilient EtM scheme requires two leak-free fixed-input-length primitives:

1. A key-derivation function \( KDF : K_e \times N \rightarrow IV \), which takes the nonce and the encryption key and generates an initial value for the encryption phase.
2. A tag-generation function \( TGF : K_m \times FV \rightarrow T \), which takes the MAC key and a fixed-length hash of the ciphertext, nonce, and associated data, and generates the verification tag using a PRF.

The scheme also uses an encryption scheme \( Enc : K \times IV \times M \rightarrow C \) and a collision-resistant hash function \( Hash : N \times A \times C \rightarrow FV \). However, these two primitives are assumed to have unlimited leakage when considering CIML2 security. The high-level blueprint is depicted in Figure 1 and the encryption of EtM|KDF, Enc, Hash, TGF|(\( K, N, A, M \)) under \( K = (K_e, K_m) \) is defined as

\[
IV \leftarrow KDF(K_e, N), \quad C \leftarrow Enc(IV, A, M), \quad FV \leftarrow Hash(N, A, C), \quad T \leftarrow TGF(K_m, FV).
\]

We observe three important properties. First, since the MAC, consisting of Hash and TGF, follows the Hash-then-PRF paradigm, it already binds the triplet \( (N, A, C) \) to any given key \( K_m \). However, \( K_e \) is not part of the binding. Second, if the two parts of the key \( K_e \) and \( K_m \) are independent, the adversary can fix \( (K_m, C, T, N, A) \) and find two pairs \( (K_{e1}, M_1) \) and \( (K_{e2}, M_2) \) to break the commitment. This implies that even if the keys are dependent, we must ensure that the EtM scheme commits to \( (K_e, K_m) \) and the MAC is collision-resistant. In Section 4, we shall show that under these restrictions, EtM is indeed context-committing. Moreover, we shall show that three of the prominent leakage-resilient Hash-then-PRF MACs are indeed collision-resistant PRFs. Two of these MACs will require a stronger assumption on the hash function, where the hash function resists not only collision but also preimage attacks, while all three require a stronger assumption on the TGF, as the analysis has to be conducted in the ideal-cipher model. However, we will show that the KDF does not affect the committing security.

**Figure 1:** The EtM blueprint for leakage-resilient context-committing nAEAD. The gray components are assumed to be strongly protected.
3.2 The Single-pass Blueprint KET

The second blueprint we will consider is used for single-pass schemes. Similar to EtM, the scheme includes leak-free KDF and TGF functions and an encryption function Enc with unlimited leakage. The encryption function is responsible for generating both the ciphertext $C$ as well as the hash value $FV$. This blueprint $\Pi[\text{KDF, Enc, TGF}]$ denoted as KET is depicted in Figure 2 and its encryption of $(N, A, M)$ under a key tuple $(K_e, K_m)$ is defined as follows:

$$ IV \leftarrow \text{KDF}(K_e, N), \quad (C, FV) \leftarrow \text{Enc}(IV, A, M), \quad T \leftarrow \text{TGF}(K_m, FV). $$

We can observe some requirements on the components. CIML2 security requires that the TGF is collision-resistant for a given key $K$. Similarly as EtM, this means that the scheme commits to $(N, A, M)$ for $K$. Similarly as for EtM, further issues arise when considering the keys. If the TGF is not collision-resistant, then we can find $K_{m_1} \neq K_{m_2}$ such that $T_1 = T_2$ for the same $(N, A, M)$. The commitment will break if $K_m$ is independent of $K_e$. However, if $K_m$ depends on $K_e$, the success of the attack depends on the properties of the KDF and the interaction between the KDF and the Enc function. Alternatively, it may be possible to relax the requirements on the KDF if the TGF is collision-resistant.

4 CMT-4 Security of EtM-based AEAD Schemes

The first blueprint we will study concerns EtM-type constructions with a MAC that follows the Hash-then-PRF design. This paradigm is used widely in leveled leakage-resilient schemes, including TEDT [BGP+20], TEDT2 [Lis21], Romulus-T [IKMP20], and ISAP [DEM+17]. Definition 1 describes the generalized EtM construction, including generating the encryption and MAC keys from a master key $K$. Therein, we abstract away some internal details. We aggregate the functions KDF and Enc into a function $\text{Enc'}$ and similarly, wrap Hash and TGF in a function MAC.

**Definition 1.** Let $\Pi[\text{KeyGen, Enc, Mac}]$ be a nonce-based AEAD scheme such that

$$(K_e, K_m) \leftarrow \text{KeyGen}(K), \quad C \leftarrow \text{Enc}(K_e, N, M), \quad T \leftarrow \text{Mac}(K_m, N, A, C).$$

Then, we call $\Pi$ an EtM scheme.

In [SW24], the EtM (or N2 [NRS14]) scheme is shown to be not context-committing in general. We show that the EtM scheme is nevertheless CMT-4-secure when KeyGen is right collision-resistant (which precludes independent keys $K_e$ and $K_m$) and MAC is collision-resistant. Similar results were already shown for complete robustness (CROB) and binding security. Thus, Theorem 1 is adapted from [FOR17, Theorem 3] and [GLR17, Theorem 3].
Theorem 1. Let II[KeyGen, Enc, MAC] be an EtM scheme such that KeyGen is \((\epsilon_k, t_1)\)-right collision-resistant and MAC is \((\epsilon_{maccr}, t_2)\)-collision-resistant for some \(t_1 = O(t)\) and \(t_2 = O(t)\). Then, for any \(t\)-bounded CMT-4 adversary \(\mathcal{A}\) against II, it holds that

\[
\text{Adv}^\text{cmt4}_{\Pi}(\mathcal{A}) \leq \epsilon_{maccr} + \epsilon_k.
\]

Proof. Suppose an adversary \(\mathcal{A}\) outputs challenge values \((K_1, N_1, A_1, M_1)\) and \((K_2, N_2, A_2, M_2)\) with corresponding ciphertexts \((C_1, T_1)\) and \((C_2, T_2)\). We bound the probability that \((C_1, T_1) = (C_2, T_2) = (C, T)\). We define a sequence of hybrid games \(G_0\) through \(G_2\) as follows, where we introduce Boolean variables \(E_i\), for \(i \in \{0, 1, 2\}\) such that \(E_i\) is true if and only if the adversary wins in Game \(G_i\).

