Tweaking Even-Mansour Ciphers

Benoît Cogliati[1], Rodolphe Lampe[1], and Yannick Seurin[2(✉)]

[1] University of Versailles, Versailles, France
benoitcogliati@hotmail.fr, rodolphe.lampe@gmail.com
[2] ANSSI, Paris, France
yannick.seurin@m4x.org

Abstract. We study how to construct efficient tweakable block ciphers in the Random Permutation model, where all parties have access to public random permutation oracles. We propose a construction that combines, more efficiently than by mere black-box composition, the CLRW construction (which turns a traditional block cipher into a tweakable block cipher) of Landecker *et al.* (CRYPTO 2012) and the iterated Even-Mansour construction (which turns a tuple of public permutations into a traditional block cipher) that has received considerable attention since the work of Bogdanov *et al.* (EUROCRYPT 2012). More concretely, we introduce the (one-round) *tweakable Even-Mansour* (TEM) cipher, constructed from a single n-bit permutation P and a uniform and almost XOR-universal family of hash functions (H_k) from some tweak space to $\{0,1\}^n$, and defined as $(k,t,x) \mapsto H_k(t) \oplus P(H_k(t) \oplus x)$, where k is the key, t is the tweak, and x is the n-bit message, as well as its generalization obtained by cascading r independently keyed rounds of this construction. Our main result is a security bound up to approximately $2^{2n/3}$ adversarial queries against adaptive chosen-plaintext and ciphertext distinguishers for the two-round TEM construction, using Patarin's H-coefficients technique. We also provide an analysis based on the coupling technique showing that asymptotically, as the number of rounds r grows, the security provided by the r-round TEM construction approaches the information-theoretic bound of 2^n adversarial queries.

Keywords: Tweakable block cipher · CLRW construction · Key-alternating cipher · Even-mansour construction · H-coefficients technique · Coupling technique

1 Introduction

Tweakable Block Ciphers. Tweakable block ciphers (TBCs for short) are a generalization of traditional block ciphers which, in addition to the usual inputs (message and cryptographic key), take an extra (potentially adversarially controlled) input for variability called a *tweak*. Hence, the signature of a tweakable

Y. Seurin—This author was partially supported by the French National Agency of Research through the BLOC project (contract ANR-11-INS-011).

R. Gennaro and M. Robshaw (Eds.): CRYPTO 2015, Part I, LNCS 9215, pp. 189–208, 2015.
DOI: 10.1007/978-3-662-47989-6_9

block cipher is $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{K}$ is the key space, $\mathcal{T}$ the tweak space, and $\mathcal{M}$ the message space. This primitive has been rigorously formalized by Liskov *et al.* [25], and has proved to be very useful to construct various higher level cryptographic schemes such as (tweakable) length-preserving encryption modes [17,18], online ciphers [2,34], message authentication codes [24,25], and authenticated encryption modes [25,32,33].

Tweakable block ciphers can be designed "from scratch" (e.g., the Hasty Pudding cipher [36], Mercy [10], or Threefish, the block cipher on which the Skein hash function [15] is based), however most of the proposed constructions are on top of an existing (traditional) block cipher, in a black-box fashion. In this latter family, constructions where changing the tweak implies to change the key of the underlying block cipher (e.g., Minematsu's construction [26]) tend to be avoided for efficiency reasons (re-keying a block cipher is often a costly operation). Hence, most of the existing proposals have the property that the key under which the underlying block cipher is called is tweak-independent. Of particular relevance to our work, the original Liskov *et al.*'s paper proposed the so-called LRW construction (sometimes called LRW2 in the literature since this was the second of two constructions suggested in [25]), based on a block cipher E with key space $\mathcal{K}_E$ and message space $\{0,1\}^n$ and an almost XOR-universal (AXU) family of hash functions $\mathcal{H} = (H_k)_{k \in \mathcal{K}_H}$ from some set $\mathcal{T}$ to $\{0,1\}^n$, and defined as

$$\mathsf{LRW}^E((k,k'),t,x) = H_{k'}(t) \oplus E_k(H_{k'}(t) \oplus x), \tag{1}$$

where $(k,k') \in \mathcal{K}_E \times \mathcal{K}_H$ is the key, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the message. This construction was proved secure in [25] up to the birthday bound, i.e., $2^{n/2}$ adversarial queries (assuming the underlying block cipher E is secure in the traditional sense, i.e., it is a strong pseudorandom permutation). This was later extended by Landecker *et al.* [24] who considered the cascade of two rounds of the LRW construction (with independent block cipher and hash function keys for each round), and proved it secure up to about $2^{2n/3}$ adversarial queries.[1] This was further generalized to longer cascades by Lampe and Seurin [23] who proved that the r-round Chained-LRW (CLRW) construction is secure up to roughly $2^{\frac{rn}{r+2}}$ adversarial queries (they also conjectured that the tight security bound is $2^{\frac{rn}{r+1}}$ queries).

The Iterated Even-Mansour Construction. The iterated Even-Mansour construction abstracts in a generic way the high-level structure of key-alternating ciphers [11]. Concretely, it defines a block cipher from a tuple of r public n-bit permutations $(P_1, \ldots, P_r)$, the ciphertext associated to some message $x \in \{0,1\}^n$ being computed as

$$y = k_r \oplus P_r(k_{r-1} \oplus P_{r-1}(\cdots P_2(k_1 \oplus P_1(k_0 \oplus x)) \cdots)),$$

where the n-bit round keys $k_0, \ldots, k_r$ are either independent or derived from a master key. This construction was extensively analyzed in the Random Permutation model, where the P_i's are modeled as public random permutation

[1] A flaw was subsequently found in the original proof of [24] and patched by Procter [31]. A different way of fixing the proof was proposed by Landecker *et al.*, see the revised version of [24].

oracles that the adversary can only query (bidirectionally) in a black-box way. This approach was originally taken for $r = 1$ round in the seminal paper of Even and Mansour [13], who showed that the block cipher encrypting x into $k_1 \oplus P(k_0 \oplus x)$ is secure up to $2^{n/2}$ adversarial queries.[2] Dunkelman *et al.* [12] subsequently remarked that the same security level is retained by the *single-key* one-round Even-Mansour cipher, i.e., when $k_0 = k_1$. An important step was later made by Bogdanov *et al.* [5], who showed that for $r = 2$ rounds, the construction ensures security up to roughly $2^{2n/3}$ adversarial queries. Bogdanov *et al.*'s paper triggered a spate of results improving the pseudorandomness bound as the number r of rounds grows [21,38], culminating with the proof by Chen and Steinberger [7] that the r-round iterated Even-Mansour construction with r-wise independent round keys ensures security up to about $2^{\frac{rn}{r+1}}$ adversarial queries (tightly matching a generic attack described in [5]). Note that a special case of r-wise independent round keys is obtained by cascading r single-key one-round Even-Mansour ciphers (with independent keys), viz.

$$E_{k_1,\ldots,k_r}(x) = k_r \oplus P_r(k_r \oplus k_{r-1} \oplus P_{r-1}(k_{r-1} \oplus \cdots \oplus k_1 \oplus P_1(k_1 \oplus x) \cdots)),$$

in which case the high-level similarity with the CLRW construction is obvious.

Besides pseudorandomness, the iterated Even-Mansour construction (with a sufficient number of rounds) has also been shown to achieve resistance to known-key attacks [3], related-key attacks [9,14], and chosen-key attacks [9], as well as indifferentiability from an ideal cipher [1,22].

