Tweaking Even-Mansour Ciphers*

Benoît Cogliati**, Rodolphe Lampe***, and Yannick Seurin†

June 2, 2015

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

** University of Versailles, France. E-mail: benoitcogliati@hotmail.fr

*** University of Versailles, France. E-mail: rodolphe.lampe@gmail.com

† ANSSI, Paris, France. E-mail: yannick.seurin@m4x.org. This author was partially supported by the French National Agency of Research through the BLOC project (contract ANR-11-INS-011).

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 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, Rivest and Wagner [LRW02], and has proved to be very useful to construct various higher level cryptographic schemes such as (tweakable) length-preserving encryption modes [HR03, HR04], online ciphers [RZ11, ABL+13], message authentication codes [LRW02, LST12], and authenticated encryption modes [LRW02, RBB03, Rog04].

Tweakable block ciphers can be designed "from scratch" (e.g., the Hasty Pudding cipher [Sch98], Mercy [Cro00], or Threefish, the block cipher on which the Skein hash function [FLS+10] 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 [Min09]) 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 [LRW02]), 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 [LRW02] 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.* [LST12] 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 [LS13b] 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 [DR01]. 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

[1] A flaw was subsequently found in the original proof of [LST12] and patched by Procter [Pro14]. A different way of fixing the proof was proposed by Landecker *et al.*, see the revised version of [LST12].

P_i's are modeled as public random permutation 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 [EM97], 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.* [DKS12] 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.* [BKL+12], 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 [Ste12, LPS12], culminating with the proof by Chen and Steinberger [CS14] 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 [BKL+12]). 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 [ABM13], related-key attacks [CS15, FP15], and chosen-key attacks [CS15], as well as indifferentiability from an ideal cipher [ABD+13, LS13a].

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 [CS15]. 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 [BK03], so that there is no hope to improve 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

[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 [CS15] 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 [CS15].

$P_1, \ldots, P_r$. However, combining existing results for CLRW on one hand [LST12, LS13b], and for the iterated Even-Mansour cipher on the other hand [CS14], 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 [LRW02] and for the one-round single-key Even-Mansour cipher [EM97, DKS12] 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 Section 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

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

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 [LST12] 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 [Pat08], which was successfully applied to the analysis of the iterated Even-Mansour cipher [CS14, CLL+14], 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

[4] For $r > 2$, since the analysis of the CLRW construction in [LS13b] 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.

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 [LST12] for the two-round CLRW construction (our own bound matching Landecker *et al.*'s one [LST12] 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 [Pro14]. We explain how to "extract" from our work a H-coefficients proof for the two-round CLRW construction in Remark 1 at the end of Section 3.3.

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 [MRS09, HR10]. This part combines in a rather straightforward way the approach of [LPS12] (which applied the coupling technique to the iterated Even-Mansour cipher) and of [LS13b] (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.

Application to Related-Key Security. There are strong connections between tweakable block ciphers and the related-key security of traditional block ciphers [LRW02, BK03]. In particular, given any traditional block cipher $E : (\{0,1\}^n)^r \times \{0,1\}^n \to \{0,1\}^n$, one can for example construct a tweakable block cipher $\widetilde{E}$ with tweak space $\{0,1\}^n$ by letting

$$\widetilde{E}((k_1,\ldots,k_r),t,x) \stackrel{\text{def}}{=} E((k_1 \oplus t,\ldots,k_r \oplus t),x). \tag{5}$$

It can easily be seen that attacking $\widetilde{E}$ in the tweakable setting is *exactly* the same as attacking E in the related-key setting when the set of related-key deriving (RKD) functions is

$$\Phi^{r-\oplus} \stackrel{\text{def}}{=} \{(k_1,\ldots,k_r) \mapsto (k_1 \oplus t,\ldots,k_r \oplus t) : t \in \{0,1\}^n\}.^8$$

Based on this observation, we explain now how our results have immediate implications for the $\Phi^{r-\oplus}$-related-key security of the traditional (iterated) Even-Mansour cipher with a nonlinear key-schedule, which was previously analyzed (for one round) by Cogliati and Seurin [CS15]. First, consider the 1-round Even-Mansour construction

$$\mathsf{EM}^P(k,x) = f(k) \oplus P(f(k) \oplus x), \tag{6}$$

[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 [LST12] 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 [CS14], 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 6, getting a combinatorial lemma similar to [CS14, Lemma 1] that would allow to analyze good transcripts for any number of rounds in the tweakable setting seems more challenging.

[8] Note that for $r > 1$, this set of related-key deriving functions is more restrictive than the set $\Phi^{\oplus}$ that would allow to xor an arbitrary rn-bit string to the master key, not just a string of the form $(t,\ldots,t)$.

where f is some (fixed) permutation of $\{0,1\}^n$. Let

$$\delta(f) = \max_{a,b \in \{0,1\}^n, a \neq 0} |\{x \in \{0,1\}^n : f(x \oplus a) \oplus f(x) = b\}|,$$

which measures the nonlinearity of f (in particular, $\delta(f) = 2$ for a so-called *almost perfect nonlinear* permutation [NK92]). Applying transformation (5) to this construction yields the tweakable Even-Mansour construction

$$\mathsf{TEM}^P(k,t,x) = f(k \oplus t) \oplus P(f(k \oplus t) \oplus x), \tag{7}$$

a special case of construction (4) with $H_k(t) = f(k \oplus t)$. Clearly, this hash function family is uniform since f is a permutation, and one can easily check that it is ε-AXU for $\varepsilon = \delta(f)2^{-n}$. Hence, Theorem 1 of Section 3.2 applies and construction (7) is secure (in the tweakable setting) up to roughly $2^{n/2}$ adversarial queries (assuming $\delta(f)$ sufficiently small). Once translated in the language of related-key attacks, this is equivalent to saying that construction (6) is secure up to roughly $2^{n/2}$ adversarial queries against $\Phi^{\oplus}$-related-key attacks, which had already been proven in [CS15] (unsurprisingly, the bound of Theorem 1 in this paper exactly matches the one of [CS15, Theorem 3]). An even more general result for the 1-round Even-Mansour construction in the related-key setting was proved by Farshim and Procter [FP15, Theorem 2] (note that one of the examples of valid set of RKD functions given by Farshim and Procter at the end of Section 4.1 corresponds exactly to the multiplication-based hash function family considered in this paper).

The same considerations apply for larger number of rounds. For example, applying transformation (5) and Theorem 2 of Section 3.3 of this paper to the 2-round Even-Mansour construction

$$\mathsf{EM}^{P_1,P_2}((k_1,k_2),x) = f(k_2) \oplus P_2(f(k_2) \oplus f(k_1) \oplus P_1(f(k_1) \oplus x))$$

shows that it is secure against $\Phi^{2-\oplus}$-related-key attacks up to roughly $2^{2n/3}$ adversarial queries. This partially solves an open problem stated in [CS15], but falls short of yielding an Even-Mansour construction provably secure beyond the birthday bound against full-fledged $\Phi^{\oplus}$-related-key attacks.

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.* [GHL+07] 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 [MI08]. Our own work seems to be the first (besides [CS15], 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.* [JNP14], 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 [STA+14] (a candidate to the CAESAR

competition) to designate a permutation-based variant of Rogaway's XEX construction [Rog04]. 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 [CLL+14] 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.

Organization. We start by giving useful definitions and describing the security model in details in Section 2. In Section 3, we prove tight bounds for the one-round and the two-round TEM construction using the H-coefficients framework. In Section 4, we prove (non tight) asymptotic bounds as the number of rounds of the TEM construction grows using the coupling technique.

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 Figure 1):

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

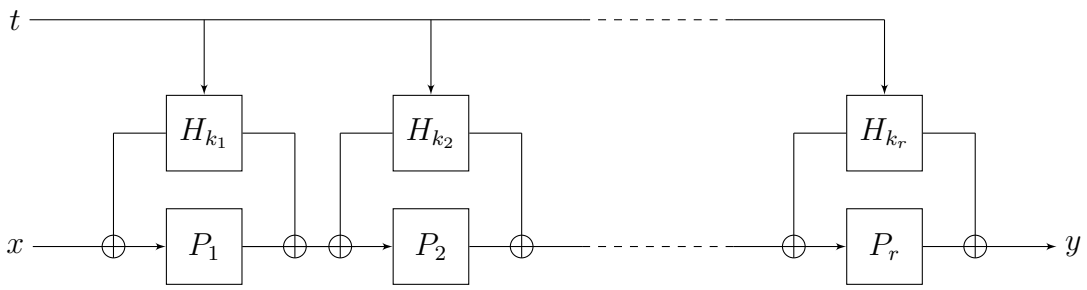

Fig. 1. The tweakable Even-Mansour construction with r rounds, based on public permutations $P_1, \ldots, P_r$ and a family of hash functions $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$.

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

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

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

$$\mathsf{TEM}^{\mathbf{P}}_{\mathbf{h}}(t,x) = h_r(t) \oplus P_r(h_r(t) \oplus h_{r-1}(t) \oplus P_{r-1}(h_{r-1}(t) \oplus \cdots \oplus h_1(t) \oplus P_1(h_1(t) \oplus x) \cdots))$$

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 $y \in \{0,1\}^n$,*

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

*$\mathcal{H}$ 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 [Sho96]. 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 $(\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}, \mathbf{P})$, 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 [LPS12], 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[9] and will only be useful as an intermediate step for the coupling-based security proof in Section 4.

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

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

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).

[9] 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.

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

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

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.

3 Tight Bounds for One and Two Rounds

3.1 The H-Coefficients Technique

We start by describing Patarin's H-coefficients technique [Pat08], 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 [CS14].

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. [CS14] 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. [CS14, CLL+14] 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*[10]

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

and that there exists ε_2 such that

$$\Pr[T_{\text{id}} \in \Theta_{\text{bad}}] \leq \varepsilon_2.$$

Then $\mathbf{Adv}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2$.