**Game \(G_0\).** This is the original cmt4 game in the real world.

**Game \(G_1\).** Game \(G_1\) is almost identical to Game \(G_0\) but adds the aspect that \(G_1\) terminates if \(K_{m_1} = K_{m_2} \land K_1 \neq K_2\). The probability of this event is at most

\[
|\Pr[E_0] - \Pr[E_1]| \leq \epsilon_k.
\]

**Game \(G_2\).** Game \(G_2\) is almost identical to \(G_1\) except that \(G_2\) also terminates if \((N_1, A_1, K_1) = (N_2, A_2, K_2)\) and \(M_1 \neq M_2\). Since this is impossible from the assumption that the encryption scheme is correct and tidy, it follows that

\[
|\Pr[E_1] - \Pr[E_2]| = 0.
\]

Finally, the adversary wins Game \(G_2\) if it is successful with \((K_{m_1}, N_1, A_1) \neq (K_{m_1}, N_2, A_2)\), \(K_{m_1} = K_{m_2} \iff K_1 = K_2^1\) and \(\text{Mac}(K_{m_1}, N_1, A_1, C) = \text{Mac}(K_{m_2}, N_2, A_2, C)\). This can happen only if there is a collision against the MAC given none of the previous conditions occurs. As a result, we can upper bound the probability by

\[
\Pr[E_2] \leq \epsilon_{maccr}.
\]

To sum up,

\[
\text{Adv}^\text{cmt4}_{\Pi}(\mathcal{A}) = \Pr[E_0] \leq \left(\sum_{i=1}^{2} |\Pr[E_{i-1}] - \Pr[E_i]|\right) + \Pr[E_2] \leq \epsilon_{maccr} + \epsilon_k,
\]

which yields our claim in Theorem 1.

---

\(^1\)Two-way implication: \(K_1 = K_2 \implies K_{m_1} = K_{m_2} \land K_{m_1} = K_{m_2} \implies K_1 = K_2\)
Theorem 2. Let \( \text{MAC} \) be relevant as it offers useful leakage resilience. It follows that \( \text{AEAD} \) is computed as \( T \leftarrow E(K_m, H_{K_h}(M)) \).

First, we define the collision-resistance game as follows. The adversary \( A \) gets the hash-function key \( K_h \) at the beginning of the game. From here on, we drop all further occurrences of hash-function keys and will proceed similarly in all following games. \( A \) asks \( q_e \) chosen-key queries to the ideal-cipher oracle \( E \) and obtains the corresponding outputs. If a query \((K_i, X_i)\) is in forward direction, \( A \) obtains \( Y_i \leftarrow E(K_i, X_i) \); if a query \((K_i, Y_i)\) is in backward direction, it obtains \( X_i \leftarrow E^{-1}(K_i, Y_i) \). At the end of its interactions, \( A \) outputs two pairs \((K_{m_1}, M_1)\) and \((K_{m_2}, M_2)\) and wins if and only if \( \text{HBC}[H, E](K_{m_1}, M_1) = \text{HBC}[H, E](K_{m_2}, M_2) \).

**Theorem 2.** Let \( E : \mathbb{K}_m \times \{0,1\}^n \rightarrow \{0,1\}^n \) be an ideal cipher and \( H : \mathcal{M} \rightarrow \{0,1\}^n \) be a \((\epsilon_{cr}, t_1)\)-collision-resistant and \((\epsilon_{epre}, t_2)\)-everywhere-preimage-resistant hash function. Then for any adversary \( A \) that runs in time \( t \) and makes \( q_e \leq 2^{-n/2} \) queries to the ideal cipher, such that \( t_1 = O(t + q_e) \) and \( t_2 = O(t + q_e) \), \( \text{HBC}[H, E] \) is \((\epsilon, t)\)-collision-resistant for

\[
\epsilon \leq q_e \epsilon_{epre} + \epsilon_{cr} + \frac{2q_e^2 + 1}{2n}.
\]

**Proof.** Suppose \( A \) outputs \((K_{m_1}, M_1)\) and \((K_{m_2}, M_2)\) such that \( \text{HBC}[H, E](K_{m_1}, M_1) = \text{HBC}[H, E](K_{m_2}, M_2) \). We define a sequence of hybrid games as follows: Let \( \mathcal{E}_i \) be the event that the adversary wins in Game \( G_i \) for \( i \in \{0, \ldots, 3\} \).

**Game \( G_0 \).** The real-world game.

**Game \( G_1 \).** Game \( G_1 \) is almost identical to Game \( G_0 \) but terminates if one of the following events happens during the ideal-cipher queries of \( A \).

- Two forward queries with different keys produce the same output. The probability of this event is upper bounded by \( \left( \frac{q_e}{2n} \right) / (2^n - q_e) \leq q_e^2 / 2^n \).

- A backward query with input \( T \) is followed by a forward query with output \( T \) with a different key. The probability of this event is at most \( q_e^2 / 2^n \).