Our Results. We consider the problem of constructing tweakable block ciphers directly from a tuple of public permutations rather than from a full-fledged block cipher. This was partially tackled by Cogliati and Seurin in [9]. They showed how to construct a TBC with n-bit keys and n-bit tweaks from three public n-bit permutations which is secure up to the birthday bound: denoting $E(k, x)$ the 3-round iterated Even-Mansour cipher with the trivial key schedule (i.e., all round keys are equal to the n-bit master key k), let $\widetilde{E}$ be the TBC defined as

$$\widetilde{E}(k, t, x) = E(k \oplus t, x). \tag{2}$$

Hence, $\widetilde{E}$ is simply the 3-round iterated Even-Mansour cipher with round keys replaced by $k \oplus t$. Cogliati and Seurin showed[3] that this TBC is provably secure up to $2^{n/2}$ adversarial queries in the Random Permutation Model (and that two rounds or less are insecure). The drawback of this simple construction is that any TBC of the form (2) with an underlying block cipher E of key-length κ can deliver at most $\kappa/2$ bits of security [4], so that there is no hope to improve

[2] When we talk about *adversarial queries* without being more specific in such a context where the attacker, in addition to the construction oracle, also has oracle access to the inner permutation(s), we mean indifferently construction and inner permutation queries.

[3] The focus of [9] is on xor-induced related-key attacks against the traditional iterated Even-Mansour cipher, but their result can be directly transposed to the TBC setting, see the full version of [9].

the number of queries that the construction can securely tolerate by merely increasing the number of rounds to four or more.

In this paper, we aim at getting a tweakable Even-Mansour-like construction with security *beyond the birthday bound*. The naive way of proceeding would be to instantiate the block cipher E in the CLRW construction with an iterated Even-Mansour cipher based on permutations $P_1, \ldots, P_r$. However, combining existing results for CLRW on one hand [23,24], and for the iterated Even-Mansour cipher on the other hand [7], one would need at least r^2 independent permutations to get provable $\mathcal{O}(2^{\frac{rn}{r+1}})$-security.[4] A more promising approach, that we take here, is to start with the construction obtained by combining the (one-round) LRW construction and the (one-round) Even-Mansour cipher, yielding what we dub the one-round *tweakable Even-Mansour* construction, defined from a single n-bit permutation P and an AXU family of hash functions $\mathcal{H}' = (H'_{k'})_{k' \in \mathcal{K}'}$ from some tweak space $\mathcal{T}$ to $\{0,1\}^n$ as

$$\mathsf{TEM}^P((k,k'),t,x) = H'_{k'}(t) \oplus k \oplus P(H'_{k'}(t) \oplus k \oplus x), \tag{3}$$

where $(k,k') \in \{0,1\}^n \times \mathcal{K}'$ is the key, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the message. Combining the security proofs for LRW [25] and for the one-round single-key Even-Mansour cipher [12,13] directly yields that this construction ensures security up to $2^{n/2}$ adversarial queries, in the Random Permutation model for P. For example, if we use the universal hash function family based on multiplication in the finite field $\mathbb{F}_{2^n}$, i.e., $H_{k'}(t) = k' \otimes t$, which is XOR-universal, one obtains a simple tweakable block cipher with $2n$-bit keys and n-bit tweaks which is secure up to the birthday bound.

Our first insight is to consider the slightly more general construction

$$\mathsf{TEM}^P(k,t,x) = H_k(t) \oplus P(H_k(t) \oplus x). \tag{4}$$

It is not too hard to show (as we do in Sect. 3.2) that this more general construction also ensures security up to $2^{n/2}$ adversarial queries, assuming that the hash function family $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$, in addition to being AXU, is also *uniform* (i.e., for any $t \in \mathcal{T}$ and any $y \in \{0,1\}^n$, the probability over $k \leftarrow_{\$} \mathcal{K}$ that $H_k(t) = y$ is equal to 2^{-n}).[5] This simple observation allows to save n bits of key material when using multiplication-based hashing, since $H_k(t) = k \otimes t$ is XOR-universal and uniform if one restricts the tweak space to $\mathbb{F}_{2^n} \setminus \{0\}$.

It is naturally tempting to consider cascading $r > 1$ rounds of construction (4) to obtain an hybrid of the iterated Even-Mansour cipher and the CLRW construction. Our main result is that the two-round construction

$$\mathsf{TEM}^{P_1,P_2}((k_1,k_2),t,x) = H_{k_2}(t) \oplus P_2(H_{k_2}(t) \oplus H_{k_1}(t) \oplus P_1(H_{k_1}(t) \oplus x))$$

[4] For $r > 2$, since the analysis of the CLRW construction in [23] is not tight, this is even worse.

[5] Construction (3) is obviously a special case of construction (4), since the hash function family defined by $H_{k,k'}(t) = H'_{k'}(t) \oplus k$, where $(H'_{k'})_{k' \in \mathcal{K}'}$ is AXU and $k \in \{0,1\}^n$, is AXU and uniform.

is secure (against adaptive chosen-plaintext and ciphertext attacks) up to approximately $2^{2n/3}$ adversarial queries (again, assuming that $\mathcal{H}$ is uniform and AXU).

To arrive at this result, we could have adapted the game-based proof of [24] for the two-round CLRW construction to accommodate the fact that in the TEM setting, the adversary has additionally oracle access to the inner permutations P_1 and P_2. Yet we preferred to use the H-coefficients technique [30], which was successfully applied to the analysis of the iterated Even-Mansour cipher [6,7], and adjust it to take into account the existence of the tweak in the TEM construction. Our choice was motivated by the fact that the H-coefficients-based security proof for the two-round Even-Mansour cipher is (in our opinion) simpler than the game-based proof for the two-round CLRW construction. Actually, our security proof for the two-round TEM construction can easily be simplified (by making the inner permutations secret, or, more formally, letting the number of queries q_p to the inner permutations be zero in our security bound as given by Theorem 2) to yield a new, H-coefficients-based proof of the security result of [24] for the two-round CLRW construction (our own bound matching Landecker *et al.*'s one [24] up to multiplicative constants).[6] It seems interesting to us that our proof entails a new and conceptually simpler (at least to us) proof of a previous result that turned out quite delicate to get right with game-based techniques [31]. We explain how to "extract" from our work a H-coefficients proof for the two-round CLRW construction in the full version of this paper [8].

We were unable to extend our H-coefficients security proof to $r > 2$ rounds.[7] Instead, we provide an asymptotic analysis of the TEM construction (as r grows) based on the coupling technique [19,28]. This part combines in a rather straightforward way the approach of [21] (which applied the coupling technique to the iterated Even-Mansour cipher) and of [23] (which applied the coupling technique to the CLRW construction). This allows us to prove that the r-round TEM construction is secure up to roughly $2^{\frac{rn}{r+2}}$ adversarial queries (against adaptive chosen-plaintext and ciphertext attacks). As with previous work, we conjecture that the "real" security bound is actually $2^{\frac{rn}{r+1}}$ queries (which we prove to hold for the weaker class of non-adaptive chosen-plaintext adversaries), but that the coupling technique is not adapted to prove this.

[6] In fact, this is not as straightforward as it might seem, since our results assume that the hash function family $\mathcal{H}$ is uniform in addition to being AXU, whereas the security result of [24] only requires $\mathcal{H}$ to be AXU. Inspection of our proof indicates however that the uniformity assumption on $\mathcal{H}$ can be safely lifted when the adversary is not allowed to query the inner permutations.

[7] For readers familiar with [7], which tightly analyzed the security of the traditional iterated EM cipher for any number of rounds, the main obstacle is that in the tweakable EM setting, the paths for two construction queries with distinct tweaks can collide at the input of inner permutations, whereas this can never happen in the traditional EM setting. While this is exactly the difficulty that we are able to handle for $r = 2$ in Lemma 3, getting a combinatorial lemma similar to [7, Lemma 1] that would allow to analyze good transcripts for any number of rounds in the tweakable setting seems more challenging.

Application to Related-Key Security. There are strong connections between tweakable block ciphers and the related-key security of traditional block ciphers [4,25]. We expand on this in the full version of the paper [8], explaining how our results have immediate implications for the related-key security of the traditional (iterated) Even-Mansour cipher with a nonlinear key-schedule.