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

$$\Pr[P \leftarrow_{\$} \mathsf{P}(n) : P \vdash \mathcal{Q}] = \frac{1}{(N)_{q_p}}. \tag{8}$$

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

$$\Pr[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n) : \widetilde{P} \vdash \widetilde{\mathcal{Q}}] = \prod_{i=1}^{m} \frac{1}{(N)_{q_i}}. \tag{9}$$

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 (8) and (9), 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

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

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

Then we have

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = \mathsf{p}(\tau) \Big/ \prod_{i=1}^{m} \frac{1}{(N)_{q_i}} = \mathsf{p}(\tau) \cdot \prod_{i=1}^{m} (N)_{q_i}. \tag{10}$$

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

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

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*

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

The proof uses the H-coefficients technique that we exposed in Section 3.1, and serves as a good warm-up before the more complex two-round case. We start by defining bad transcripts.

Definition 1. We say that an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, h_1)$ is bad if one of the four following conditions is fulfilled:

(C-1) there exists distinct queries $(t, x, y), (t', x', y') \in \mathcal{Q}_C$ such that $h_1(t) \oplus h_1(t') = x \oplus x'$;
(C-2) there exists distinct queries $(t, x, y), (t', x', y') \in \mathcal{Q}_C$ such that $h_1(t) \oplus h_1(t') = y \oplus y'$;
(C-3) there exists $(t, x, y) \in \mathcal{Q}_C$ and $(u, v) \in \mathcal{Q}_{P_1}$ such that $x \oplus h_1(t) = u$;
(C-4) there exists $(t, x, y) \in \mathcal{Q}_C$ and $(u, v) \in \mathcal{Q}_{P_1}$ such that $y \oplus h_1(t) = v$.

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

We first upper bound the probability to get a bad transcript in the ideal world.

Lemma 2.

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

Proof. Let $(\mathcal{Q}_C, \mathcal{Q}_{P_1})$ be any attainable queries transcript. Recall that in the ideal world, the key h_1 is drawn at random from $\mathcal{H}$ independently from the queries transcript. Fix any pair of distinct queries (t, x, y) and $(t', x', y') \in \mathcal{Q}_C$. By the ε-AXU property of $\mathcal{H}$, we have

$$\Pr[h_1 \leftarrow_{\$} \mathcal{H} : h_1(t) \oplus h_1(t') = x \oplus x' \vee h_1(t) \oplus h_1(t') = y \oplus y'] \leq 2\varepsilon.$$

Note that this also holds when $t = t'$ since in that case necessarily $x \neq x'$ and $y \neq y'$ by the assumption that $\mathcal{D}$ never makes pointless queries. Hence, by summing over the $q_c(q_c - 1)/2$ possible pairs, the probability that condition (C-1) or (C-2) is fulfilled is at most $q_c^2 \varepsilon$.

Moreover, for each $(t, x, y) \in \mathcal{Q}_C$ and each $(u, v) \in \mathcal{Q}_{P_1}$, the probability over the random draw of h_1 that $h_1(t) = x \oplus u$ or $h_1(t) = y \oplus v$ is at most $2/N$ by the property of uniformity of $\mathcal{H}$. Hence, the probability that (C-3) or (C-4) is satisfied is at most $2 q_c q_p / N$. □

We then analyze good transcripts.

Lemma 3. *For any good transcript τ, one has*

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \geq 1.$$

Proof. Let τ be a good transcript. By (10), we need to lower bound

$$\mathsf{p}(\tau) \stackrel{\mathrm{def}}{=} \Pr[P_1 \leftarrow_{\$} \mathsf{P}(n) : \forall (t,x,y) \in \mathcal{Q}_C, P_1(x \oplus h_1(t)) = y \oplus h_1(t) \mid P_1 \vdash \mathcal{Q}_{P_1}].$$

Since τ is good, all values $x \oplus h_1(t)$ for $(t,x,y) \in \mathcal{Q}_C$ are distinct since otherwise τ would fulfill condition (C-1), and also distinct from all values u for $(u,v) \in \mathcal{Q}_{P_1}$ since otherwise τ would fulfill condition (C-3). Similarly, all values $y \oplus h_1(t)$ for $(t,x,y) \in \mathcal{Q}_C$ are distinct since otherwise τ would fulfill condition (C-2), and also distinct from all values v for $(u,v) \in \mathcal{Q}_{P_1}$ since otherwise τ would fulfill condition (C-4). This clearly implies that

$$\mathsf{p}(\tau) = \frac{1}{(N - q_p)_{q_c}},$$

so that by (10), we have

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = \frac{\prod_{i=1}^{m} (N)_{q_i}}{(N - q_p)_{q_c}} \geq \frac{(N)_{q_c}}{(N - q_p)_{q_c}} \geq 1. \qquad \square$$

Concluding. Theorem 1 now follows from Lemmas 1 (with $\varepsilon_1 = 0$), 2, and 3.

3.3 Security Proof for Two Rounds

3.3.1 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

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

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*

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

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.

3.3.2 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

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

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

$$\beta_1 = \sum_{\substack{u \in \{0,1\}^n : \\ |X_u| > 1}} |X_u|, \qquad \beta_2 = \sum_{\substack{v \in \{0,1\}^n : \\ |Y_v| > 1}} |Y_v|. \tag{11}$$

Definition 2. We say that an attainable transcript τ is bad if at least one of the following conditions is fulfilled (see Figure 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 4. *For any integers q_c and q_p, one has*

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

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,

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

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

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

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

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

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,

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

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

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

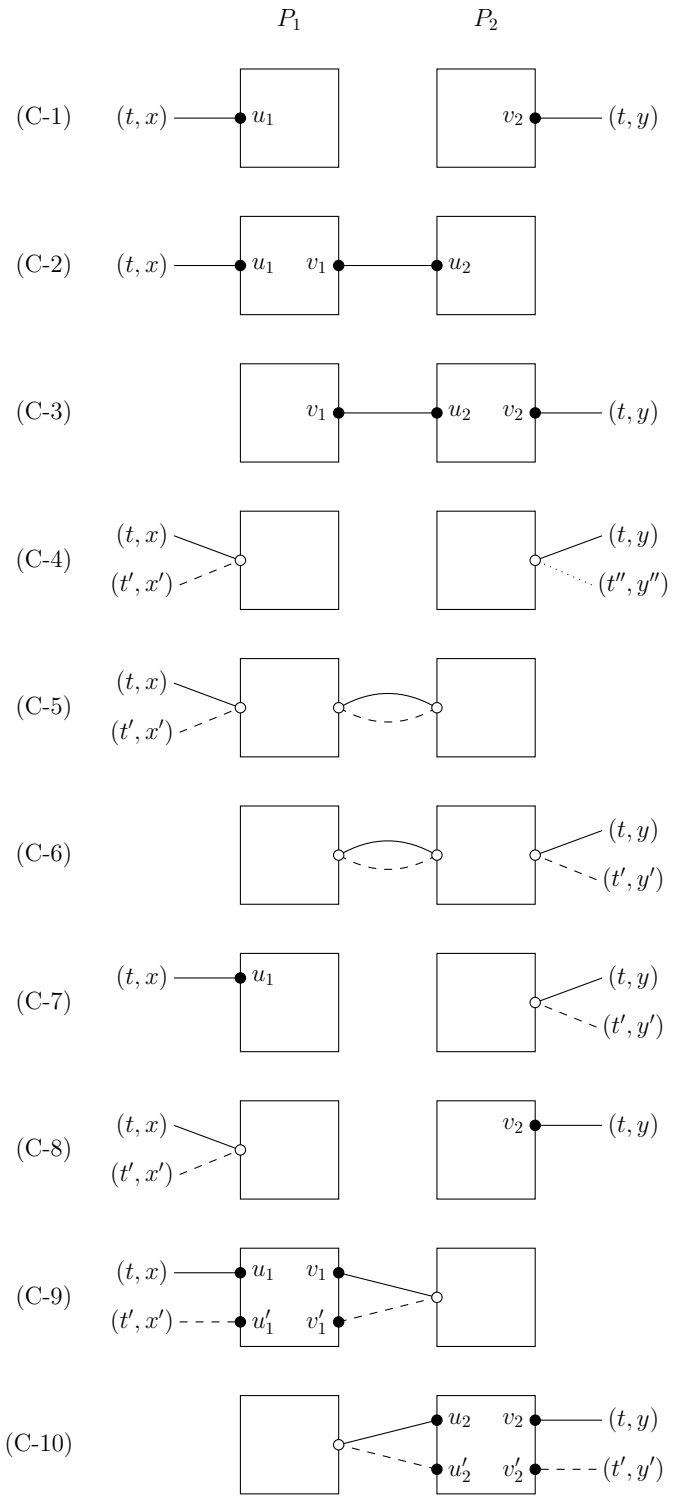

Fig. 2. The ten "collision" conditions characterizing a bad transcript. Black dots correspond to pairs $(u_1, v_1) \in \mathcal{Q}_{P_1}$ or $(u_2, v_2) \in \mathcal{Q}_{P_2}$. Note that for (C-4) one might have $(t', x') = (t'', x'')$, for (C-9) one might have $(u_1, v_1) = (u'_1, v'_1)$, and for (C-10)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

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,

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

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

$$\Pr\left[T_{\mathrm{id}} \in \Theta_5\right] \leq \frac{\varepsilon^2 q_c^2}{2}.$$

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,

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

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

$$\Pr[T_{\mathrm{id}} \in \Theta_7] \leq \frac{\varepsilon q_c^2 q_p}{2N}.$$

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

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

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,

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

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. □

3.3.3 Analysis of Good Transcripts

Next, we have to study good transcripts. The following technical lemma, adapted from [CLL+14], will be useful.