It follows that

\[
| \Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1] | \leq \frac{2q_e^2}{2^n}.
\]
Game $G_2$. Game $G_2$ is almost identical to $G_1$ except that $G_2$ terminates if $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. The probability of this event is at most

$$\left| \Pr[E_1] - \Pr[E_2] \right| \leq \epsilon_{cr}.$$ 

Game $G_3$. We define that Game $G_3$ keeps a set $\mathcal{X} = \{ X_i : i \in [q_e] \}$, where the values $X_i \leftarrow E^{-1}(K, Y_i)$ represent the responses of backward ideal-cipher queries with key $K$ and input $Y_i$. Game $G_3$ is almost identical to $G_2$ except that $G_3$ terminates also if $H(M_1) \in \mathcal{X}$ or $H(M_2) \in \mathcal{X}$. Then, from the definition of everywhere-pre-image resistance, we have

$$\left| \Pr[E_2] - \Pr[E_3] \right| \leq q_e \epsilon_{epre}.$$ 

Finally, we study the probability that $A$ wins in Game $G_3$. Then, one of the following cases must have occurred.

- Case 1: $K_{m_1} = K_{m_2}$. This case implies that $M_1 \neq M_2$. If $H(M_1) = H(M_2)$, there exists an adversary against the collision resistance of the hash function $H$. Otherwise, if $H(M_1) \neq H(M_2)$, a collision of the tags $T_1 = T_2$ is impossible since $E$ is a permutation for the same key $K_m$. This case cannot happen: if a hash collision existed, the game would terminate.

- Case 2: $K_{m_1} \neq K_{m_2}$. In this case, a collision can happen only if $E(K_{m_1}, H(M_1)) = E(K_{m_2}, H(M_2))$. Note that $H(M_1) \notin \mathcal{X}$ and $H(M_2) \notin \mathcal{X}$ by assumption. Thus, a collision can happen only randomly with a probability of

$$\Pr[E_3] = \Pr[E(K_{m_1}, H(M_1)) = E(K_{m_2}, H(M_2))] = 1/2^n.$$ 

Our result follows from the sum of the individual bounds. \hfill \Box

5.2 Collision Resistance of Hash-then-TBC (HTBC)

The MAC HTBC [BGP+19] is defined as follows. Let $H : \mathcal{M} \rightarrow \{0,1\}^n \times \{0,1\}^r$ be a hash function and $\tilde{E} : \mathcal{K}_m \times \{0,1\}^r \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a TBC. Then, for a given message $M$ and keys $K_m \in \mathcal{K}_m$, HTBC[$H, \tilde{E}$]$_{K_m}$ computes a tag $T$ as

$$T \leftarrow \tilde{E}(K_m, W, V) \quad \text{where} \quad (V, W) \leftarrow H(M) .$$

We define the collision-resistance game similarly to that for HBC.

Theorem 3. Let $\tilde{E} : \mathcal{K}_m \times \{0,1\}^r \times \{0,1\}^n \rightarrow \{0,1\}^n$ be an ideal cipher and $H : \mathcal{M} \rightarrow \{0,1\}^r \times \{0,1\}^n$ be a $(\epsilon_{cr}, t_1)$-collision-resistant and $(\epsilon_{epre}, t_2)$-everywhere-preimage-resistant hash function. Then, for any adversary $A$ that runs in time $t$ and makes $q_e \leq 2^{n-1}$ queries to the ideal cipher, such that $t_1 = O(t + q_e)$ and $t_2 = O(t + q_e)$, HTBC[$H, \tilde{E}$] is $(\epsilon, t)$-collision-resistant for

$$\epsilon \leq q_e \epsilon_{epre} + \epsilon_{cr} + \frac{2q_e^2 + 1}{2^n} .$$

Proof. Suppose $A$ outputs $(K_{m_1}, M_1)$ and $(K_{m_2}, M_2)$ such that HTBC[$H, \tilde{E}$]$_{K_{m_1}}(K_{m_2}, M_1) = HTBC[H, \tilde{E}](K_{m_2}, M_2)$. Again, we define a sequence of hybrid games $G_0$ through $G_3$ and define $E_i$ as the event that the adversary wins in game $G_i$.

Game $G_0$. This is the real-world game.
Game $G_1$. Game $G_1$ differs from $G_0$ in the fact that it terminates if one of the following events happens during the ideal-cipher queries.

- Two forward queries with different keys produce the same output. This probability is bounded by $q_c^2/2^n$.

- A backward query with input $T$ is followed by a forward query with output $T$ with a different key. This probability is also bounded by $q_c^2/2^n$.

We obtain

$$\left| \Pr[E_0] - \Pr[E_1] \right| \leq \frac{2q_c^2}{2^n}.$$ 

Game $G_2$. Game $G_2$ is almost identical to $G_1$ but adds the fact that it terminates if $M_1 \neq M_2$ and $H(M_1) = H(M_2)$. The probability of this event can be bounded by

$$\left| \Pr[E_1] - \Pr[E_2] \right| \leq \epsilon_{cr}.$$ 

Game $G_3$. We adopt the definition of the set of backward-query responses $X$ from Game $G_3$ of the proof of HBC. Besides it, Game $G_3$ adds to $G_2$ only the fact that $G_3$ also terminates if $H(M_1) \in X$ or $H(M_2) \in X$. From the definition of everywhere-pre-image resistance, we obtain

$$\left| \Pr[E_2] - \Pr[E_3] \right| \leq q_c \epsilon_{epre}.$$ 

Finally, we study the probability that $A$ wins in Game $G_3$. Similar to Theorem 2, the adversary cannot win if $(K_{m_1}, W_1) = (K_{m_2}, W_2)$. However, if $K_{m_1} \neq K_{m_2}$, a collision can happen if $\tilde{E}(K_{m_1}, W_1, V_1) = \tilde{E}(K_{m_2}, W_2, V_2)$. For this event, we have to consider two mutually exclusive cases that cover all possibilities as follows.