Related Work and Perspectives. There are very few papers studying generic ways of building tweakable block ciphers from some lower-level primitive than a traditional block cipher. One notable exception is the work of Goldenberg *et al.* [16] who studied how to tweak (generically) Feistel ciphers (in other words, they showed how to construct tweakable block ciphers from pseudorandom functions). This was extended to generalized Feistels by Mitsuda and Iwata [27]. Our own work seems to be the first (besides [9], that capped at the birthday bound) to explore theoretically sound ways to construct "by-design" tweakable block ciphers with an SPN or more generally a key-alternating structure. In a sense, it can be seen as complementary to the recent TWEAKEY framework introduced by Jean *et al.* [20], that tackled a similar goal but adopted a more practical and attack-driven (rather than proof-oriented) angle. We hope that combining these two approaches will pave the way towards efficient and theoretically sound ways of building tweakable key-alternating ciphers, or tweaking existing ones such as AES. We also note that the term *tweakable Even-Mansour* was previously used by the designers of Minalpher [35] (a candidate to the CAESAR competition) to designate a permutation-based variant of Rogaway's XEX construction [32]. It relates to construction (4) by eliminating the AXU hash function $H_k(t)$ and replacing it by $\Delta = (k\|t) \oplus P(k\|t)$ (thereby halving tweak- and key-length), in about the same way XEX replaces the AXU hash function of the LRW construction (1) by a "gadget" calling the underlying block cipher E_k. The designers of Minalpher prove that this construction also achieves birthday-bound security.

Finally, we bring up some open problems. First, as already mentioned, it would be very interesting to give a tight analysis of the TEM construction for any number $r > 2$ of rounds (a first, hopefully simpler step towards this goal would be to give a tight bound for the CLRW construction for $r > 2$). Second, variants with the same permutation and/or non-independent round keys are also worth studying, as was done in [6] for the (traditional) two-round iterated Even-Mansour cipher. Third, since implementing an AXU hash function family might be costly, it would be very valuable to explore whether linear operations for mixing the key and the tweak into the state of an Even-Mansour-like construction might be enough to get security beyond the birthday bound.

2 Preliminaries

2.1 Notation and General Definitions

General Notation. In all the following, we fix an integer $n \geq 1$ and denote $N = 2^n$. For integers $1 \leq b \leq a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0 = 1$ by convention. The set of all permutations of $\{0,1\}^n$ will be denoted

$\mathsf{P}(n)$. Given a non-empty set X, we denote $x \leftarrow_{\$} X$ the draw of an element x from X uniformly at random.

Tweakable Block Ciphers. A *tweakable block cipher* with key space $\mathcal{K}$, tweak space $\mathcal{T}$, and message space $\mathcal{M}$ is a mapping $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ such that for any key $k \in \mathcal{K}$ and any tweak $t \in \mathcal{T}$, $x \mapsto \widetilde{E}(k, t, x)$ is a permutation of $\mathcal{M}$. We denote $\mathsf{TBC}(\mathcal{K}, \mathcal{T}, n)$ the set of all tweakable block ciphers with key space $\mathcal{K}$, tweak space $\mathcal{T}$, and message space $\{0,1\}^n$. A *tweakable permutation* with tweak space $\mathcal{T}$ and message space $\mathcal{M}$ is a mapping $\widetilde{P} : \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ such that for any tweak $t \in \mathcal{T}$, $x \mapsto \widetilde{P}(t, x)$ is a permutation of $\mathcal{M}$. We denote $\mathsf{TP}(\mathcal{T}, n)$ the set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^n$.

The Iterated Tweakable Even-Mansour Construction. Fix integers $n, r \geq 1$. Let $\mathcal{T}$ and $\mathcal{K}$ be two sets, and $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$ be a family of functions from $\mathcal{T}$ to $\{0,1\}^n$ indexed by $\mathcal{K}$. The r-round iterated tweakable Even-Mansour construction $\mathsf{TEM}[n, r, \mathcal{H}]$ specifies, from an r-tuple $\mathbf{P} = (P_1, \ldots, P_r)$ of permutations of $\{0,1\}^n$, a tweakable block cipher with key space $\mathcal{K}^r$, tweak space $\mathcal{T}$, and message space $\{0,1\}^n$, simply denoted $\mathsf{TEM}^{\mathbf{P}}$ in the following (parameters $[n, r, \mathcal{H}]$ will always be clear from the context) which maps a key $\mathbf{k} = (k_1, \ldots, k_r) \in \mathcal{K}^r$, a tweak $t \in \mathcal{T}$, and a plaintext $x \in \{0,1\}^n$ to the ciphertext defined as (see Fig. 1):

$$\mathsf{TEM}^{\mathbf{P}}(\mathbf{k}, t, x) = \mathit{\Pi}^{P_r}_{k_r,t} \circ \cdots \circ \mathit{\Pi}^{P_1}_{k_1,t}(x),$$

where $\mathit{\Pi}^{P}_{k,t}$ is the permutation of $\{0,1\}^n$ (corresponding to one round of the construction) defined as

$$\mathit{\Pi}^{P}_{k,t}(x) = H_k(t) \oplus P(H_k(t) \oplus x).$$

We will denote $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}$ the mapping taking as input $(t, x) \in \mathcal{T} \times \{0,1\}^n$ and returning $\mathsf{TEM}^{\mathbf{P}}(\mathbf{k}, t, x)$.

Convention 1. In order to lighten the notation, we will often identify the hash function family $\mathcal{H}$ and its key space $\mathcal{K}$. This way, the key space of the r-round $\mathsf{TEM}^{\mathbf{P}}$ tweakable block cipher is simply $\mathcal{H}^r$, and we write

$$\mathsf{TEM}^{\mathbf{P}}_{\mathbf{h}}(t, x) = h_r(t) \oplus P_r(h_r(t) \oplus \cdots \oplus h_1(t) \oplus P_1(h_1(t) \oplus x) \cdots)$$

where $\mathbf{h} = (h_1, \ldots, h_r) \in \mathcal{H}^r$ is the key of $\mathsf{TEM}^{\mathbf{P}}$.

Uniform AXU Hash Function Family. We will need the following properties of the hash function family $\mathcal{H}$.

Definition 1. *Let $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$ be a family of functions from some set $\mathcal{T}$ to $\{0,1\}^n$ indexed by a set of keys $\mathcal{K}$. $\mathcal{H}$ is said to be* uniform *if for any $t \in \mathcal{T}$ and $y \in \{0,1\}^n$,*

$$\Pr[k \leftarrow_{\$} \mathcal{K} : H_k(t) = y] = 2^{-n}.$$

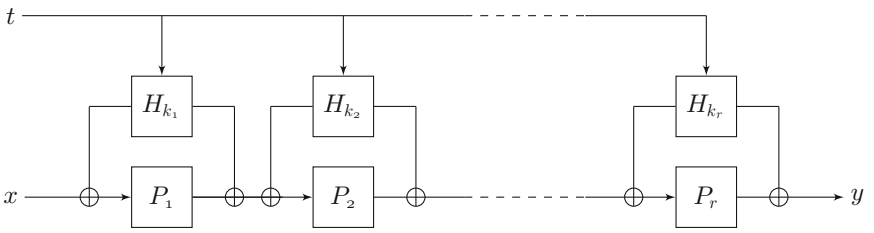

Fig. 1. The tweakable Even-Mansour construction with r rounds, based on public permutations $P_1, \ldots, P_r$ and a family of hash functions $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$.