Lemma 5. *Let N, a, b, c be positive integers such that $a + b \leq N/2$ and $a + c \leq N/2$. Then*

$$\frac{(N)_a (N-b-c)_a}{(N-b)_a (N-c)_a} \geq 1 - \frac{4abc}{N^2}.$$

Proof. One has

$$\begin{aligned}
\frac{(N)_a(N-b-c)_a}{(N-b)_a(N-c)_a} &= \prod_{i=0}^{a-1} \frac{(N-i)(N-b-c-i)}{(N-b-i)(N-c-i)} \\
&= \prod_{i=0}^{a-1} \frac{N^2 - N(b+c+2i) + i(b+c+i)}{N^2 - N(b+c+2i) + i(b+c+i) + bc} \\
&= \prod_{i=0}^{a-1} \left(1 - \frac{bc}{N^2 - N(b+c+2i) + i(b+c+i) + bc}\right) \\
&= \prod_{i=0}^{a-1} \left(1 - \frac{bc}{(N-b-i)(N-c-i)}\right) \\
&\geq \prod_{i=0}^{a-1} \left(1 - \frac{bc}{(N-b-a)(N-c-a)}\right) \\
&\geq 1 - \frac{abc}{(N-b-a)(N-c-a)} \\
&\geq 1 - \frac{4abc}{N^2},
\end{aligned}$$

where for the last inequality we used $a + b \leq N/2$ and $a + c \leq N/2$. □

Lemma 6. *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. Let $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (h_1, h_2))$ be a good transcript. By (10), we have to lower bound

$$\mathsf{p}(\tau) \stackrel{\mathrm{def}}{=} \Pr\left[P_1, P_2 \leftarrow_{\$} \mathsf{P}(n) : \mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_C \middle| P_1 \vdash \mathcal{Q}_{P_1} \wedge P_2 \vdash \mathcal{Q}_{P_2}\right].$$

Notation. We will group the construction queries according to the type of collision they are involved in. Namely, we define (see also Figure 3 for a diagram of these sets of queries)

$$\begin{aligned}
\mathcal{Q}_{U_1} &= \{(t,x,y) \in \mathcal{Q}_C : x \oplus h_1(t) \in U_1\}, \\
\mathcal{Q}_{V_2} &= \{(t,x,y) \in \mathcal{Q}_C : y \oplus h_2(t) \in V_2\}, \\
\mathcal{Q}_X &= \{(t,x,y) \in \mathcal{Q}_C : |X_{x \oplus h_1(t)}| > 1 \text{ and } x \oplus h_1(t) \notin U_1\}, \\
\mathcal{Q}_Y &= \{(t,x,y) \in \mathcal{Q}_C : |Y_{y \oplus h_2(t)}| > 1 \text{ and } y \oplus h_2(t) \notin V_2\}, \\
\mathcal{Q}_0 &= \{(t,x,y) \in \mathcal{Q}_C : |X_{x \oplus h_1(t)}| = |Y_{y \oplus h_2(t)}| = 1,\ x \oplus h_1(t) \notin U_1, \text{ and } y \oplus h_2(t) \notin V_2\}.
\end{aligned}$$

Note that by definition, $|\mathcal{Q}_{U_1}| = \alpha_1$ and $|\mathcal{Q}_{V_2}| = \alpha_2$. Note also that these sets form a partition of $\mathcal{Q}_C$:

- $\mathcal{Q}_{U_1} \cap \mathcal{Q}_{V_2} = \emptyset$ since otherwise τ would satisfy (C-1),
- $\mathcal{Q}_{U_1} \cap \mathcal{Q}_Y = \emptyset$ since otherwise τ would satisfy (C-7),
- $\mathcal{Q}_{V_2} \cap \mathcal{Q}_X = \emptyset$ since otherwise τ would satisfy (C-8),

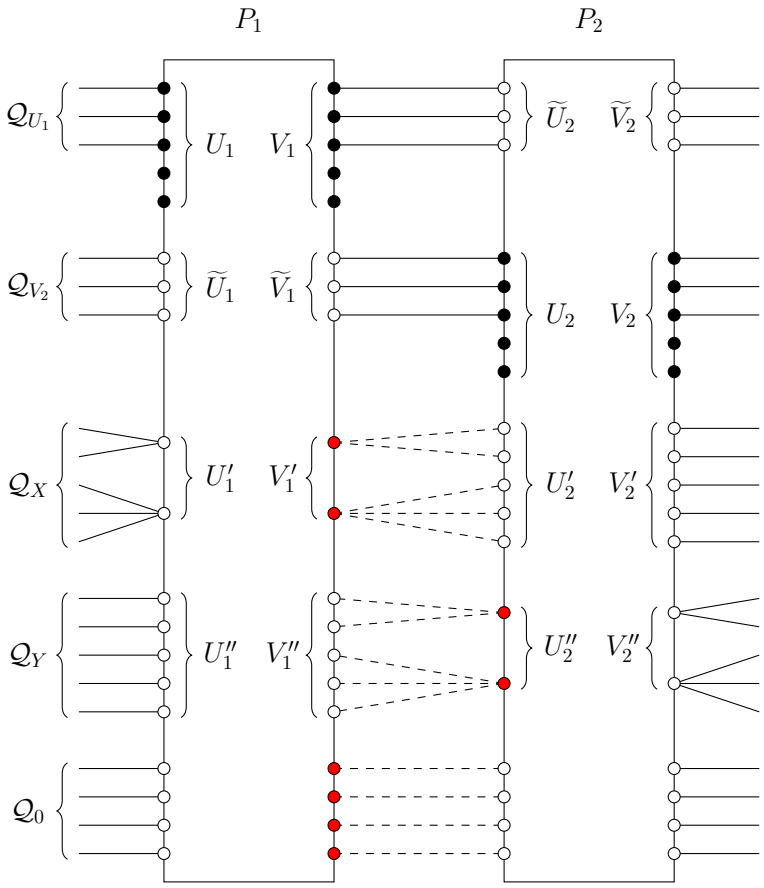

Fig. 3. Partition of the queries in $\mathcal{Q}_C$. Black dots correspond to values fixed by the internal permutation transcripts $\mathcal{Q}_{P_1}$ and $\mathcal{Q}_{P_2}$. Red dots correspond to values $(v'_{1,i})_{1\le i\le \alpha'_1}$, $(u''_{2,i})_{1\le i\le \alpha''_2}$, and $(\bar{v}_{1,i,j})_{1\le i\le m, 1\le j\le q'_i}$ over which we sum when lower bounding $\mathsf{p}''(\tau)$ in the proof of Lemma 6.

– $\mathcal{Q}_X \cap \mathcal{Q}_Y = \emptyset$ since otherwise τ would satisfy (C-4),
– $\mathcal{Q}_{U_1} \cap \mathcal{Q}_X = \mathcal{Q}_{U_1} \cap \mathcal{Q}_0 = \mathcal{Q}_{V_2} \cap \mathcal{Q}_Y = \mathcal{Q}_{V_2} \cap \mathcal{Q}_0 = \mathcal{Q}_X \cap \mathcal{Q}_0 = \mathcal{Q}_Y \cap \mathcal{Q}_0 = \emptyset$ by definition.

We denote respectively E_{U_1}, E_{V_2}, E_X, E_Y, and E_0 the event that $\mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_{U_1}$, $\mathcal{Q}_{V_2}$, $\mathcal{Q}_X$, $\mathcal{Q}_Y$, and $\mathcal{Q}_0$. Since the event $\mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_C$ is equivalent to $\mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2} \wedge \mathsf{E}_X \wedge \mathsf{E}_Y \wedge \mathsf{E}_0$, we have

$$\begin{aligned}\mathsf{p}(\tau) &= \Pr\left[\mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_C \middle| P_i \vdash \mathcal{Q}_{P_i}, i = 1,2\right] \\ &= \Pr\left[\mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2} \wedge \mathsf{E}_X \wedge \mathsf{E}_Y \wedge \mathsf{E}_0 | P_i \vdash \mathcal{Q}_{P_i}, i = 1,2\right] \\ &= \mathsf{p}'(\tau) \cdot \mathsf{p}''(\tau), \end{aligned} \tag{12}$$

where

$$\begin{aligned}\mathsf{p}'(\tau) &= \Pr\left[\mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2} | P_i \vdash \mathcal{Q}_{P_i}, i = 1,2\right] \\ \mathsf{p}''(\tau) &= \Pr\left[\mathsf{E}_X \wedge \mathsf{E}_Y \wedge \mathsf{E}_0 | \mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1,2)\right]\end{aligned}$$

and the probabilities are taken over the random choice of P_1 and P_2. We now lower bound $\mathsf{p}'(\tau)$ and $\mathsf{p}''(\tau)$ in turn.

Lower Bounding $\mathsf{p}'(\tau)$. Conditioned on $(P_i \vdash \mathcal{Q}_{P_i}, i = 1,2)$, P_1 and P_2 are fixed on exactly q_p values each. For each $(t,x,y) \in \mathcal{Q}_{U_1}$, there is a unique $(u_1, v_1) \in \mathcal{Q}_{P_1}$ such that $x \oplus h_1(t) = u_1$, so that $P_1(x \oplus h_1(t))$ is well defined (and equal to v_1). In the following, we let (see Figure 3)

$$\begin{aligned}\widetilde{U}_2 &= \{P_1(x \oplus h_1(t)) \oplus h_1(t) \oplus h_2(t) : (t,x,y) \in \mathcal{Q}_{U_1}\} \\ \widetilde{V}_2 &= \{y \oplus h_2(t) : (t,x,y) \in \mathcal{Q}_{U_1}\}.\end{aligned}$$

Note that all values defining $\widetilde{U}_2$ are distinct since otherwise τ would satisfy (C-9), and all values defining $\widetilde{V}_2$ are distinct since otherwise τ would satisfy (C-7). Moreover, note that U_2 and $\widetilde{U}_2$ are disjoint since otherwise τ would satisfy (C-2), and V_2 and $\widetilde{V}_2$ are disjoint since otherwise τ would satisfy (C-1). Hence, the event E_{U_1} is equivalent to α_1 "new" and distinct equations on P_2, so that

$$\Pr\left[\mathsf{E}_{U_1} | P_2 \vdash \mathcal{Q}_{P_2}\right] = \frac{1}{(N - q_p)_{\alpha_1}}. \tag{13}$$