- Case 1: $M_1 = M_2$. In this case, we have $H(M_1) = H(M_2) = (V, W)$. Thus, the adversary will be successful if it can find two keys $K_{m_1}, K_{m_2}$ such that $\tilde{E}(K_{m_1}, W, V) = \tilde{E}(K_{m_2}, W, V)$. This is impossible since the game would terminate as defined in either $G_1$ or $G_3$.

- Case 2: $M_1 \neq M_2$. If $H(M_1) = H(M_2)$, the game would terminate as defined in $G_2$. Otherwise, a collision can happen only if $\tilde{E}(K_{m_1}, W_1, V_1) = \tilde{E}(K_{m_2}, W_2, V_2)$. If these two queries had appeared in any ideal-cipher queries, the conditions that allowed this collision to occur would have led the game to terminate.

If $K_{m_1} = K_{m_2}$ and $W_1 \neq W_2$, then $H(M_1) = H(M_2)$ and $M_1 = M_2$ are impossible, but the analysis of the case when $M_1 \neq M_2$ is the same. This means that $\tilde{E}(K_{m_1}, W_1, V_1) = \tilde{E}(K_{m_2}, W_2, V_2)$ holds but at least one of these queries must have not appeared in any ideal-cipher query, as the game would have terminated otherwise. If none of the above happens, then a collision can happen only randomly with probability at most

$$\Pr[E_3] = \Pr[\tilde{E}(K_{m_1}, W_1, V_1) = \tilde{E}(K_{m_2}, W_2, V_2)] \leq \frac{1}{2^n}.$$ 

Our claim in Theorem 3 follows from adding $E_3$ to the transition differences. \qed
5.3 Collision Resistance of TEDT Variants

**TEDT.** The authentication part of the original TEDT [BGP+20] (depicted in Figure 3) and Romulus-T [IKMP20] follow exactly our HTBC format. Therein, the hash function $H$ is based on Hirose’s compression function and Merkle-Damgård strengthening, which outputs a $2n$-bit value $V \parallel W$. Note that for any tuple of key and nonce, the adversary can choose a suitable message to achieve any desirable ciphertext. Thus, finding $(K_1, U_1)$ and $(K_2, U_2)$, where $U_i \leftarrow \text{pad}(N_i, A_i, C_i, PK)$ and $PK$ denotes the public key for multi-user security, that lead to the same tag $T$ is equivalent to breaking CMT-4 security.

**TEDT2.** The authentication function of TEDT2 [Lis21] (depicted in Figure 4) also follows our HTBC format, except for the fact that $8 \parallel N \parallel W$ is used as a tweak in the final TBC call. Let $N_1$ and $N_2$ be two nonces corresponding to the same $(C,T)$ output. Then, we will have two cases:

- **Case 1:** $N_1 = N_2$. Then, the analysis is exactly the same as in Theorem 3.
- **Case 2:** $N_1 \neq N_2$. In this case, $N$ can be seen as part of the hash output. Thus, in this case, the commitment can be broken only by finding a collision in the ideal-cipher queries. Then, we consider two subcases depending on ideal-cipher queries concerning the $T$-producing TBC call:
  - Both queries are forward ideal-cipher queries: Here, the adversary will be successful only if it can find two different tweaks producing the same tag. The success probability is upper bounded by $\frac{q_e^2}{2^n}$.
  - At least one of the queries is a backward ideal-cipher query: In this case, the success probability can be upper bounded by $\epsilon_{\text{pre}}$.

Thus, the analysis is the same as for HTBC with a hash function $H' (N, A, C) = N \parallel H(A, C)$.

5.4 Collision Resistance of LRMAC1

The MAC LRMAC1 [BGPS21] is defined as follows. Let $H : \mathcal{M} \rightarrow \{0,1\}^\tau \times \{0,1\}^n$ be a hash function and $\tilde{E} : K_m \times \{0,1\}^\tau \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a TBC. Given $K_m \in K_m$ and a message $M \in \mathcal{M}$, $\text{LRMAC1}[H, \tilde{E}]$ computes the authentication tag as

$$T \leftarrow \tilde{E}(K_m, V, 0^n) \quad \text{where} \quad V \leftarrow H(M).$$

We define the collision-resistance game similarly as in the case of HBC.

**Theorem 4.** Let $\tilde{E} : K_m \times \{0,1\}^\tau \times \{0,1\}^n \rightarrow \{0,1\}^n$ be an ideal cipher and $H : \mathcal{M} \rightarrow \{0,1\}^\tau \times \{0,1\}^n$ be a $(\epsilon_{\alpha}, t_1)$-collision-resistant hash function. Then, for any adversary $A$ that runs in time $t$ and makes $q_e \leq 2n^{-1}$ queries to the ideal cipher, such that $t_1 = O(t + q_e)$, $\text{LRMAC1}[H, \tilde{E}]$ is $(\epsilon, t)$-collision-resistant for

$$\epsilon \leq \epsilon_{\alpha} + \frac{q_e^2 + 2q_e + 5}{2^n}.$$
Figure 4: High-level structure of TEDT2.

Proof. Suppose $A$ outputs $(K_{m_1}, M_1)$ and $(K_{m_2}, M_2)$ such that \( \text{LRMAC}_1[H, \tilde{E}](K_{m_1}, M_1) = \text{LRMAC}_1[H, \tilde{E}](K_{m_2}, M_2) \). Again, we will define a sequence of hybrid games and use $E_i$ as the event that the adversary wins in game $G_i$.