$\mathcal{H}$ is said ε-almost XOR-universal *(ε-AXU) if for all distinct $t, t' \in \mathcal{T}$ and all $y \in \{0,1\}^n$,*

$$\Pr[k \leftarrow_{\$} \mathcal{K} : H_k(t) \oplus H_k(t') = y] \leq \varepsilon.$$

$\mathcal{H}$ is simply said XOR-universal *(XU) if it is 2^{-n}-AXU.*

Example 1. Let $\mathbb{F}_{2^n}$ be the set $\{0,1\}^n$ seen as the field with 2^n elements defined by some irreducible polynomial of degree n over $\mathbb{F}_2$, the field with two elements, and denote $a \otimes b$ the field multiplication of two elements $a, b \in \mathbb{F}_{2^n}$. For any integer $\ell \geq 1$, we define the family of functions $\mathcal{H} = (H_k)_{k \in \mathbb{F}_{2^n}}$ with domain $(\mathbb{F}_{2^n})^\ell$ and range $\mathbb{F}_{2^n}$ as

$$H_k(t_1, \ldots, t_\ell) = \sum_{i=1}^{\ell} k^i \otimes t_i.$$

Then $\mathcal{H}$ is $\ell \cdot 2^{-n}$-AXU [37]. Note however that $\mathcal{H}$ is not uniform since $(0, \ldots, 0)$ is always mapped to 0 independently of the key. This can be handled either by adding an independent key (resulting in $2n$-bit keys), i.e., defining $\mathcal{H}' = (H'_{k,k'})_{(k,k') \in (\mathbb{F}_{2^n})^2}$ where $H'_{k,k'}(t_1, \ldots, t_\ell) = H_k(t_1 \ldots, t_\ell) \oplus k'$, or by forbidding the all-zero tweak, in which case the family is not exactly uniform, but rather $\ell \cdot 2^{-n}$-almost uniform, i.e., for any $t \in \mathcal{T} \setminus \{(0, \ldots, 0)\}$ and $y \in \{0,1\}^n$, $\Pr[k \leftarrow_{\$} \mathcal{K} : H_k(t) = y] \leq \ell \cdot 2^{-n}$. Our results can be straightforwardly extended to the case of ε-almost uniform families of functions.

2.2 Security Definitions

Fix some family of functions $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$ from $\mathcal{T}$ to $\{0,1\}^n$. To study the security of the construction $\mathsf{TEM}[n, r, \mathcal{H}]$ in the Random Permutation Model, we consider a distinguisher $\mathcal{D}$ which interacts with $r+1$ oracles that we denote generically $(\widetilde{P}_0, P_1, \ldots, P_r)$, where syntactically $\widetilde{P}_0$ is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\{0,1\}^n$, and $P_1, \ldots, P_r$ are permutations of $\{0,1\}^n$. The goal of $\mathcal{D}$ is to distinguish two "worlds": the so-called *real world*,

where $\mathcal{D}$ interacts with $(\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}, \mathbf{P})$, where $\mathbf{P} = (P_1, \ldots, P_r)$ is a tuple of public random permutations and the key $\mathbf{k} = (k_1, \ldots, k_r)$ is drawn uniformly at random from $\mathcal{K}^r$, and the so-called *ideal world* $(\widetilde{P}_0, \mathbf{P})$, where $\widetilde{P}_0$ is a uniformly random tweakable permutation and $\mathbf{P}$ is a tuple of random permutations of $\{0,1\}^n$ independent from $\widetilde{P}_0$. We will refer to $\widetilde{P}_0$ as the *construction oracle* and to $P_1, \ldots, P_r$ as the *inner permutation oracles*.

Similarly to [21], we consider two classes of distinguishers depending on how they can issue their queries:

- a *non-adaptive chosen-plaintext* (NCPA) distinguisher runs in two phases: during the first phase, it only queries the inner permutations, adaptively and in both directions; in the second phase, it issues a tuple of non-adaptive chosen-plaintext queries to the construction oracle and receives the corresponding answers (this tuple of queries may depend on the answers received in the first phase, but all queries must be chosen non-adaptively before receiving any answer from the construction oracle);
- an *adaptive chosen-plaintext and ciphertext* (CCA) distinguisher is not restricted in how it queries its oracles: it can make adaptive bidirectional queries to all its oracles.

We stress that the NCPA model is not very interesting in itself[8] and will only be useful as an intermediate step for the coupling-based security proof in Sect. 4.

The distinguishing advantage of a distinguisher $\mathcal{D}$ is defined as

$$\mathbf{Adv}(\mathcal{D}) \stackrel{\text{def}}{=} \left| \Pr\left[\mathcal{D}^{\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}, \mathbf{P}} = 1\right] - \Pr\left[\mathcal{D}^{\widetilde{P}_0, \mathbf{P}} = 1\right] \right|,$$

where the first probability is taken over the random choice of $\mathbf{k}$ and $\mathbf{P}$, and the second probability is taken over the random choice of $\widetilde{P}_0$ and $\mathbf{P}$. In all the following, we consider computationally unbounded distinguishers, and hence we can assume *wlog* that they are deterministic. We also assume that they never make pointless queries (i.e., queries whose answers can be unambiguously deduced from previous answers).

For non-negative integers q_c, q_p and $\mathrm{ATK} \in \{\mathrm{NCPA}, \mathrm{CCA}\}$, we define the insecurity of the $\mathsf{TEM}[n, r, \mathcal{H}]$ construction against ATK-attacks as

$$\mathbf{Adv}^{\mathrm{atk}}_{\mathsf{TEM}[n,r,\mathcal{H}]}(q_c, q_p) = \max_{\mathcal{D}} \mathbf{Adv}(\mathcal{D}),$$

where the maximum is taken over all distinguishers in the class ATK making exactly q_c queries to the construction oracle and exactly q_p queries to each inner permutation oracle.

[8] Indeed, forbidding the adversary to query the inner permutation oracles at some point of the attack takes us away from the spirit of the Random Permutation model, which is thought as a heuristically sound way of modeling some complex (but otherwise public and fully described) permutation that the adversary can always evaluate at will.

3 Tight Bounds for One and Two Rounds

3.1 The H-Coefficients Technique

We start by describing Patarin's H-coefficients technique [30], which has enjoyed increasing adoption since Chen and Steinberger used it to prove the security of the iterated Even-Mansour cipher for an arbitrary number of rounds [7].

Transcript. We summarize the interaction of $\mathcal{D}$ with its oracles in what we call the *queries transcript* $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ of the attack, where $\mathcal{Q}_C$ records the queries to the construction oracle and $\mathcal{Q}_{P_i}$, $1 \leq i \leq r$, records the queries to inner permutation P_i. More precisely, $\mathcal{Q}_C$ contains all triples $(t, x, y) \in \mathcal{T} \times \{0,1\}^n \times \{0,1\}^n$ such that $\mathcal{D}$ either made the direct query (t, x) to the construction oracle and received answer y, or made the inverse query (t, y) and received answer x. Similarly, for $1 \leq i \leq r$, $\mathcal{Q}_{P_i}$ contains all pairs $(u, v) \in \{0,1\}^n \times \{0,1\}^n$ such that $\mathcal{D}$ either made the direct query u to permutation P_i and received answer v, or made the inverse query v and received answer u. Note that queries are recorded in a directionless and unordered fashion, but by our assumption that the distinguisher is deterministic, there is a one-to-one mapping between this representation and the raw transcript of the interaction of $\mathcal{D}$ with its oracles (see e.g. [7] for more details). Note also that by our assumption that $\mathcal{D}$ never makes pointless queries, each query to the construction oracle results in a distinct triple in $\mathcal{Q}_C$, and each query to P_i results in a distinct pair in $\mathcal{Q}_{P_i}$, so that $|\mathcal{Q}_C| = q_c$ and $|\mathcal{Q}_{P_i}| = q_p$ for $1 \leq i \leq r$ since we assume that the distinguisher always makes the maximal number of allowed queries to each oracle. In all the following, we also denote m the number of distinct tweaks appearing in $\mathcal{Q}_C$, and q_i the number of queries for the i-th tweak, $1 \leq i \leq m$, using an arbitrary ordering of the tweaks. Note that m may depend on the answers received from the oracles, yet one always has $\sum_{i=1}^{m} q_i = q_c$.

We say that a queries transcript is *attainable* (with respect to some fixed distinguisher $\mathcal{D}$) if there exists oracles $(\widetilde{P}_0, \mathbf{P})$ such that the interaction of $\mathcal{D}$ with $(\widetilde{P}_0, \mathbf{P})$ yields this transcript (said otherwise, the probability to obtain this transcript in the "ideal" world is non-zero). Moreover, in order to have a simple definition of bad transcripts, we reveal to the adversary at the end of the experiment the actual tuple of keys $\mathbf{k} = (k_1, \ldots, k_r)$ if we are in the real world, while in the ideal world, we simply draw dummy keys $(k_1 \ldots, k_r) \leftarrow_{\$} \mathcal{K}^r$ independently from the answers of the oracle $\widetilde{P}_0$. (This can obviously only increase the advantage of the distinguisher, so that this is without loss of generality). All in all, a transcript τ is a tuple $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, \mathbf{k})$, and we say that a transcript is attainable if the corresponding queries transcript $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ is attainable. We denote Θ the set of attainable transcripts. In all the following, we denote T_{re}, resp. T_{id}, the probability distribution of the transcript τ induced by the real world, resp. the ideal world (note that these two probability distributions depend on the distinguisher). By extension, we use the same notation to denote a random variable distributed according to each distribution. The main lemma of the H-coefficients technique is the following one (see e.g. [6,7] for the proof).