Similarly, for each $(t,x,y) \in \mathcal{Q}_{V_2}$, there is a unique $(u_2, v_2) \in \mathcal{Q}_{P_2}$ such that $y \oplus h_2(t) = v_2$, so that $P_2^{-1}(y \oplus h_2(t))$ is well defined (and equal to u_2). In the following, we let (see Figure 3)

$$\begin{aligned}\widetilde{V}_1 &= \{P_2^{-1}(y \oplus h_2(t)) \oplus h_1(t) \oplus h_2(t) : (t,x,y) \in \mathcal{Q}_{V_2}\} \\ \widetilde{U}_1 &= \{x \oplus h_1(t) : (t,x,y) \in \mathcal{Q}_{V_2}\}.\end{aligned}$$

By a similar reasoning as above (viz., all values in $\widetilde{V}_1$, resp. $\widetilde{U}_1$, are distinct by (C-10), resp. (C-8), $V_1 \cap \widetilde{V}_1 = \emptyset$ by (C-3), and $U_1 \cap \widetilde{U}_1 = \emptyset$ by (C-1)), one has that E_{V_2} is equivalent to α_2 new and distinct equations on P_1. Hence,

$$\Pr\left[\mathsf{E}_{V_2} | P_1 \vdash \mathcal{Q}_{P_1}\right] = \frac{1}{(N - q_p)_{\alpha_2}}. \tag{14}$$

Combining (13) and (14), we obtain

$$\mathsf{p}'(\tau) = \frac{1}{(N - q_p)_{\alpha_1}(N - q_p)_{\alpha_2}}. \tag{15}$$

LOWER BOUNDING $\mathsf{p}''(\tau)$. Conditioned on $\mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1, 2)$, P_1 and P_2 are now fixed on respectively $q_p + \alpha_2$ and $q_p + \alpha_1$ values. Our goal is now to lower bound the number of possible "intermediate values" such that the event $\mathsf{E}_X \wedge \mathsf{E}_Y \wedge \mathsf{E}_0$ is equivalent to new and distinct equations on P_1 and P_2. We encourage the reader to refer to Figure 3 all along the counting.

We start with $\mathcal{Q}_X$. Let $U_1' = \{x \oplus h_1(t) : (t, x, y) \in \mathcal{Q}_X\}$ and $\alpha_1' = |U_1'|$. Note that

$$\alpha_1' \leq \sum_{\substack{u \in \{0,1\}^n: \\ |X_u|>1}} 1 \leq \sum_{\substack{u \in \{0,1\}^n: \\ |X_u|>1}} \frac{|X_u|}{2} = \frac{\beta_1}{2} \leq \frac{\sqrt{q_c}}{2}, \tag{16}$$

where the last inequality follows from the fact that τ does not satisfy (C-13). For clarity, we denote, using some arbitrary ordering,

$$U_1' = \{u_{1,1}', \ldots, u_{1,\alpha_1'}'\}.$$

Note that U_1' is disjoint from U_1 by definition of $\mathcal{Q}_X$, and disjoint from $\widetilde{U}_1$ since otherwise τ would satisfy (C-8).

On the other hand, note that all values $y \oplus h_2(t)$ for $(t, x, y) \in \mathcal{Q}_X$ are distinct since otherwise τ would satisfy (C-4). Let $V_2' = \{y \oplus h_2(t) : (t, x, y) \in \mathcal{Q}_X\}$ and $\alpha_2' = |V_2'| = |\mathcal{Q}_X|$. One has

$$\alpha_2' = \sum_{i=1}^{\alpha_1'} |X_{u_{1,i}'}| \leq \sum_{\substack{u \in \{0,1\}^n: \\ |X_u|>1}} |X_u| = \beta_1 \leq \sqrt{q_c}, \tag{17}$$

where the last inequality follows from the fact that τ does not satisfy (C-13). Note that V_2' is disjoint from V_2 since otherwise τ would satisfy (C-8), and disjoint from $\widetilde{V}_2$ by definition of $\mathcal{Q}_X$.

Let N_X be the number of tuples of distinct values $(v_{1,i}')_{1 \leq i \leq \alpha_1'}$ in $\{0,1\}^n \setminus (V_1 \cup \widetilde{V}_1)$ satisfying the following two conditions:

(i) for each i and each $(t, x, y) \in X_{u_{1,i}'}$, $v_{1,i}' \oplus h_1(t) \oplus h_2(t) \notin (U_2 \cup \widetilde{U}_2)$ (which excludes at most $(|U_2| + |\widetilde{U}_2|)|X_{u_{1,i}'}| = (q_p + \alpha_1)|X_{u_{1,i}'}|$ values for $v_{1,i}'$),

(ii) for each i and each $(t, x, y) \in X_{u_{1,i}'}$, $v_{1,i}' \oplus h_1(t) \oplus h_2(t)$ is distinct from any value $v_{1,j}' \oplus h_1(t') \oplus h_2(t')$, for $j < i$ and $(t', x', y') \in X_{u_{1,j}'}$ (which excludes at most $|X_{u_{1,i}'}| \cdot \sum_{j=1}^{i-1} |X_{u_{1,j}'}| \leq \alpha_2' |X_{u_{1,i}'}|$ values for $v_{1,i}'$).

Then, since $|\{0,1\}^n \setminus (V_1 \cup \widetilde{V}_1)| = N - q_p - \alpha_2$, one has

$$N_X \geq \prod_{i=1}^{\alpha_1'} \left(N - q_p - \alpha_2 - (i-1) - (q_p + \alpha_1 + \alpha_2')|X_{u_{1,i}'}| \right). \tag{18}$$

Note that for any tuple of values $(v_{1,i}')$ satisfying these conditions, the set of values $v_{1,i}' \oplus h_1(t) \oplus h_2(t)$ for $i = 1, \ldots, \alpha_1'$ and $(t, x, y) \in X_{u_{1,i}'}$ are all outside $U_2 \cup \widetilde{U}_2$ by condition (i), and all distinct by condition (ii) and the fact that τ does not satisfy (C-5). Hence, conditioned on $P_1(u_{1,i}') = v_{1,i}'$ for $i = 1, \ldots, \alpha_1'$, the event $\mathsf{TEM}_{(h_1,h_2)}^{P_1,P_2} \vdash \mathcal{Q}_X$ is equivalent to α_2' distinct and "new" equations on P_2.

From now on, we fix such a tuple of values $(v'_{1,i})$, and we let

$$V'_1 = \{v'_{1,1}, \ldots, v'_{1,\alpha'_1}\}$$
$$U'_2 = \{v'_{1,i} \oplus h_1(t) \oplus h_2(t) : i = 1, \ldots, \alpha'_1 \text{ and } (t,x,y) \in X_{u'_{1,i}}\}.$$

We then deal with queries in $\mathcal{Q}_Y$. Let $V''_2 = \{y \oplus h_2(t) : (t,x,y) \in \mathcal{Q}_V\}$ and $\alpha''_2 = |V''_2|$. Note that

$$\alpha''_2 \leq \sum_{\substack{v \in \{0,1\}^n: \\ |Y_v|>1}} 1 \leq \sum_{\substack{v \in \{0,1\}^n: \\ |Y_v|>1}} \frac{|Y_v|}{2} = \frac{\beta_2}{2} \leq \frac{\sqrt{q_c}}{2}, \tag{19}$$

where the last inequality follows from the fact that τ does not satisfy (C-14). For clarity, we denote, using some arbitrary ordering,

$$V''_2 = \{v''_{2,1}, \ldots, v''_{2,\alpha''_2}\}.$$

Note that V''_2 is disjoint from V_2 by definition of $\mathcal{Q}_Y$, disjoint from $\widetilde{V}_2$ since otherwise τ would satisfy (C-7), and disjoint from V'_2 since otherwise τ would satisfy (C-4).

On the other hand, note that all values $x \oplus h_1(t)$ for $(t,x,y) \in \mathcal{Q}_Y$ are distinct since otherwise τ would satisfy (C-4). Let $U''_1 = \{x \oplus h_1(t) : (t,x,y) \in \mathcal{Q}_Y\}$ and $\alpha''_1 = |U''_1| = |\mathcal{Q}_Y|$. One has

$$\alpha''_1 = \sum_{i=1}^{\alpha''_2} |Y_{v''_{2,i}}| \leq \sum_{\substack{v \in \{0,1\}^n: \\ |Y_v|>1}} |Y_v| = \beta_2 \leq \sqrt{q_c}, \tag{20}$$

where the last inequality follows from the fact that τ does not satisfy (C-14). Note that U''_1 is disjoint from U_1 since otherwise τ would satisfy (C-7), disjoint from $\widetilde{U}_1$ by definition of $\mathcal{Q}_Y$, and disjoint from U'_1 since otherwise τ would satisfy (C-4).

Let N_Y be the number of tuples of distinct values $(u''_{2,i})_{1 \leq i \leq \alpha''_2}$ in $\{0,1\}^n \setminus (U_2 \cup \widetilde{U}_2 \cup U'_2)$ satisfying the following two conditions:

(i) for each i and each $(t,x,y) \in Y_{v''_{2,i}}$, $u''_{2,i} \oplus h_1(t) \oplus h_2(t) \notin (V_1 \cup \widetilde{V}_1 \cup V'_1)$ (which excludes at most $(|V_1| + |\widetilde{V}_1| + |V'_1|)|Y_{v''_{2,i}}| = (q_p + \alpha_2 + \alpha'_1)|Y_{v''_{2,i}}|$ values for $u''_{2,i}$),

(ii) for each i and each $(t,x,y) \in Y_{v''_{2,i}}$, $u''_{2,i} \oplus h_1(t) \oplus h_2(t)$ is distinct from any value $u''_{2,j} \oplus h_1(t') \oplus h_2(t')$ for $j < i$ and $(t',x',y') \in Y_{v''_{2,j}}$ (which excludes at most $|Y_{v''_{2,i}}| \cdot \sum_{j=1}^{i-1} |Y_{v''_{2,j}}| \leq \alpha''_1 |Y_{v''_{2,i}}|$ values for $u''_{2,i}$).