Game $G_0$. The real-world game.

Game $G_1$. The game terminates if one of the following events happens during the ideal-cipher queries.

- Two forward queries with different keys produce the same output. This probability is bounded by $q_n^2/2^n$.
- A backward query with input $T$ outputs $0^n$. This probability is bounded by $2q_e/2^n$.

It follows that
\[
| \Pr[E_0] - \Pr[E_1] | \leq q_n^2 + 2q_e/2^n.
\]

Game $G_2$. Game $G_2$ is almost identical to $G_1$ but adds the fact that $G_2$ will terminate if $M_1 \neq M_2$ and $H(M_1) = V_1 = V_2 = H(M_2)$. The probability of this event is bounded by
\[
| \Pr[E_1] - \Pr[E_2] | \leq \epsilon_{cr}.
\]

Finally, we study the probability that $A$ wins in $G_2$. We have to consider only the case that $V_1 \neq V_2$ as $V_1 = V_2$ would lead the game to terminate.

- Case 1: $(K_1, V_1, 0^n, T)$ appeared in an ideal-cipher query. Then,
  \[
  \Pr[\tilde{E}(K_2, V_2, 0^n) = T] \leq \frac{1}{2^n - q_2} \leq \frac{2}{2^n}.
  \]

- Case 2: $(K_2, V_2, 0^n, T)$ appeared in an ideal-cipher query. Then,
  \[
  \Pr[\tilde{E}(K_1, V_1, 0^n) = T] \leq \frac{1}{2^n - q_1} \leq \frac{2}{2^n}.
  \]

- Case 3: neither TBC call appeared in any ideal-cipher query. Then,
  \[
  \Pr[\tilde{E}(K_1, V_1, 0^n) = \tilde{E}(K_2, V_2, 0^n)] \leq \frac{1}{2^n}.
  \]

Thus, $\Pr[E_3] \leq 5/2^n$. The bound in Theorem 4 follows from adding it to all transition probabilities.

Increasing the tag size and bit-security level. In all considered MACs, the security is bounded by half of the tag size. One way around this limitation is to use a Double-Block-Length (DBL) construction for the TGF. For instance, the TGF of LRMAC1 can be replaced by $\tilde{E}(K, H(M), 0^n) || \tilde{E}(K, H(M), 1^n)$, that is Hirose’s DBL compression function with an initial value of $0^n$ [Hir06]. The construction is still invertible and compatible with CIML2 security. Similar standard constructions can be found for HBC and HTBC.
Table 2: Different variants of KET and the requirements on their components for CMT-4 security. (R)CR = (right) collision resistance.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>KeyGen</th>
<th>KDF</th>
<th>Enc</th>
<th>TGF</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>KET-1</td>
<td>-</td>
<td>CR</td>
<td>RCR</td>
<td>CR</td>
<td>Theorem 5</td>
</tr>
<tr>
<td>KET-1a</td>
<td>LCR</td>
<td>CR</td>
<td>RCR</td>
<td>partial CR</td>
<td>Theorem 6</td>
</tr>
<tr>
<td>KET-2</td>
<td>RCR</td>
<td>-</td>
<td>RCR</td>
<td>CR</td>
<td>Theorem 7</td>
</tr>
<tr>
<td>KET-2a</td>
<td>RCR</td>
<td>CR</td>
<td>partial RCR</td>
<td>CR</td>
<td>Theorem 8</td>
</tr>
</tbody>
</table>

\section{CMT-4 Security of Single-pass Leveled Schemes}

In this section, we study the second blueprint KET from Figure 2. We call this blueprint KET as a short-hand for its three components: a KDF, an Enc function, and a TGF. KET can be seen as the paradigm underlying single-pass leveled leakage-resilient schemes such as Triplex \cite{SPS22} or Multiplex \cite{PSS24}.

In this section, we establish three goals. First, we show that the KET composition is CMT-4-secure when each component satisfies a specific set of collision-resistance properties. Second, we show that it can fulfill the compact commitment, wherein verifying the tag suffices to verify the commitment. Finally, we show that if the keys used in the first and last components are identical (or generated by KeyGen having specific CR properties), we can relax the collision-resistance requirements for certain components.

\subsection{CMT-4 Security of the Generic KET scheme}

We begin with the generic KET scheme wherein the keys in the KDF and the TGF are independent, i.e. no constraints are imposed on their keys. For such schemes, we demonstrate that achieving CMT-4 security requires collision resistance in all three components, KDF, Enc, and TGF, with the minor relaxation that we require only right collision resistance for Enc, i.e. collision resistance for the part of its outputs that are used in the TGF.

\begin{definition}
Let II[KeyGen, KDF, Enc, TGF] be a nonce-based AEAD scheme. If, for a given key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, associated data $A \in \mathcal{A}$, and a message $M \in \mathcal{M}$, it encrypts $M$ to a ciphertext $(C, T)$ as
\[
(K_c, K_m) \leftarrow \text{KeyGen}(K) \quad IV \leftarrow \text{KDF}(K_c, N),
(C, FV) \leftarrow \text{Enc}(IV, A, M), \quad T \leftarrow \text{TGF}(K_m, FV),
\]
then, we call II a KET-1 scheme.
\end{definition}

We will study four relevant variants of this scheme which differ in their assumptions posed on their individual components. Table 2 summarizes their properties.