Lemma 1. *Fix a distinguisher $\mathcal{D}$. Let $\Theta = \Theta_{\text{good}} \sqcup \Theta_{\text{bad}}$ be a partition of the set of attainable transcripts. Assume that there exists ε_1 such that for any $\tau \in \Theta_{\text{good}}$, one has*[9]

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \varepsilon_1,$$

and that there exists ε_2 such that $\Pr[T_{\text{id}} \in \Theta_{\text{bad}}] \leq \varepsilon_2$. Then $\boldsymbol{Adv}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2$.

Additional Notation. Given a permutation queries transcript $\mathcal{Q}$ and a permutation P, we say that P *extends* $\mathcal{Q}$, denoted $P \vdash \mathcal{Q}$, if $P(u) = v$ for all $(u, v) \in \mathcal{Q}$. By extension, given a tuple of permutation queries transcript $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ and a tuple of permutations $\mathbf{P} = (P_1, \ldots, P_r)$, we say that $\mathbf{P}$ extends $\mathcal{Q}_{\mathbf{P}}$, denoted $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$, if $P_i \vdash \mathcal{Q}_{P_i}$ for each $i = 1, \ldots, r$. Note that for a permutation transcript of size q_p, one has

$$\Pr[P \leftarrow_{\$} \mathsf{P}(n) : P \vdash \mathcal{Q}] = \frac{1}{(N)_{q_p}}. \tag{5}$$

Similarly, given a tweakable permutation transcript $\widetilde{\mathcal{Q}}$ and a tweakable permutation $\widetilde{P}$, we say that $\widetilde{P}$ *extends* $\widetilde{\mathcal{Q}}$, denoted $\widetilde{P} \vdash \widetilde{\mathcal{Q}}$, if $\widetilde{P}(t, x) = y$ for all $(t, x, y) \in \widetilde{\mathcal{Q}}$. For a tweakable permutation transcript $\widetilde{\mathcal{Q}}$ with m distinct tweaks and q_i queries corresponding to the i-th tweak, one has

$$\Pr[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n) : \widetilde{P} \vdash \widetilde{\mathcal{Q}}] = \prod_{i=1}^{m} \frac{1}{(N)_{q_i}}. \tag{6}$$

Preliminary Observations. It is easy to see that the interaction of a distinguisher $\mathcal{D}$ with oracles $(\widetilde{P}_0, P_1, \ldots, P_r)$ yields any attainable queries transcript $(\mathcal{Q}_C, \mathcal{Q}_{\mathbf{P}})$ with $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ *iff* $\widetilde{P}_0 \vdash \mathcal{Q}_C$ and $P_i \vdash \mathcal{Q}_{P_i}$ for $1 \leq i \leq r$. In the ideal world, the key $\mathbf{k}$, the permutations $P_1, \ldots, P_r$, and the tweakable permutation $\widetilde{P}_0$ are all uniformly random and independent, so that, by (5) and (6), the probability of getting any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{\mathbf{P}}, \mathbf{k})$ in the ideal world is

$$\Pr[T_{\text{id}} = \tau] = \frac{1}{|\mathcal{K}|^r} \times \left(\frac{1}{(N)_{q_p}}\right)^r \times \prod_{i=1}^{m} \frac{1}{(N)_{q_i}}.$$

In the real world, the probability to obtain τ is

$$\Pr[T_{\text{re}} = \tau] = \frac{1}{|\mathcal{K}|^r} \times \left(\frac{1}{(N)_{q_p}}\right)^r \times \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}} \vdash \mathcal{Q}_C \,\middle|\, \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right].$$

Let

$$\mathsf{p}(\tau) \stackrel{\text{def}}{=} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}} \vdash \mathcal{Q}_C \,\middle|\, \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right].$$

[9] Recall that for an attainable transcript, one has $\Pr[T_{\text{id}} = \tau] > 0$.

Then we have

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = \mathsf{p}(\tau) \Big/ \prod_{i=1}^{m} \frac{1}{(N)_{q_i}} = \mathsf{p}(\tau) \cdot \prod_{i=1}^{m} (N)_{q_i}. \tag{7}$$

Hence, to apply Lemma 1, we will have to compare $\mathsf{p}(\tau)$ and $\prod_{i=1}^{m} 1/(N)_{q_i}$, assuming τ is good (for some adequate definition of bad and good transcripts).

3.2 Security Proof for One Round

We consider here the one-round construction $\mathsf{TEM}[n, 1, \mathcal{H}]$. Using Convention 1, we have

$$\mathsf{TEM}_{h_1}^{P_1}(t, x) = h_1(t) \oplus P_1(h_1(t) \oplus x)$$

where the key is $h_1 \leftarrow_{\$} \mathcal{H}$. We prove the following theorem.

Theorem 1. *Let $\mathcal{H}$ be a uniform ε-AXU family of functions from $\mathcal{T}$ to $\{0,1\}^n$. For any integers q_c and q_p, one has*

$$\boldsymbol{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,1,\mathcal{H}]}(q_c, q_p) \leq q_c^2 \varepsilon + \frac{2 q_c q_p}{N}.$$

The proof uses the H-coefficients technique that we exposed in Sect. 3.1, and serves as a good warm-up before the more complex two-round case. For reasons of space, it is deferred to the full version of the paper [8].

3.3 Security Proof for Two Rounds

Statement of the Result and Discussion. Let $\mathcal{H}$ be an ε-AXU and uniform function family. Using Convention 1, the two-round tweakable Even-Mansour construction is written

$$\mathsf{TEM}_{(h_1,h_2)}^{P_1,P_2}(t, x) = h_2(t) \oplus P_2\big(h_2(t) \oplus h_1(t) \oplus P_1(h_1(t) \oplus x)\big)$$

where P_1, P_2 are two public random permutations, $(h_1, h_2) \leftarrow_{\$} \mathcal{H}^2$ is the key, t is the tweak and x the plaintext. The main result of our paper is the following theorem.

Theorem 2. *Let $\mathcal{H}$ be a uniform ε-AXU family of functions from $\mathcal{T}$ to $\{0,1\}^n$. Assume that $q_p + 3q_c \leq N/2$ and $q_c \leq \min\{N^{2/3}, \varepsilon^{-2/3}\}$. Then*

$$\boldsymbol{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,2,\mathcal{H}]}(q_c, q_p) \leq \frac{29\sqrt{q_c} q_p}{N} + \varepsilon \sqrt{q_c} q_p + 4\varepsilon q_c^{3/2} + \frac{30 q_c^{3/2}}{N}.$$

In particular, assuming $\mathcal{H}$ is XU for simplicity (i.e., $\varepsilon = 2^{-n}$), one can see that the two-round TEM construction ensures security up to approximately $2^{2n/3}$ adversarial queries. In fact, for any number $q_c \ll 2^{2n/3}$ of construction queries,

the two-round TEM construction remains secure as long as q_p is small compared with $2^n/\sqrt{q_c}$.

The proof uses the H-coefficients technique. As usual, we will first define bad transcripts and upper bound their probability in the ideal world, and then show that the probabilities to obtain any good transcript in the real world and the ideal world are sufficiently close.