Then, since $|\{0,1\}^n \setminus (U_2 \cup \widetilde{U}_2 \cup U'_2)| = N - q_p - \alpha_1 - \alpha'_2$, one has

$$N_Y \geq \prod_{i=1}^{\alpha''_2} \left(N - q_p - \alpha_1 - \alpha'_2 - (i-1) - (q_p + \alpha_2 + \alpha'_1 + \alpha''_1)|Y_{v''_{2,i}}|\right). \tag{21}$$

Note that for any tuple of values $(u''_{2,i})$ satisfying these conditions, the set of values $u''_{2,i} \oplus h_1(t) \oplus h_2(t)$ for $i = 1, \ldots, \alpha''_2$ and $(t,x,y) \in Y_{v''_{2,i}}$ are all outside $V_1 \cup \widetilde{V}_1 \cup V'_1$ by condition (i), and all distinct by condition (ii) and the fact that τ does not satisfy (C-6). Hence, conditioned on $P_2^{-1}(v''_{2,i}) = u''_{2,i}$ for $i = 1, \ldots, \alpha''_2$, the event $\mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_Y$ is equivalent to α''_1 distinct and "new" equations on P_1.

From now on, we fix such a tuple of values $(u''_{2,i})$, and we denote

$$U''_2 = \{u''_{2,1}, \ldots, u''_{2,\alpha''_2}\}$$
$$V''_1 = \{u''_{2,i} \oplus h_1(t) \oplus h_2(t) : i = 1, \ldots, \alpha''_2 \text{ and } (t,x,y) \in Y_{v''_{2,i}}\}.$$

It remains to handle queries in $\mathcal{Q}_0$. We let

$$q'_c = |\mathcal{Q}_0| = q_c - \alpha_1 - \alpha_2 - \alpha'_2 - \alpha''_1$$
$$q'_{p_1} = |U_1 \cup \widetilde{U}_1 \cup U'_1 \cup U''_1| = q_p + \alpha_2 + \alpha'_1 + \alpha''_1$$
$$q'_{p_2} = |V_2 \cup \widetilde{V}_2 \cup V'_2 \cup V''_2| = q_p + \alpha_1 + \alpha'_2 + \alpha''_2.$$

Recall that m denotes the number of distinct tweaks appearing in $\mathcal{Q}_C$. We denote $t_1, \ldots, t_m$ these tweaks (using some arbitrary order), and for $i = 1, \ldots, m$, we denote $\mathcal{Q}_{0,i}$ the subset of queries of $\mathcal{Q}_0$ whose tweak is t_i, and $q'_i = |\mathcal{Q}_{0,i}|$ (some of these subsets might be empty). Note that $\sum_{i=1}^m q'_i = q'_c$.

To ease the subsequent counting, we order queries in $\mathcal{Q}_0$ so that the first q'_1 queries correspond to tweak t_1, etc. Hence, we write

$$\mathcal{Q}_0 = \{(t_1, x_{1,1}, y_{1,1}), \ldots, (t_1, x_{1,q'_1}, y_{1,q'_1}), \ldots, (t_m, x_{m,1}, y_{m,1}), \ldots, (t_m, x_{m,q'_m}, y_{m,q'_m})\}.$$

For $i = 1, \ldots, m$ and $j = 1, \ldots, q'_i$, we let

$$\bar{u}_{1,i,j} = x_{i,j} \oplus h_1(t_i)$$
$$\bar{v}_{2,i,j} = y_{i,j} \oplus h_2(t_i).$$

Note that by definition of $\mathcal{Q}_0$, the $\bar{u}_{1,i,j}$'s are distinct and outside $U_1 \cup \widetilde{U}_1 \cup U'_1 \cup U''_1$, and the $\bar{v}_{2,i,j}$'s are distinct and outside $V_2 \cup \widetilde{V}_2 \cup V'_2 \cup V''_2$.

Let N_0 be the number of tuples of distinct values $(\bar{v}_{1,i,j})_{1 \le i \le m, 1 \le j \le q'_i}$ in $\{0,1\}^n \setminus (V_1 \cup \widetilde{V}_1 \cup V'_1 \cup V''_1)$ satisfying the following two conditions:

(i) for each (i,j), $\bar{v}_{1,i,j} \oplus h_1(t_i) \oplus h_2(t_i) \notin (U_2 \cup \widetilde{U}_2 \cup U'_2 \cup U''_2)$ (which excludes at most q'_{p_2} values for $\bar{v}_{1,i,j}$),

(ii) for each $i = 1, \ldots, m$ and $j = 1, \ldots, q'_i$, $\bar{v}_{1,i,j} \oplus h_1(t_i) \oplus h_2(t_i)$ is distinct from any value $\bar{v}_{1,k,\ell} \oplus h_1(t_k) \oplus h_2(t_k)$ for $k < i$ and $\ell = 1, \ldots, q'_k$ (which excludes at most $\sum_{k=1}^{i-1} q'_k$ values for $\bar{v}_{1,i,j}$).

Then, since $|\{0,1\}^n \setminus (V_1 \cup \widetilde{V}_1 \cup V'_1 \cup V''_1)| = N - q'_{p_1}$, and since $\bar{v}_{1,i,j}$ must also be chosen distinct from the $\sum_{k=1}^{i-1} q'_k + (j-1)$ previous values $\bar{v}_{1,k,\ell}$, $k < i$ and $\ell = 1, \ldots, q'_k$, and $\bar{v}_{1,i,\ell}$, $\ell < j$, one has

$$\begin{aligned} N_0 &\ge \prod_{i=1}^{m} \prod_{j=1}^{q'_i} \left(N - q'_{p_1} - q'_{p_2} - 2\sum_{k=1}^{i-1} q'_k - (j-1) \right) \\ &= \prod_{i=1}^{m} \left(N - q'_{p_1} - q'_{p_2} - 2\sum_{k=1}^{i-1} q'_k \right)_{q'_i}. \end{aligned} \tag{22}$$

For any tuple of values $(\bar{v}_{1,i,j})$ satisfying the above conditions, the set of values $\bar{v}_{1,i,j} \oplus h_1(t_i) \oplus h_2(t_i)$ for $i = 1, \ldots, m$ and $j = 1, \ldots, q'_i$ are all outside $U_2 \cup \widetilde{U}_2 \cup U'_2 \cup U''_2$ by condition (i),

and all distinct by condition (ii) and the obvious fact that for $i = 1, \ldots, m$, the q'_i values $\bar{v}_{1,i,j} \oplus h_1(t_i) \oplus h_2(t_i)$ $(1 \le j \le q'_i)$ are necessarily distinct since the $\bar{v}_{1,i,j}$'s are distinct. Hence, conditioned on P_1 satisfying the q'_c equation $P_1(\bar{u}_{1,i,j}) = \bar{v}_{1,i,j}$, the event $\mathsf{TEM}^{P_1,P_2}_{(h_1,h_2)} \vdash \mathcal{Q}_0$ is equivalent to q'_c distinct and "new" equations on P_2.

All in all, we have that for any of the (at least) $N_X \cdot N_Y \cdot N_0$ possible choices for the tuples $(v'_{1,i})_{1\le i\le \alpha'_1}$, $(u''_{2,i})_{1\le i\le \alpha''_2}$, and $(\bar{v}_{1,i,j})_{1\le i\le m, 1\le j\le q'_i}$ satisfying all conditions above (red dots on Figure 3), the event $\mathsf{E}_X \wedge \mathsf{E}_Y \wedge \mathsf{E}_0$ is equivalent to exactly $\alpha'_1 + \alpha''_1 + q'_c$ "new" equations on P_1 and exactly $\alpha'_2 + \alpha''_2 + q'_c$ "new" equations on P_2 (by new, we mean not imposed by $P_1 \vdash \mathcal{Q}_{P_1} \wedge P_2 \vdash \mathcal{Q}_{P_2} \wedge \mathsf{E}_{U_1} \wedge \mathsf{E}_{V_2}$). Hence, it follows that

$$\mathsf{p}''(\tau) \ge \frac{N_X \cdot N_Y \cdot N_0}{(N - q_p - \alpha_2)_{\alpha'_1+\alpha''_1+q'_c} (N - q_p - \alpha_1)_{\alpha'_2+\alpha''_2+q'_c}}. \tag{23}$$

Gathering (12), (15), and (23), we obtain

$$\mathsf{p}(\tau) \ge \frac{N_X \cdot N_Y \cdot N_0}{(N - q_p)_{\alpha_2+\alpha'_1+\alpha''_1+q'_c} (N - q_p)_{\alpha_1+\alpha'_2+\alpha''_2+q'_c}}. \tag{24}$$

Finally, combining (10) and (24), we arrive at

$$\begin{aligned}
\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} &\ge \frac{N_X \cdot N_Y \cdot N_0 \cdot \prod_{i=1}^m (N)_{q_i}}{(N - q_p)_{\alpha_2+\alpha'_1+\alpha''_1+q'_c} (N - q_p)_{\alpha_1+\alpha'_2+\alpha''_2+q'_c}} \\
&= \underbrace{\frac{N_X}{(N - q_p - \alpha_2)_{\alpha'_1}}}_{R_X} \times \underbrace{\frac{N_Y}{(N - q_p - \alpha_1 - \alpha'_2)_{\alpha''_2}}}_{R_Y} \times \underbrace{\frac{N_0 \cdot \prod_{i=1}^m (N)_{q'_i}}{(N - q'_{p_1})_{q'_c} (N - q'_{p_2})_{q'_c}}}_{R_0} \\
&\quad \times \underbrace{\frac{\prod_{i=1}^m (N)_{q_i}}{\prod_{i=1}^m (N)_{q'_i} (N - q_p)_{\alpha_2} (N - q_p - \alpha_2 - \alpha'_1)_{\alpha''_1} (N - q_p)_{\alpha_1+\alpha'_2}}}_{R'}.
\end{aligned}$$

It remains to lower bound R_X, R_Y, R_0, and R'. Injecting (18) in R_X, we have

$$\begin{aligned}
R_X &\ge \frac{\prod_{i=1}^{\alpha'_1} \left(N - q_p - \alpha_2 - (i-1) - (q_p + \alpha_1 + \alpha'_2)|X_{u'_{1,i}}|\right)}{(N - q_p - \alpha_2)_{\alpha'_1}} \\
&= \prod_{i=1}^{\alpha'_1} \left(1 - \frac{(q_p + \alpha_1 + \alpha'_2)|X_{u'_{1,i}}|}{N - q_p - \alpha_2 - (i-1)}\right) \\
&\ge 1 - \frac{(q_p + \alpha_1 + \alpha'_2) \sum_{i=1}^{\alpha'_1} |X_{u'_{1,i}}|}{N - q_p - \alpha_2 - \alpha'_1} \\
&= 1 - \frac{(q_p + \alpha_1 + \alpha'_2)\alpha'_2}{N - q_p - \alpha_2 - \alpha'_1} \\
&\ge 1 - \frac{2\sqrt{q_c}(q_p + 2\sqrt{q_c})}{N},
\end{aligned} \tag{25}$$

where for the last inequality we used that $\alpha_1 \le \sqrt{q_c}$ since τ is good, $\alpha'_2 \le \sqrt{q_c}$ by (17), and $q_p + \alpha_2 + \alpha'_1 \le q_p + 2q_c \le N/2$ by assumption.