\begin{theorem}
Let II[KeyGen, KDF, Enc, TGF] be a KET-1 scheme such that
\begin{itemize}
    \item the KDF is $(\epsilon_{\text{KDF}}, t_1)$-collision-resistant,
    \item Enc is $(\epsilon_{\text{Enc}}, t_2)$-right collision-resistant, and
    \item the TGF is $(\epsilon_{\text{TGF}}, t_3)$-collision-resistant
\end{itemize}
for some $t_1 = O(t)$, $t_2 = O(t)$, and $t_3 = O(t)$. Then, for any $t$-bounded CMT-4 adversary $\mathcal{A}$ against II it holds that
\[
\text{Adv}_{\text{II}}^{\text{CMT4}}(\mathcal{A}) \leq \epsilon_{\text{KDF}} + \epsilon_{\text{Enc}} + \epsilon_{\text{TGF}}.
\]
Proof. Since there is no restriction on KeyGen inputs and outputs, the CMT-4 security for the context \((K, N, A, M)\) follows from the CMT-4 security of the context \((K_m, K_e, N, A, M)\). Suppose an adversary \(\mathcal{A}\) outputs challenge values \((N_1, A_1, K_1, M_1)\) and \((N_2, A_2, K_2, M_2)\) with corresponding ciphertexts \((C_1, T_1)\) and \((C_2, T_2)\). We upper bound the probability that \((C_1, T_1) = (C_2, T_2) = (C, T)\). We consider the following disjoint cases that cover all possibilities.

Case 1: \(K_{m_1} \neq K_{m_2}\). In this case, there must be a collision against the TGF.

Case 2: \(K_{m_1} = K_{m_2}, \ (A_1, M_1) \neq (A_2, M_2)\). Then, we consider the following subcases.

- Case 2a: \(FV_1 \neq FV_2\). Then, there is a collision against the TGF.
- Case 2b: \(FV_1 = FV_2\). In this case, there is a right collision against the Enc function.

Case 3: \(K_{m_1} = K_{m_2}, \ (A_1, M_1) = (A_2, M_2), \ (K_e_1, N_1) \neq (K_e_2, N_2)\). Again, we study two subcases.

- Case 3a: \(FV_1 \neq FV_2\). Then, there is a collision against the TGF.
- Case 3b: \(FV_1 = FV_2, IV_1 \neq IV_2\). Then, there is a right-output collision against the Enc function.
- Case 3c: \(FV_1 = FV_2, IV_1 = IV_2\). Then, there is a collision against the KDF.

For each of the cases above, the advantage of the adversary is bounded by the collision resistance property of the individual components, as given in Equation 1. \(\square\)

### 6.2 CMT-4 Security of the KET-1a scheme

Theorem 5 does not require any collision resistance property for KeyGen and holds even when the keys \(K_e\) and \(K_m\) are independent. However, if KeyGen is left-collision-resistant, we can lift the requirement of full i.e. \((FV, K_m)\)-collision resistance from the TGF. Instead, left collision resistance on the values \(FV\) will suffice, as captured by the following theorem.

**Theorem 6.** Let II[KeyGen, KDF, Enc, TGF] be a KET-1a scheme such that

- KeyGen is \((\epsilon_k, t_1)\)-left collision-resistant,
- the KDF is \((\epsilon_kdf, t_2)\)-collision-resistant,
- Enc is \((\epsilon_enc, t_3)\)-right collision-resistant, and
- the TGF is \((\epsilon_tgf, t_4)\)-FV-collision-resistant (partial CR only on input \(FV\) but not on input \(K_m\)).

for some \(t_1 = O(t), t_2 = O(t), t_3 = O(t),\) and \(t_4 = O(t)\). Then, for any \(t\)-bounded CMT-4 adversary \(\mathcal{A}\) against II, it holds that

\[
\text{Adv}_{\text{cm4}}^{\text{cmt4}}(\mathcal{A}) \leq \epsilon_{kdf} + \epsilon_{enc} + \epsilon_{tgf} + \epsilon_k.
\]  

**Proof.** Suppose an adversary \(\mathcal{A}\) outputs challenge values \((N_1, A_1, K_1, M_1)\) and \((N_2, A_2, K_2, M_2)\) with corresponding ciphertexts \((C_1, T_1)\) and \((C_2, T_2)\). We upper bound the probability that \((C_1, T_1) = (C_2, T_2) = (C, T)\), where we have to consider the following disjoint cases.
Case 1: \((A_1, M_1) \neq (A_2, M_2)\). We have to study two subcases.

- Case 1a: \(FV_1 \neq FV_2\). Then, there is a collision against the TGF.
- Case 1b: \(FV_1 = FV_2\). Then, there is a right collision against Enc.

Case 2: \((A_1, M_1) = (A_2, M_2), (K_1, N_1) \neq (K_2, N_2)\). Since \(\text{KeyGen}\) is left collision-resistant, the probability of \(K_1 \neq K_2 \land K_{e_2} = K_{e_2}\) is bounded by \(\epsilon_k\). Accounting for \(\epsilon_k\) by a standard hybrid argument, we can safely assume \(K_1 \neq K_2\) and therefore \(K_{e_1} \neq K_{e_2}\) in the remainder. Thus, this case reduces to \((K_{e_1}, N_1) \neq (K_{e_2}, N_2)\).

- Case 2a: \(FV_1 \neq FV_2\). Then, there is a collision against the TGF.
- Case 2b: \(FV_1 = FV_2, IV_1 \neq IV_2\). Then, there is a right collision against the Enc.
- Case 2c: \(FV_1 = FV_2, IV_1 = IV_2\). Then, there is a collision against the KDF, as \((K_{e_1}, N_1) \neq (K_{e_2}, N_2)\).

For each of the cases above, the advantage of the adversary is bounded by the collision resistance property of its respective three components, as given in Equation 2.