Definition and Probability of Bad Transcripts. Let $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (h_1, h_2))$ be an attainable transcript, with $|\mathcal{Q}_C| = q_c$ and $|\mathcal{Q}_{P_1}| = |\mathcal{Q}_{P_2}| = q_p$. We let

$$U_1 = \{u_1 \in \{0,1\}^n : (u_1, v_1) \in \mathcal{Q}_{P_1}\}, \quad V_1 = \{v_1 \in \{0,1\}^n : (u_1, v_1) \in \mathcal{Q}_{P_1}\},$$
$$U_2 = \{u_2 \in \{0,1\}^n : (u_2, v_2) \in \mathcal{Q}_{P_2}\}, \quad V_2 = \{v_2 \in \{0,1\}^n : (u_2, v_2) \in \mathcal{Q}_{P_2}\}$$

denote the domains and ranges of $\mathcal{Q}_{P_1}$ and $\mathcal{Q}_{P_2}$ respectively. For each u and $v \in \{0,1\}^n$, let

$$X_u = \{(t,x,y) \in \mathcal{Q}_C : x \oplus h_1(t) = u\},$$
$$Y_v = \{(t,x,y) \in \mathcal{Q}_C : y \oplus h_2(t) = v\}.$$

We define four quantities characterizing a transcript τ, namely

$$\alpha_1 \stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C : x \oplus h_1(t) \in U_1\}|,$$
$$\alpha_2 \stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C : y \oplus h_2(t) \in V_2\}|,$$
$$\beta_1 \stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C : \exists (t',x',y') \neq (t,x,y), x \oplus h_1(t) = x' \oplus h_1(t')\}|,$$
$$\beta_2 \stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C : \exists (t',x',y') \neq (t,x,y), y \oplus h_2(t) = y' \oplus h_2(t')\}|.$$

In words, α_1 (resp. α_2) is the number of queries $(t,x,y) \in \mathcal{Q}_C$ which "collide" with a query $(u_1,v_1) \in \mathcal{Q}_{P_1}$ (resp. that collide with a query $(u_2,v_2) \in \mathcal{Q}_{P_2}$), and β_1 (resp. β_2) is the number of queries $(t,x,y) \in \mathcal{Q}_C$ which "collide" with another query (t',x',y') at the input of P_1 (resp. at the output of P_2). Note that one also has

$$\beta_1 = \sum_{\substack{u \in \{0,1\}^n : \\ |X_u| > 1}} |X_u|, \qquad \beta_2 = \sum_{\substack{v \in \{0,1\}^n : \\ |Y_v| > 1}} |Y_v|. \tag{8}$$

Definition 2. We say that an attainable transcript τ is bad if at least one of the following conditions is fulfilled (see Fig. 2 for a diagram of the first ten conditions):

(C-1) there exists $(t,x,y) \in \mathcal{Q}_C$, $u_1 \in U_1$, and $v_2 \in V_2$ such that $x \oplus h_1(t) = u_1$ and $y \oplus h_2(t) = v_2$;
(C-2) there exists $(t,x,y) \in \mathcal{Q}_C$, $(u_1,v_1) \in \mathcal{Q}_{P_1}$, and $u_2 \in U_2$ such that $x \oplus h_1(t) = u_1$ and $v_1 \oplus h_1(t) \oplus h_2(t) = u_2$;
(C-3) there exists $(t,x,y) \in \mathcal{Q}_C$, $(u_2,v_2) \in \mathcal{Q}_{P_2}$, and $v_1 \in V_1$ such that $y \oplus h_2(t) = v_2$ and $v_1 \oplus h_1(t) \oplus h_2(t) = u_2$;

(C-4) there exists $(t,x,y),(t',x',y'),(t'',x'',y'') \in \mathcal{Q}_C$ with (t,x,y) distinct from (t',x',y') and from (t'',x'',y'') such that $x \oplus h_1(t) = x' \oplus h_1(t')$ and $y \oplus h_2(t) = y'' \oplus h_2(t'')$;
(C-5) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ such that $x \oplus h_1(t) = x' \oplus h_1(t')$ and $h_1(t) \oplus h_2(t) = h_1(t') \oplus h_2(t')$;
(C-6) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ such that $y \oplus h_2(t) = y' \oplus h_2(t')$ and $h_1(t) \oplus h_2(t) = h_1(t') \oplus h_2(t')$;
(C-7) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ and $u_1 \in U_1$ such that $y \oplus h_2(t) = y' \oplus h_2(t')$ and $x \oplus h_1(t) = u_1$;
(C-8) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ and $v_2 \in V_2$ such that $x \oplus h_1(t) = x' \oplus h_1(t')$ and $y \oplus h_2(t) = v_2$;
(C-9) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$, $(u_1,v_1),(u_1',v_1') \in \mathcal{Q}_{P_1}$ such that $x \oplus h_1(t) = u_1$, $x' \oplus h_1(t') = u_1'$ and $v_1 \oplus h_1(t) \oplus h_2(t) = v_1' \oplus h_1(t') \oplus h_2(t')$;
(C-10) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$, $(u_2,v_2),(u_2',v_2') \in \mathcal{Q}_{P_2}$ such that $y \oplus h_2(t) = v_2$, $y' \oplus h_2(t') = v_2'$ and $u_2 \oplus h_1(t) \oplus h_2(t) = u_2' \oplus h_1(t') \oplus h_2(t')$;
(C-11) $\alpha_1 \geq \sqrt{q_c}$;
(C-12) $\alpha_2 \geq \sqrt{q_c}$;
(C-13) $\beta_1 \geq \sqrt{q_c}$;
(C-14) $\beta_2 \geq \sqrt{q_c}$.

Otherwise we say that τ is good. We denote Θ_{good}, resp. Θ_{bad} the set of good, resp. bad transcripts. $\Diamond$

We start by upper bounding the probability to get a bad transcript in the ideal world.

Lemma 2. *For any integers q_c and q_p, one has*

$$\Pr[T_{\text{id}} \in \Theta_{\text{bad}}] \leq \frac{3q_c q_p^2}{N^2} + 2\varepsilon^2 q_c^3 + \frac{\varepsilon q_c^2 q_p}{N} + \frac{2\sqrt{q_c} q_p}{N} + 2\varepsilon q_c^{3/2}.$$

Proof. Let $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2})$ be any attainable queries transcript. Recall that in the ideal world, (h_1, h_2) is drawn independently from the queries transcript. We upper bound the probabilities of the fourteen conditions in turn. We denote Θ_i the set of attainable transcripts fulfilling condition (C-i).

Conditions (C-1), (C-2), and (C-3). Consider condition (C-1). For any $(t,x,y) \in \mathcal{Q}_C$, $u_1 \in U_1$, and $v_2 \in V_2$, one has, by the uniformity of $\mathcal{H}$ and since h_1 and h_2 are independently drawn,

$$\Pr\left[\big(h_1(t) = x \oplus u_1\big) \wedge \big(h_2(t) = y \oplus v_2\big)\right] = \frac{1}{N^2}.$$

Hence, summing over the $q_c q_p^2$ possibilities for (t,x,y), u_1, and v_1 yields

$$\Pr[T_{\text{id}} \in \Theta_1] \leq \frac{q_c q_p^2}{N^2}.$$

Similarly, for (C-2) and (C-3), one obtains

$$\Pr\left[T_{\text{id}} \in \Theta_2\right] \leq \frac{q_c q_p^2}{N^2}, \qquad \Pr\left[T_{\text{id}} \in \Theta_3\right] \leq \frac{q_c q_p^2}{N^2}.$$