Similarly, injecting (21) in R_Y, we have

$$\begin{aligned}
R_Y &\geq \frac{\prod_{i=1}^{\alpha_2''}(N-q_p-\alpha_1-\alpha_2'-(i-1)-(q_p+\alpha_2+\alpha_1'+\alpha_1'')|Y_{v_{2,i}''}|)}{(N-q_p-\alpha_1-\alpha_2')_{\alpha_2''}} \\
&= \prod_{i=1}^{\alpha_2''}\left(1-\frac{(q_p+\alpha_2+\alpha_1'+\alpha_1'')|Y_{v_{2,i}''}|}{N-q_p-\alpha_1-\alpha_2'-(i-1)}\right) \\
&\geq 1-\frac{(q_p+\alpha_2+\alpha_1'+\alpha_1'')\sum_{i=1}^{\alpha_2''}|Y_{v_{2,i}''}|}{N-q_p-\alpha_1-\alpha_2'-\alpha_2''} \\
&= 1-\frac{(q_p+\alpha_2+\alpha_1'+\alpha_1'')\alpha_1''}{N-q_p-\alpha_1-\alpha_2'-\alpha_2''} \\
&\geq 1-\frac{2\sqrt{q_c}(q_p+3\sqrt{q_c})}{N},
\end{aligned} \tag{26}$$

where for the last inequality we used that $\alpha_2 \leq \sqrt{q_c}$ since τ is good, $\alpha_1' \leq \sqrt{q_c}$ by (16), $\alpha_1'' \leq \sqrt{q_c}$ by (20), and $q_p+\alpha_1+\alpha_2'+\alpha_2'' \leq q_p+3q_c \leq N/2$ by assumption.

For R_0, using (22), we have

$$\begin{aligned}
R_0 &\geq \frac{\prod_{i=1}^{m}(N)_{q_i'}\left(N-q_{p_1}'-q_{p_2}'-2\sum_{k=1}^{i-1}q_k'\right)_{q_i'}}{(N-q_{p_1}')_{q_c'}(N-q_{p_2}')_{q_c'}} \\
&= \prod_{i=1}^{m}\frac{(N)_{q_i'}\left(N-q_{p_1}'-q_{p_2}'-2\sum_{k=1}^{i-1}q_k'\right)_{q_i'}}{\left(N-q_{p_1}'-\sum_{k=1}^{i-1}q_k'\right)_{q_i'}\left(N-q_{p_2}'-\sum_{k=1}^{i-1}q_k'\right)_{q_i'}} \\
&\geq \prod_{i=1}^{m}\left(1-\frac{4q_i'\left(q_{p_1}'+\sum_{k=1}^{i-1}q_k'\right)\left(q_{p_2}'+\sum_{k=1}^{i-1}q_k'\right)}{N^2}\right),
\end{aligned}$$

where for the last inequality we used Lemma 5 with $a=q_i'$, $b=q_{p_1}'+\sum_{k=1}^{i-1}q_k'$, and $c=q_{p_2}'+\sum_{k=1}^{i-1}q_k'$ (note that $a+b \leq q_c'+q_{p_1}' \leq q_c+q_p+\alpha_1' \leq q_p+2q_c \leq N/2$ by assumption, and similarly $a+c \leq N/2$).

Note that by definition of q_c', q_{p_1}', and q_{p_2}', one has

$$\begin{aligned}
q_{p_1}'+\sum_{k=1}^{i-1}q_k' &\leq q_{p_1}'+q_c' \leq q_p+q_c+\alpha_1' \leq q_p+2q_c \\
q_{p_2}'+\sum_{k=1}^{i-1}q_k' &\leq q_{p_2}'+q_c' \leq q_p+q_c+\alpha_2'' \leq q_p+2q_c
\end{aligned}$$

where we used inequalities (16) and (19), so that we finally arrive at

$$R_0 \geq 1-\frac{4q_c(q_p+2q_c)^2}{N^2}. \tag{27}$$

Finally, we have

$$\begin{aligned} R' &= \frac{\prod_{i=1}^{m}(N-q'_i)_{q_i-q'_i}}{(N-q_p)_{\alpha_2}(N-q_p-\alpha_2-\alpha'_1)_{\alpha''_1}(N-q_p)_{\alpha_1+\alpha'_2}} \\ &\geq \frac{\prod_{i=1}^{m}(N-q'_i)_{q_i-q'_i}}{N^{\alpha_1+\alpha_2+\alpha'_2+\alpha''_1}} \\ &\geq \frac{(N-q_c)^{\sum_{i=1}^{m} q_i-q'_i}}{N^{\alpha_1+\alpha_2+\alpha'_2+\alpha''_1}} \\ &= \frac{(N-q_c)^{q_c-q'_c}}{N^{\alpha_1+\alpha_2+\alpha'_2+\alpha''_1}} \\ &\geq 1-\frac{4q_c^{3/2}}{N}, \end{aligned} \tag{28}$$

where we used that

$$q_c - q'_c = \alpha_1 + \alpha_2 + \alpha'_2 + \alpha''_1 \leq 4\sqrt{q_c}.$$

Collecting (25), (26), (27), and (28) concludes the proof. □

3.3.4 Concluding the Proof of Theorem 2

We are now ready to prove Theorem 2. Combining Lemmas 1, 4, and 6, one has

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

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

Remark 1. We quickly explain how to derive a H-coefficients proof for the two-round CLRW construction [LST12, Pro14] from the proof of Theorem 2. First, since in the CLRW setting, the inner permutations are secret, one can drop from the definition of bad transcripts all conditions involving queries to P_1 and P_2. This leaves us with conditions (C-4,5,6) and (C-13,14). It can be checked that the probability of these conditions can be upper bounded without appealing to the uniformity of the function family $\mathcal{H}$, and that the probability to get a bad transcript in the ideal world boils down to $2\varepsilon^2 q_c^3 + 2\varepsilon q_c^{3/2}$. For the analysis of good transcripts (Lemma 6), one has $\mathcal{Q}_{U_1} = \mathcal{Q}_{V_2} = \emptyset$, so that only the lower bound on $\mathsf{p}''(\tau)$ matters. It can then be checked that letting $q_p = 0$ in the lower bound of Lemma 6 yields the result. This gives the security bound for the two-round CLRW construction with a perfect block cipher, which can be turned into a corresponding result for a concrete block cipher (with a non-zero PRP distinguishing advantage) through a standard hybrid argument.

4 Asymptotic Bounds via the Coupling Technique

4.1 Preliminaries and Notation

Fix an integer $q \leq N$. Given a tuple $\mathbf{t} = (t_1, \ldots, t_q) \in \mathcal{T}^q$, we will denote $\Omega_{\mathbf{t}} \subset (\{0,1\}^n)^q$ the set of possible inputs $\mathbf{x} = (x_1, \ldots, x_q) \in (\{0,1\}^n)^q$ such that all pairs (t_i, x_i) are pairwise distinct, i.e.,

$$\Omega_{\mathbf{t}} = \{\mathbf{x} := (x_1, \ldots, x_q) \in (\{0,1\}^n)^q : \forall i \neq j, (x_i, t_i) \neq (x_j, t_j)\}\,.$$

Given a finite event space Ω and two probability distributions μ and ν defined on Ω, the *statistical distance* (or total variation distance) between μ and ν, denoted $\|\mu - \nu\|$ is defined as:

$$\|\mu - \nu\| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)|.$$

The following definitions can easily be seen equivalent:

$$\|\mu - \nu\| = \max_{S \subset \Omega} \{\mu(S) - \nu(S)\} = \max_{S \subset \Omega} \{\nu(S) - \mu(S)\} = \max_{S \subset \Omega} \{|\mu(S) - \nu(S)|\}\,.$$

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that for all $x \in \Omega$, $\sum_{y \in \Omega} \lambda(x, y) = \mu(x)$ and for all $y \in \Omega$, $\sum_{x \in \Omega} \lambda(x, y) = \nu(y)$. In other words, λ is a joint distribution whose marginal distributions are resp. μ and ν. The fundamental result of the coupling technique is the following one. See e.g. [LPS12, LS13b] for a proof.

Lemma 7 (Coupling Lemma). *Let μ and ν be probability distributions on a finite event space Ω, let λ be a coupling of μ and ν, and let $(X, Y) \sim \lambda$ (i.e., (X, Y) is a random variable sampled according to distribution λ). Then $\|\mu - \nu\| \leq \Pr[X \neq Y]$.*

For the analysis of CCA attacks, we will rely on the following lemma (see [LPS12] for a proof).

Lemma 8. *Let Ω be some finite event space and μ^* be the uniform probability distribution on Ω. Let μ be a probability distribution on Ω such that $\|\mu - \mu^*\| \leq \varepsilon$. Then there is a set $S \subset \Omega$ such that:*

- $|S| \geq (1 - \sqrt{\varepsilon})|\Omega|$,
- $\forall x \in S$, $\mu(x) \geq (1 - \sqrt{\varepsilon})\mu^*(x)$.