Next, we consider variants of \(\text{KET}\) that use the nonce as an additional input of the encryption function. For those variants, collision resistance of the KDF is not necessary. This is intuitive since we can view the next scheme as \(\text{KET-1}\) where \(N\) is appended to the output of the KDF.

**Definition 3.** Let II[\(\text{KeyGen, KDF, Enc, TGF}\)] be a nonce-based AEAD scheme. If, for a given key \(K \in \mathcal{K}\), a nonce \(N \in \mathcal{N}\), associated data \(A \in \mathcal{A}\), II encrypts a message \(M \in \mathcal{M}\) to a ciphertext \((C, T)\) as

\[
\begin{align*}
(K_e, K_m) & \leftarrow \text{KeyGen}(K) \\
IV & \leftarrow \text{KDF}(K_e, N), \\
(C, FV) & \leftarrow \text{Enc}(IV, N, A, M), \\
T & \leftarrow \text{TGF}(K_m, FV),
\end{align*}
\]

then, we call II an \(\text{KET-2}\) scheme.

**Theorem 7.** Let II[\(\text{KeyGen, KDF, Enc, TGF}\)] be an \(\text{KET-2}\) scheme such that

- the \(\text{KeyGen}\) function is \((\epsilon_k, t_1)\)-right collision-resistant,
- and \(\text{Enc}\) is \((\epsilon'_\text{enc}, t_2)\)-right collision-resistant, and
- the \(\text{TGF}\) is \((\epsilon_{\text{tgf}}, t_3)\)-collision-resistant

for \(t_1 = O(t), t_2 = O(t)\) and \(t_3 = O(t)\). Then, for any adversary \(A\) running in time at most \(t\) against the CMT-4 security of II, it holds that

\[
\text{Adv}_{\text{cmt4}}^\text{II}(A) \leq \epsilon'_\text{enc} + \epsilon_{\text{tgf}} + \epsilon_k.
\]

**Proof.** Suppose \(A\) outputs challenge values \((N_1, A_1, K_1, M_1)\) and \((N_2, A_2, K_2, M_2)\) with corresponding ciphertexts \((C_1, T_1)\) and \((C_2, T_2)\). We bound the probability that \((C_1, T_1) = (C_2, T_2) = (C, T)\). We consider the following disjoint cases.

**Case 1: \(K_1 \neq K_2\).** Here, we have the following subcases.

- Case 1a: \(K_m = K_m\). Then, there is a right collision on \(K_m\) against the KeyGen function.
- Case 1b: \(K_m \neq K_m\). Then, there is a collision against the TGF.
Case 2: $K_1 = K_2$, $(N_1, A_1, M_1) \neq (N_2, A_2, M_2)$. Again, we have two subcases.

- Case 2a: $FV_1 \neq FV_2$. Then, there is a collision against the TGF.
- Case 2b: $FV_1 = FV_2$. Then, there is a right-output collision against $Enc$.

For each of the cases above, the advantage of the adversary is bounded by the collision resistance property of the three components, as given in Equation 3.

Finally, we consider a special case of KET-2 that we call KET-2a, where Enc is only collision-resistant when $IV$, $A$, or $C$ change, i.e., it may be easy to find $(IV, A, C, N_1)$ and $(IV, A, C, N_2)$ such that $FV_1 = FV_2$. However, if $(IV_1, A_1) \neq (IV_2, A_2)$, then collisions are hard to find. The following theorem demonstrates that, despite this restrictive assumption on the collision resistance of $Enc$, we can still attain CMT-4 security by imposing a milder condition. In this case, it is essential to also assume that KDF is collision-resistant.

Theorem 8. Let $II[\text{KeyGen}, \text{KDF}, \text{Enc}, \text{TGF}]$ be a KET-2a scheme such that

- the KeyGen function is $(\epsilon_k, t_1)$-right collision-resistant,
- the KDF is $(\epsilon_{kdf}, t_2)$-collision-resistant,
- Enc is $(\epsilon_{enc}, t_3)$-($IV, A$)-right collision-resistant i.e. Enc is RCR only on input $(IV, A)$, and
- the TGF is $(\epsilon_{tgf}, t_4)$-collision-resistant.

for $t_1 = O(t)$, $t_2 = O(t)$, $t_3 = O(t)$, and $t_4 = O(t)$. Then, for any adversary $A$ running in time at most $t$ against the CMT-4 security of $II$, it holds that

$$\text{Adv}_{\text{Enc}}^{\text{CMT-4}}(A) \leq \epsilon_{kdf} + \epsilon_{enc} + \epsilon_{tgf} + \epsilon_k. \quad (4)$$

Proof. Suppose an adversary $A$ outputs challenge values $(N_1, A_1, K_1, M_1)$ and $(N_2, A_2, K_2, M_2)$ with corresponding ciphertexts $(C_1, T_1)$ and $(C_2, T_2)$. We bound the probability that $(C_1, T_1) = (C_2, T_2) = (C, T)$ with the following cases.

Case 1: $K_1 \neq K_2$. Here, we have the following two subcases.

- Case 1a: $K_{m_1} = K_{m_2}$. Then, there is a right-output collision against the KeyGen function, i.e. on $K_m$.
- Case 1b: $K_{m_1} \neq K_{m_2}$. Then, there is a collision against the TGF.

Case 2: $K_1 = K_2$, $(N_1, A_1, M_1) \neq (N_2, A_2, M_2)$.