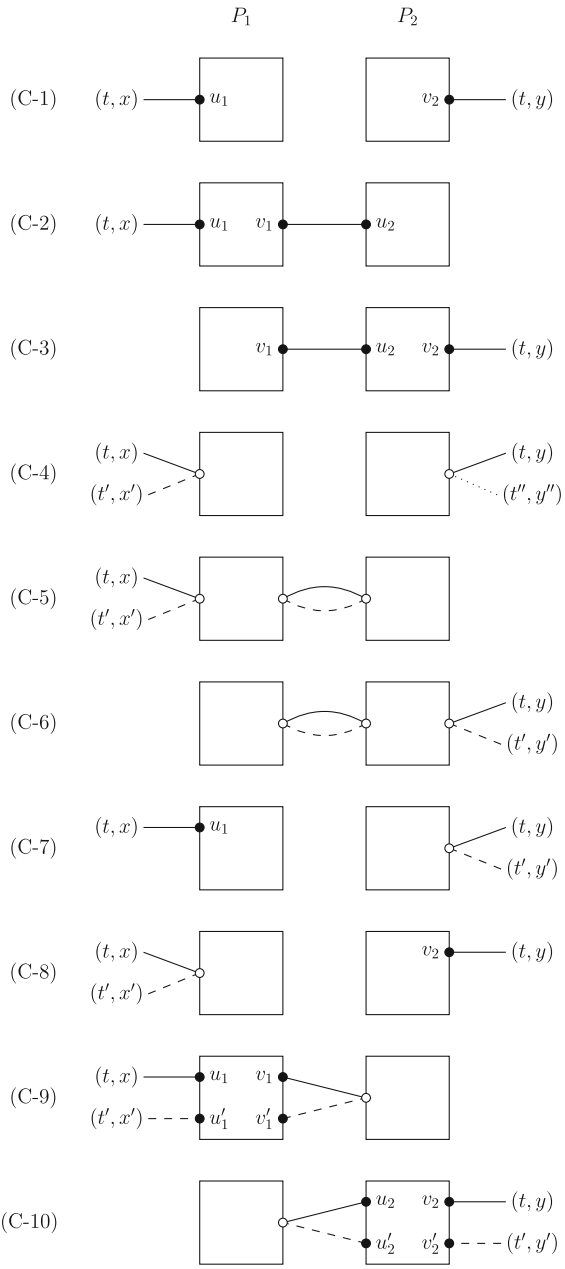

Fig. 2. The ten "collision" conditions characterizing a bad transcript. Black dots correspond to pairs $(u_1, v_1) \in \mathcal{Q}_{P_1}$ or $(u_2, v_2) \in \mathcal{Q}_{P_2}$. Note that for (C-4) one might have $(t', x') = (t'', x'')$, for (C-9) one might have $(u_1, v_1) = (u'_1, v'_1)$, and for (C-10) one might have $(u_2, v_2) = (u'_2, v'_2)$.

Condition (C-4). For any $(t,x,y),(t',x',y'),(t'',x'',y'') \in \mathcal{Q}_C$ with (t,x,y) distinct from (t',x',y') and from (t'',x'',y''), one has, by the ε-AXU property of $\mathcal{H}$ and since h_1 and h_2 are drawn independently,

$$\Pr\left[\left(h_1(t) \oplus h_1(t') = x \oplus x'\right) \wedge \left(h_2(t) \oplus h_2(t'') = y \oplus y''\right)\right] \leq \varepsilon^2.$$

Note that this also holds when $t = t'$ (resp. $t = t''$) since in that case necessarily $x \neq x'$ (resp. $y \neq y''$) by the assumption that $\mathcal{D}$ never makes pointless queries. Hence, summing over the (at most) q_c^3 possibilities for (t,x,y), (t',x',y'), (t'',x'',y''), one obtains

$$\Pr\left[T_{\mathrm{id}} \in \Theta_4\right] \leq \varepsilon^2 q_c^3.$$

Conditions (C-5) and (C-6). For any two distinct queries $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$, one has, by the ε-AXU property of $\mathcal{H}$ and since h_1 and h_2 are drawn independently,

$$\Pr\left[\left(h_1(t) \oplus h_1(t') = x \oplus x'\right) \wedge \left(h_2(t) \oplus h_2(t') = h_1(t) \oplus h_1(t')\right)\right] \leq \varepsilon^2.$$

Hence, summing over the $q_c(q_c-1)/2$ possible pairs of distinct queries, we get

$$\Pr\left[T_{\mathrm{id}} \in \Theta_5\right] \leq \frac{\varepsilon^2 q_c^2}{2}, \qquad \text{and similarly } \Pr\left[T_{\mathrm{id}} \in \Theta_6\right] \leq \frac{\varepsilon^2 q_c^2}{2}.$$

Conditions (C-7) and (C-8). For any two distinct queries $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ and any $u_1 \in U_1$, one has, by the ε-AXU property and uniformity of $\mathcal{H}$ and since h_1 and h_2 are drawn independently,

$$\Pr\left[\left(h_2(t) \oplus h_2(t') = y \oplus y'\right) \wedge \left(h_1(t) = x \oplus u_1\right)\right] \leq \frac{\varepsilon}{N}.$$

Then, summing over $(t,x,y) \neq (t',x',y')$ and u_1,

$$\Pr[T_{\mathrm{id}} \in \Theta_7] \leq \frac{\varepsilon q_c^2 q_p}{2N}, \qquad \text{and similarly } \Pr[T_{\mathrm{id}} \in \Theta_8] \leq \frac{\varepsilon q_c^2 q_p}{2N}.$$

Conditions (C-9), (C-10), (C-11), and (C-12). We will deal with conditions (C-9) and (C-11) together, using the fact that

$$\Pr\left[T_{\mathrm{id}} \in \Theta_9 \cup \Theta_{11}\right] = \Pr\left[T_{\mathrm{id}} \in \Theta_{11}\right] + \Pr\left[T_{\mathrm{id}} \in \Theta_9 \setminus \Theta_{11}\right].$$

To upper bound $\Pr\left[T_{\mathrm{id}} \in \Theta_{11}\right]$, we see α_1 as a random variable over the random choice of h_1 (since α_1 does not depend on h_2). First, note that by the uniformity of $\mathcal{H}$,

$$\mathbb{E}[\alpha_1] = \sum_{(t,x,y) \in \mathcal{Q}_C} \sum_{u_1 \in U_1} \Pr\left[x \oplus h_1(t) = u_1\right] = \frac{q_c q_p}{N},$$

so that by Markov's inequality,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_{11}\right] \leq \frac{\sqrt{q_c} q_p}{N}.$$

Fix any $h_1' \in \mathcal{H}$ such that, when $h_1 = h_1'$, $\alpha_1 < \sqrt{q_c}$, and fix any queries $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$, $(u_1,v_1),(u_1',v_1') \in \mathcal{Q}_{P_1}$ such that $x \oplus h_1(t) = u_1$ and $x' \oplus h_1(t') = u_1'$. Note that since $\alpha_1 < \sqrt{q_c}$, there are at most $\frac{q_c}{2}$ such tuple of queries. Then

$$\Pr\left[\left(h_1 = h_1'\right) \wedge \left(h_2(t) \oplus h_2(t') = v_1 \oplus h_1(t) \oplus v_1' \oplus h_1(t')\right)\right] \leq \frac{\varepsilon}{|\mathcal{H}|},$$

and, by summing over every h_1 such that $\alpha_1 < \sqrt{q_c}$ and every such tuple of queries, one has

$$\Pr\left[T_{\mathrm{id}} \in \Theta_9 \setminus \Theta_{11}\right] \leq \frac{\varepsilon q_c}{2}.$$

Finally,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_9 \cup \Theta_{11}\right] \leq \frac{\sqrt{q_c} q_p}{N} + \frac{\varepsilon q_c}{2}.$$

Similarly,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_{10} \cup \Theta_{12}\right] \leq \frac{\sqrt{q_c} q_p}{N} + \frac{\varepsilon q_c}{2}.$$

Conditions (C-13) and (C-14). For every $u \in \{0,1\}^n$, we see $|X_u|$ as a random variable over the random choice of h_1. We also introduce the random variable

$$C = |\{((t,x,y),(t',x',y')) \in \mathcal{Q}_C^2, (t,x,y) \neq (t',x',y') : x \oplus h_1(t) = x' \oplus h_1(t')\}|.$$

Then, by definition of β_1,

$$\beta_1 = |\{(t,x,y) \in \mathcal{Q}_C : \exists (t',x',y') \neq (t,x,y), x \oplus h_1(t) = x' \oplus h_1(t')\}| \leq C.$$

Hence, $\Pr\left[T_{\mathrm{id}} \in \Theta_{13}\right] \leq \Pr\left[C \geq \sqrt{q_c}\right]$. Note that

$$\mathbb{E}[C] = \sum_{(t,x,y) \neq (t',x',y')} \Pr\left[x \oplus h_1(t) = x' \oplus h_1(t')\right] \leq \frac{\varepsilon q_c^2}{2}.$$

By Markov's inequality,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_{13}\right] \leq \frac{\varepsilon q_c^{3/2}}{2}, \qquad \text{and similarly } \Pr\left[T_{\mathrm{id}} \in \Theta_{14}\right] \leq \frac{\varepsilon q_c^{3/2}}{2}.$$

The result follows by an union bound over all conditions. □

Analysis of Good Transcripts. Next, we have to study good transcripts.