4.2 Security Analysis for Non-Adaptive Adversaries

We first deal with non-adaptive chosen-plaintext (NCPA) adversaries. Using a coupling argument, we will prove the following theorem.

Theorem 3. *Let n, r, q_c, q_p be positive integers and $\mathcal{H}$ be an ε-AXU and uniform family of functions from some set $\mathcal{T}$ to $\{0,1\}^n$. Then one has:*

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

Using an ε-AXU function family with $\varepsilon \simeq 2^{-n}$, one can see that the construction ensures security up to approximately $2^{\frac{rn}{r+1}}$ queries against NCPA-adversaries.

The crucial point of the proof will be to upper bound the statistical distance between the distribution of the outputs of the tweakable Even-Mansour cipher *conditioned on partial information on the inner permutations* (namely $P_i \vdash \mathcal{Q}_{P_i}$ for $i = 1, \ldots, r$) and the uniform distribution on $\Omega_{\mathbf{t}}$. We introduce the following important definitions and notations.

Let q_c, q_p be positive integers, and fix a (q_c, q_p)-NCPA-distinguisher $\mathcal{D}$. Such a distinguisher first queries the inner permutations $(P_1, \ldots, P_r)$. Let $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ be the resulting transcript. We say that a transcript $\mathcal{Q}_{\mathbf{P}}$ is *attainable* if there exists a tuple of permutations $\mathbf{P}$ such that the interaction of $\mathcal{D}$ with $\mathbf{P}$ results in $\mathcal{Q}_{\mathbf{P}}$. Recall that we denote $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$ the event $\wedge_{i=1}^{r}(P_i \vdash \mathcal{Q}_{P_i})$.

Definition 3. Fix any attainable queries transcript $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ resulting from the adaptive interaction of the distinguisher with the inner permutations during the first phase of the attack. For $\mathbf{t} = (t_1, \ldots, t_{q_c}) \in \mathcal{T}^{q_c}$ and $\mathbf{x} = (x_1, \ldots, x_{q_c}) \in \Omega_{\mathbf{t}}$, we denote $\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}}$ the distribution of the tuple

$$\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}(\mathbf{t}, \mathbf{x}) \stackrel{\text{def}}{=} \left(\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}(t_1, x_1), \ldots, \mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}(t_{q_c}, x_{q_c})\right)$$

conditioned on the event $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$ (i.e., when the key $\mathbf{k} = (k_1, \ldots, k_r)$ is uniformly random and the permutations $\mathbf{P} = (P_1, \ldots, P_r)$ are uniformly random among permutations satisfying $\wedge_{i=1}^{r}(P_i \vdash \mathcal{Q}_{P_i})$). We also denote $\mu_{\mathbf{t}}^{*}$ the uniform distribution on $\Omega_{\mathbf{t}}$. $\lozenge$

The following lemma states that the advantage of a NCPA-distinguisher is upper bounded by the maximum over every tuple of values $\mathbf{t} \in \mathcal{T}^{q_c}$ and $\mathbf{x} \in \Omega_{\mathbf{t}}$ of the total variation distance between $\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}}$ and $\mu_{\mathbf{t}}^{*}$. This is a straightforward extension of [LPS12, Lemma 4].

Lemma 9. *Let q_c, q_p be positive integers. Assume that there exists α such that for any attainable queries transcript from the first phase of the attack $\mathcal{Q}_{\mathbf{P}}$ and every $\mathbf{t} \in \mathcal{T}^{q_c}, \mathbf{x} \in \Omega_{\mathbf{t}}$, one has*

$$\|\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}} - \mu_{\mathbf{t}}^{*}\| \leq \alpha.$$

Then $\mathbf{Adv}_{\mathsf{TEM}[n,r,\mathcal{H}]}^{\text{ncpa}}(q_c, q_p) \leq \alpha$.

Proof. Fix a (q_c, q_p)-NCPA-distinguisher $\mathcal{D}$. Let $\mathcal{Q}_{\mathbf{P}}$ be the transcript of the interaction of $\mathcal{D}$ with the inner permutations during the first phase of the attack. We denote Γ the set of attainable transcripts. The number of attainable transcripts is exactly

$$|\Gamma| = ((N)_{q_p})^r. \tag{29}$$

This can be easily seen as follows. The first query of $\mathcal{D}$ is fixed in all executions. Assume *wlog* that this is a query to P_1. There are exactly N possible answers. The next query is determined by the answer received to the first query. If this is again a query to P_1, there are now $N-1$ possible answers, whereas if this a query to P_i, $i \neq 1$, there are N possible answers. This can be easily extended by induction to obtain the above claim.

The tuples of non-adaptive queries $((t_1, x_1), \ldots, (t_{q_c}, x_{q_c}))$ of $\mathcal{D}$ to the construction oracle is a deterministic function of the transcript $\mathcal{Q}_{\mathbf{P}}$ of the first phase of the attack. Denote $\mathbf{t}(\mathcal{Q}_{\mathbf{P}}) = (t_1, \ldots, t_{q_c})$ and $\mathbf{x}(\mathcal{Q}_{\mathbf{P}}) = (x_1, \ldots, x_{q_c})$. The output of $\mathcal{D}$ is then a deterministic

function of $\mathcal{Q}_{\mathbf{P}}$ and the answers $\mathbf{y} = (y_1, \ldots, y_{q_c})$ received from the construction oracle to the tuple of queries $((t_1, x_1), \ldots, (t_{q_c}, x_{q_c}))$. For any attainable transcript $\mathcal{Q}_{\mathbf{P}}$, we denote $\Sigma_{\mathcal{Q}_{\mathbf{P}}}$ the set of tuples $\mathbf{y}$ such that $\mathcal{D}$ outputs 1 when receiving answers $\mathbf{y}$ to its queries to the construction oracle. Denote

$$\mathsf{p}_{\mathrm{id}} = \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n), \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathcal{D}^{\widetilde{P},\mathbf{P}} = 1\right]$$
$$\mathsf{p}_{\mathrm{re}} = \Pr\left[\mathbf{k} \leftarrow_{\$} \mathcal{K}^r, \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathcal{D}^{\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}},\mathbf{P}} = 1\right].$$

Then, by definition, we have

$$\begin{aligned}
\mathsf{p}_{\mathrm{id}} &= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \sum_{\mathbf{y} \in \Sigma_{\mathcal{Q}_{\mathbf{P}}}} \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n), \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}} \wedge \widetilde{P}(\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}})) = \mathbf{y}\right] \\
&= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \sum_{\mathbf{y} \in \Sigma_{\mathcal{Q}_{\mathbf{P}}}} \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n) : \widetilde{P}(\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}})) = \mathbf{y}\right] \cdot \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \\
&= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \cdot \mu^*_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}})}(\Sigma_{\mathcal{Q}_{\mathbf{P}}}). \qquad (30)
\end{aligned}$$

Also, we have:

$$\begin{aligned}
\mathsf{p}_{\mathrm{re}} &= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \sum_{\mathbf{y} \in \Sigma_{\mathcal{Q}_{\mathbf{P}}}} \Pr\left[\mathbf{k} \leftarrow_{\$} \mathcal{K}^r, \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}} \wedge \mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}})) = \mathbf{y}\right] \\
&= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \sum_{\mathbf{y} \in \Sigma_{\mathcal{Q}_{\mathbf{P}}}} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \cdot \mu_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}}), \mathcal{Q}_{\mathbf{P}}}(\mathbf{y}) \\
&= \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \cdot \mu_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}}), \mathcal{Q}_{\mathbf{P}}}(\Sigma_{\mathcal{Q}_{\mathbf{P}}}). \qquad (31)
\end{aligned}$$

By definition and using (30) and (31), one has

$$\begin{aligned}
\mathbf{Adv}(\mathcal{D}) &= |\mathsf{p}_{\mathrm{id}} - \mathsf{p}_{\mathrm{re}}| \\
&\leq \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \cdot \left|\mu^*_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}})}(\Sigma_{\mathcal{Q}_{\mathbf{P}}}) - \mu_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}}), \mathcal{Q}_{\mathbf{P}}}(\Sigma_{\mathcal{Q}_{\mathbf{P}}})\right| \\
&\leq \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \cdot \|\mu^*_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}})} - \mu_{\mathbf{t}(\mathcal{Q}_{\mathbf{P}}), \mathbf{x}(\mathcal{Q}_{\mathbf{P}}), \mathcal{Q}_{\mathbf{P}}}\| \\
&\leq \alpha \sum_{\mathcal{Q}_{\mathbf{P}} \in \Gamma} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}\right] \\
&\leq \alpha,
\end{aligned}$$

where for the last inequality we used $\Pr[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^r : \mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] = \frac{1}{((N)_{q_p})^r} = \frac{1}{|\Gamma|}$. □

We will now establish an appropriate upper bound α for $\|\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}} - \mu^*_{\mathbf{t}}\|$ as required to apply Lemma 9.