- Case 2a: $FV_1 \neq FV_2$. Then, there is a collision against the TGF.
- Case 2b: $FV_1 = FV_2$.
  - If $IV_1 \neq IV_2$, there is a $(IV, A)$-right-output collision against the Enc function.
  - Otherwise, if $IV_1 = IV_2$ and $N_1 \neq N_2$ holds, there is collision against the KDF.
  - Finally, if $IV_1 = IV_2$ and $N_1 = N_2$ hold, we must have $A_1 \neq A_2$ by injectivity of Enc over the message space when the other parameters remain unchanged. $A_1 \neq A_2$ implies that there will be a collision against $(IV, A)$-right-output collision of Enc.

For each of the cases above, the advantage of the adversary is bounded by the collision resistance property of the four components, as given in Equation 4.
7 Triplex as an Instantiation of KET-2

In this section, we demonstrate the usefulness of the KET blueprint by showing that the recent single-pass scheme Triplex [SPS + 22] can be viewed as an instance of KET-2.

**Triplex.** Triplex operates with a KDF that consists of three TBCs, a protected call followed by two parallel calls to an unprotected TBC. The KDF takes a key $K = sk||pk$ — that combines a secret part $sk$ with a public part $pk$ for higher multi-user security — and a nonce $N$ and produces a 2n-bit output $IV = h_1||k_1$. The encryption function of Triplex takes various inputs including $pk$, $N$, $A$, $M$, and $IV = h_1||k_1$. It outputs a ciphertext $C$ along with $FV = V||W$. Its TGF is essentially a single TBC call. It takes $sk$ as the key, $V||W$ as the tweak, and a fixed input $0^n$ to generate a tag $T$. Note that both $Enc$ and KDF take $N$ as input and both the KDF and the TGF use the same key $sk$.

There are multiple ways to view Triplex, and each one leads to the application of a different theorem. We will view the CMT-4 security of Triplex as an application of Theorem 7. We can consider $pk$ as part of the nonce instead of the key since it is not utilized as a key anywhere. This simplification allows us to view Triplex as a specific instance of the generic KET-2 construction. According to Theorem 7, for achieving CMT-4 security, we need to demonstrate collision resistance of the TGF and right-output collision resistance of $Enc$.

**Corollary 1.** Let $II[KDF, Enc, TGF]$ denote Triplex. Then, there exists an $(\epsilon_{cr}, t_1)$-collision-resistant hash function $H$, such that for any adversary $A$ running in time at most $t$ against the CMT-4 security of Triplex, it holds that

$$\text{Adv}_{II}^{\text{cmt4}}(A) \leq \frac{q_e^2 + 2q_e + 5}{2^n} + \epsilon_{cr},$$

where $t_1 = O(t)$.

**Proof.** First, we will redefine the KDF function of Triplex. This is done by moving the two parallel TBC calls from out of the KDF into the $Enc$ function. We denote the modified KDF and $Enc$ functions as $KDF'$ and $Enc'$, respectively, as visualized in Figure 5. This
change does not affect the scheme’s security but only moves the boundary of where the KDF ends and $\text{Enc}$ begins. In this representation, KDF is not collision-resistant, and we apply Theorem 7. We know that $\epsilon_k = 0$ since $sk$ is used as both $K_e$ and $K_m$. Moreover, the collision resistance of the TGF is similar to that of the TGF used in LRMAC1. In other words, we obtain from the analysis of Theorem 4 that

$$\epsilon_{\text{tgf}} \leq q_e^2 + 2q_e + 5\frac{2^n}{n}.$$ 

What remains is to bound $\epsilon_{\text{enc}}$. Note that the function $\text{Enc}'$ can be visualized as shown in Figure 6, wherein the bottom part is the Triplex hash function of the input $\text{pad}(IV, N, pk, A, C)$ for some injective padding function. The top symmetric encryption (SE) component computes ciphertext $C$ being input to the hash function. Thus, if $N_1 = N_2$, the top part (SE) is bijective and $FV$-collision-resistant. If $N_1 \neq N_2$, it is still $FV$-collision-resistant since $N$ is part of the input to the hash function. Then,

$$\epsilon_{\text{enc}} \leq \epsilon_{\text{cr}}.$$ 

Finally, the hash function $H$ used in Triplex is the Merkle-Damgård with Permutation (MDP) hash function [HPY07] instantiated with Hir, Hirose’s double-block-length function [Hir06]. From the indifferentiability of this MDPH hash function, we have that $\epsilon_{\text{cr}}$ is negligible, which implies the commitment security of Triplex.

8 Conclusion

In this paper, we studied the CMT-4 security of two families of leveled leakage-resilient schemes: Grade-3 schemes based on EtM and single-pass Grade-2 schemes. In both cases, we give positive results. We show that EtM is committing as long as the keys satisfy a particular definition of dependence and the MAC is collision-resistant. We give positive results on the collision resistance of different leakage-resilient MACs: HBC, HTBC and LRMAC1, and apply this to show the CMT-4 security of TEDT. We also discuss how to increase the security by increasing the tag size. For single-pass schemes, we give different variants with different assumptions on their components and show that the recently proposed scheme, Triplex, achieves CMT-4 security up to half the tag size.

We believe our work shows an interesting connection between context commitment and leakage-resilient schemes. Even though the two security goals are different and not implied by each other, the underlying design principles allow for efficient schemes that achieve both goals.

An interesting future direction is to study how to design leakage-resilient schemes that are also committing beyond half the tag size. Another direction is to study if there is a connection that can be derived between CIML2 security and CMT-4 security.
Acknowledgments

We would like to thank Ling Song and Yaobin Shen for organizing the Asian Symmetric Workshop (ASK) 2023 in Guangzhou, China, where this work was initiated. Mustafa Khairallah is funded by the Wallenberg-NTU Postdoctoral Presidential Fellowship. Eik List has been supported by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – LI 4223/1-1.

References