Lemma 3. *Let q_c and q_p be integers such that $q_p + 3q_c \leq N/2$. Then for any good transcript τ, one has*

$$\frac{\Pr\left[T_{\mathrm{re}} = \tau\right]}{\Pr\left[T_{\mathrm{id}} = \tau\right]} \geq 1 - \left(\frac{4q_c(q_p + 2q_c)^2}{N^2} + \frac{14q_c^{3/2} + 4\sqrt{q_c} q_p}{N}\right).$$

Proof. Deferred to the full version of the paper [8] for reasons of space. □

Concluding the Proof of Theorem 2. We are now ready to prove Theorem 2. Combining Lemmas 1, 2, and 3, one has

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,2,\mathcal{H}]}(q_c,q_p) &\le \frac{3q_cq_p^2}{N^2}+2\varepsilon^2q_c^3+\frac{\varepsilon q_c^2q_p}{N}+\frac{2\sqrt{q_c}q_p}{N}+2\varepsilon q_c^{3/2}\\ &\quad+\frac{4q_c(q_p+2q_c)^2}{N^2}+\frac{14q_c^{3/2}+4\sqrt{q_c}q_p}{N}\\ &=\frac{7q_cq_p^2}{N^2}+\frac{16q_c^2q_p}{N^2}+\frac{6\sqrt{q_c}q_p}{N}+\frac{\varepsilon q_c^2q_p}{N}+2\varepsilon^2q_c^3+2\varepsilon q_c^{3/2}\\ &\quad+\frac{16q_c^3}{N^2}+\frac{14q_c^{3/2}}{N}\\ &\le\frac{7q_cq_p^2}{N^2}+\frac{16q_c^2q_p}{N^2}+\frac{6\sqrt{q_c}q_p}{N}+\frac{\varepsilon q_c^2q_p}{N}+4\varepsilon q_c^{3/2}+\frac{30q_c^{3/2}}{N},\end{aligned}$$

where for the last inequality we used the assumption that $q_c \le \min\{N^{2/3}, \varepsilon^{-2/3}\}$. Since the result holds trivially when $q_cq_p^2 > N^2$, we can assume that $q_cq_p^2 \le N^2$, so that $q_cq_p^2/N^2 \le \sqrt{q_c}q_p/N$. Moreover, since $q_c \le N^{2/3}$, one has $q_c^2/N^2 \le \sqrt{q_c}/N$ and $q_c^2/N \le \sqrt{q_c}$, which concludes the proof of Theorem 2.

4 Asymptotic Bounds via the Coupling Technique

When the number of rounds r of the TEM construction grows, one has the following result.

Theorem 3. *Let r be an even integer and $r' = r/2$. Let q_c, q_p be positive integers, and $\mathcal{H}$ be a uniform ε-AXU family of functions from $\mathcal{T}$ to $\{0,1\}^n$. Then:*

$$\boldsymbol{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,r,\mathcal{H}]}(q_c,q_p) \le \sqrt{2^{r'+4}\frac{q_c(N\varepsilon q_c+q_p)^{r'}}{N^{r'}}}.$$

For odd r, we have $\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,r,\mathcal{H}]} \le \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,r-1,\mathcal{H}]}$, so that we can use the above bound with $r-1$. Using an ε-AXU function family with $\varepsilon \simeq 2^{-n}$, we see that the iterated tweakable Even-Mansour cipher with an even number r of rounds achieves CCA-security up to roughly $2^{\frac{rn}{r+2}}$ adversarial queries.

The proof relies on the coupling technique. Since it combines in a rather straightforward way the approach of [21,23], the proof is entirely deferred to the full version of the paper [8].

References

1. Andreeva, E., Bogdanov, A., Dodis, Y., Mennink, B., Steinberger, J.P.: On the indifferentiability of key-alternating ciphers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 531–550. Springer, Heidelberg (2013). http://eprint.iacr.org/2013/061

2. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013)
3. Andreeva, E., Bogdanov, A., Mennink, B.: Towards understanding the known-key security of block ciphers. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 348–366. Springer, Heidelberg (2014)
4. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
5. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.-X., Steinberger, J., Tischhauser, E.: Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012)
6. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.: Minimizing the two-round even-mansour cipher. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 39–56. Springer, Heidelberg (2014). http://eprint.iacr.org/2014/443
7. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014). http://eprint.iacr.org/2013/222
8. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking even-mansour ciphers. Full version of this paper. http://eprint.iacr.org/2015/539
9. Cogliati, B., Seurin, Y.: On the provable security of the iterated even-mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (2015). http://eprint.iacr.org/2015/069
10. Crowley, P.: Mercy: a fast large block cipher for disk sector encryption. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 49–63. Springer, Heidelberg (2001)
11. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
12. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: the even-mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer, Heidelberg (2012)
13. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Crypt. **10**(3), 151–162 (1997)
14. Farshim, P., Procter, G.: The related-key security of iterated even-mansour ciphers. In: Fast Software Encryption - FSE 2015 (2015, to appear). Full version available at http://eprint.iacr.org/2014/953
15. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The skein hash function family. SHA3 Submission to NIST (Round 3) (2010)
16. Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H.: On tweaking luby-rackoff blockciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 342–356. Springer, Heidelberg (2007)
17. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (2003)
18. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 292–304. Springer, Heidelberg (2004)
19. Hoang, V.T., Rogaway, P.: On generalized feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010)

20. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for block ciphers: the tweakey framework. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 274–288. Springer, Heidelberg (2014)
21. Lampe, R., Patarin, J., Seurin, Y.: An asymptotically tight security analysis of the iterated even-mansour cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 278–295. Springer, Heidelberg (2012)
22. Lampe, R., Seurin, Y.: How to construct an ideal cipher from a small set of public permutations. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 444–463. Springer, Heidelberg (2013). http://eprint.iacr.org/2013/255
23. Lampe, R., Seurin, Y.: Tweakable blockciphers with asymptotically optimal security. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 133–152. Springer, Heidelberg (2014)
24. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012). http://eprint.iacr.org/2012/450
25. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002)
26. Minematsu, K.: Beyond-birthday-bound security based on tweakable block cipher. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 308–326. Springer, Heidelberg (2009)
27. Mitsuda, A., Iwata, T.: Tweakable pseudorandom permutation from generalized feistel structure. In: Baek, J., Bao, F., Chen, K., Lai, X. (eds.) ProvSec 2008. LNCS, vol. 5324, pp. 22–37. Springer, Heidelberg (2008)
28. Morris, B., Rogaway, P., Stegers, T.: How to encipher messages on a small domain. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 286–302. Springer, Heidelberg (2009)
29. Nyberg, K., Knudsen, L.R.: Provable security against differential cryptanalysis. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 566–574. Springer, Heidelberg (1993)
30. Patarin, J.: The "Coefficients H" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009)
31. Procter, G.: A note on the CLRW2 tweakable block cipher construction. IACR Cryptology ePrint Archive, report 2014/111 (2014). http://eprint.iacr.org/2014/111
32. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004)
33. Rogaway, P., Bellare, M., Black, J.: OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. **6**(3), 365–403 (2003)
34. Rogaway, P., Zhang, H.: Online ciphers from tweakable blockciphers. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 237–249. Springer, Heidelberg (2011)
35. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher v1. Submission to the CAESAR competition (2014)
36. Schroeppel, R.: The hasty pudding cipher. AES submission to NIST (1998)
37. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 313–328. Springer, Heidelberg (1996)
38. Steinberger, J.: Improved security bounds for Key-alternating ciphers via Hellinger distance. IACR Cryptology ePrint Archive, report 2012/481 (2012). http://eprint.iacr.org/2012/481