Lemma 10. *Let q_c, q_p be positive integers. Fix any attainable queries transcript of the first phase of the attack $\mathcal{Q}_{\mathbf{P}}$ and any $\mathbf{t} \in \mathcal{T}^{q_c}, \mathbf{x} \in \Omega_{\mathbf{t}}$. Then:*

$$\|\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}} - \mu^*_{\mathbf{t}}\| \leq q_c \left(2q_c\varepsilon + \frac{2q_p}{N}\right)^r.$$

Proof. Fix any attainable queries transcript $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ and $\mathbf{t} \in \mathcal{T}^{q_c}, \mathbf{x} \in \Omega_{\mathbf{t}}$, with $\mathbf{t} = (t_1, \ldots, t_{q_c})$ and $\mathbf{x} = (x_1, \ldots, x_{q_c})$. For each $l \in \{0, \ldots, q_c\}$, let $\mathbf{z} = (z_1, \ldots, z_{q_c})$ be a tuple of queries such that $z_i = x_i$ for $i \leq l$, and z_i is uniformly random in $\{0,1\}^n \setminus \{z_j | t_j = t_i, j < i\}$ for $i > l$. Denote ν_l the distribution of $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(\mathbf{t}, \mathbf{z})$, conditioned on $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$. Note that $\nu_0 = \mu^*_{\mathbf{t}}$ since for $l = 0$ the tuple of inputs is uniformly random in $\Omega_{\mathbf{t}}$, and $\nu_{q_c} = \mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}}$. Hence we have:

$$\|\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}}} - \mu^*_{\mathbf{t}}\| = \|\nu_{q_c} - \nu_0\| \leq \sum_{l=0}^{q_c-1} \|\nu_{l+1} - \nu_l\|. \tag{32}$$

There still remains to upper bound the total variation distance between ν_{l+1} and ν_l, for each $l \in \{0, \ldots, q_c - 1\}$. For this, we will construct a suitable coupling of the two distributions. Note that we only have to consider the first $l+1$ elements of the two tuples of outputs since for both distributions, the i-th inputs for $i > l+1$ are sampled at random. In other words, $\|\nu_{l+1} - \nu_l\| = \|\nu'_{l+1} - \nu'_l\|$, where ν'_{l+1} and ν'_l are the respective distributions of the $l+1$ first outputs of the cipher. To define the coupling of ν'_{l+1} and ν'_l, we consider the tweakable Even-Mansour cipher $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}$, where $\mathbf{P}$ satisfies $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$, that receives inputs $\mathbf{x}' = (x_1, \ldots, x_{l+1})$ and $\mathbf{t}' = (t_1, \ldots, t_{l+1})$, so that $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(\mathbf{t}', \mathbf{x}')$ is distributed according to ν'_{l+1}. We will construct a second tweakable Even-Mansour cipher $\mathsf{TEM}^{\mathbf{P}'}_{\mathbf{k}'}$, with inputs $\mathbf{z}' = (z_1, \ldots, z_{l+1})$ and $\mathbf{t}' = (t_1, \ldots, t_{l+1})$, satisfying the following properties:

(i) $z_i = x_i$ for $i = 1, \ldots, l$, and z_{l+1} is uniformly random in $\{0,1\}^n \setminus \{x_j | t_j = t_i, j < i\}$;
(ii) for $i = 1, \ldots, l+1$, if the outputs of the j-th inner permutation in the computations of $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(t_i, x_i)$ and $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}'}(t_i, z_i)$ are equal, then this also holds for any subsequent inner permutation;
(iii) $\mathbf{P}'$ is uniformly random among permutation tuples satisfying $\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}$ and $\mathbf{k}'$ is uniformly random in $\mathcal{K}^r$.

Note that the same tweaks are used for both ciphers. Properties (i) and (iii) will ensure that $\mathsf{TEM}^{\mathbf{P}'}_{\mathbf{k}'}(\mathbf{t}', \mathbf{z}')$ is distributed according to ν'_l. We stress that $(\mathbf{P}', \mathbf{k}')$ will *not* be independent from $(\mathbf{P}, \mathbf{k})$, however this is not required for the Coupling Lemma to apply. The only requirement is that both $(\mathbf{P}, \mathbf{k})$ and $(\mathbf{P}', \mathbf{k}')$ have the correct marginal distribution.

NOTATION. For $i = 1, \ldots, r$, we denote

$$U_i = \{u_i | (u_i, v_i) \in \mathcal{Q}_{P_i}\},$$
$$V_i = \{v_i | (u_i, v_i) \in \mathcal{Q}_{P_i}\}.$$

For $i = 1, \ldots, l+1$ and $j = 1, \ldots, r$, we also define x_i^j as the output of the j-th round when computing $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(t_i, x_i)$, and similarly z_i^j as the output of the j-th round when computing $\mathsf{TEM}^{\mathbf{P}'}_{\mathbf{k}'}(t_i, z_i)$, i.e.,

$$\begin{cases} x_i^0 = x_i, \\ z_i^0 = z_i, \\ x_i^j = H_{k_j}(t_i) \oplus P_j(H_{k_j}(t_i) \oplus x_i^{j-1}), \\ z_i^j = H_{k'_j}(t_i) \oplus P'_j(H_{k'_j}(t_i) \oplus z_i^{j-1}). \end{cases} \tag{33}$$

We now describe how the second iterated Even-Mansour cipher is constructed. First, it uses the same keys as the original one, namely $\mathbf{k}' = \mathbf{k} = (k_1, \ldots, k_r)$. In order to construct permutations $\mathbf{P}'$ (on points encountered when computing $\mathsf{TEM}^{\mathbf{P}'}_{\mathbf{k}}(\mathbf{t}', \mathbf{z}')$), we compare the computations of $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(t_i, x_i)$ and $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}(t_i, z_i)$ for $i = 1, \ldots, l+1$.

Coupling of the first l queries. For every $i \leq l$, the i-th queries x_i^0 and z_i^0 are equal by definition. Considering the system (33), we set $P'_{j+1}(x_i^j \oplus H_{k_{j+1}}(t_i)) = P_{j+1}(x_i^j \oplus H_{k_{j+1}}(t_i))$ for every $i \leq l$ and $i < r$. This implies that the first l outputs $(x_1^r, \ldots, x_l^r)$ and $(z_1^r, \ldots, z_l^r)$ are equal.

Coupling of the $(l+1)$-th query. For every $j = 0, \ldots, r-1$ we define the coupling for the $l+1$-th query as follows:

(1) if $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \in U_{j+1}$ or there exists $i \leq l$ such that $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = z_i^j \oplus H_{k_{j+1}}(t_i)$, then $P'_{j+1}(H_{k_{j+1}}(t_{l+1}) \oplus z_{l+1}^j)$ is already determined; unless we have coupled z_{l+1}^j and x_{l+1}^j at a previous round, we cannot do it at this round;
(2) if $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \notin U_{j+1}$ and $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \neq z_i^j \oplus H_{k_{j+1}}(t_i)$ for $i \leq l$, then:
   (a) if $x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \in U_{j+1}$ or there exists $i \leq l$ such that $x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = x_i^j \oplus H_{k_{j+1}}(t_i)$, then we choose $P'_{j+1}(z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}))$ uniformly at random in $\{0,1\}^n \setminus (V_{j+1} \cup \{P'_{j+1}(z_i^j \oplus H_{k_{j+1}}(t_i)), i \leq l\})$ and we cannot couple z_{l+1}^{j+1} and x_{l+1}^{j+1} at this round;
   (b) else we define $P'_{j+1}(z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1})) = P_{j+1}(x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}))$, thus $z_{l+1}^{j+1} = x_{l+1}^{j+1}$.

Property (ii) can easily be seen to follow from these rules and the fact that the keys and the tweaks are the same for both ciphers.

Checking that $(\mathbf{P}', \mathbf{k}')$ is uniformly random. Since we set $\mathbf{k}' = \mathbf{k}$ and $\mathbf{k}$ is uniformly random, so is $\mathbf{k}'$. During the coupling of the first l queries, we set $P'_j(x_i^{j-1} \oplus H_{k_j}(t_i)) = P_j(x_i^{j-1} \oplus H_{k_j}(t_i))$ for every $i \leq l$ and $1 \leq j \leq r$; $P_j(x_i^{j-1} \oplus H_{k_j}(t_i))$ is uniformly random among possible values thus so is $P'_j(x_i^{j-1} \oplus H_{k_j}(t_i))$. Rule (1) says that if there is a collision with a previous input of P'_j, we cannot choose the value of $P'_j(z_{l+1}^{j-1} \oplus H_{k_j}(t_i))$ so this does not change anything to the distribution of P'_j. When conditions of rule (2)(a) are met, we have:

– for some $i \leq l$:

$$\begin{cases} P_j(x_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1})) = P_j(x_i^{j-1} \oplus H_{k_j}(t_i)) = P'_j(z_i^{j-1} \oplus H_{k_j}(t_i)) \\ z_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}) \neq z_i^{j-1} \oplus H_{k_j}(t_i), \end{cases}$$

– or for some $(u_j, v_j) \in \mathcal{Q}_{P_j}$:

$$\begin{cases} P_j(x_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1})) = P_j(u_j) = P'_j(u_j) \\ z_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}) \neq u_j. \end{cases}$$

Both implies that $P'_j(z_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1})) \neq P_j(x_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}))$. This means that the coupling is impossible and we choose $P'_j(z_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}))$ uniformly at random among possible values to keep P'_j uniformly distributed. Finally, when conditions of rule (2)(b) are met, we have no problem to couple: $P_j(x_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}))$ and $P'_j(z_{l+1}^{j-1} \oplus H_{k_j}(t_{l+1}))$ are both uniformly random among possible values. In conclusion, the permutations P'_j are uniformly random and independent as wanted, so that $(z_1^r, \ldots, z_{l+1}^r)$ is distributed according to ν'_l.

Failure Probability of the Coupling. There remains to upper bound the probability that the coupling fails, i.e.,

$$(z_1^r, \ldots, z_{l+1}^r) \neq (x_1^r, \ldots, x_{l+1}^r).$$

For every $j \in \{0, \ldots, r-1\}$, we denote F_j the event that $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \in U_{j+1}$ or $x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) \in U_{j+1}$ or there exists $i \leq l$ such that $z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = z_i^j \oplus H_{k_{j+1}}(t_i)$ or $x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = x_i^j \oplus H_{k_{j+1}}(t_i)$. This is the event of failing to couple at round $j+1$. Then we have:

$$\begin{aligned}
\Pr[F_j] &\leq \sum_{i \leq l} \Pr[z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = z_i^j \oplus H_{k_{j+1}}(t_i)] \\
&\quad + \sum_{i \leq l} \Pr[x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = x_i^j \oplus H_{k_{j+1}}(t_i)] \\
&\quad + \sum_{u_{j+1} \in U_{j+1}} \Pr[z_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = u_{j+1}] \\
&\quad + \sum_{u_{j+1} \in U_{j+1}} \Pr[x_{l+1}^j \oplus H_{k_{j+1}}(t_{l+1}) = u_{j+1}] \\
&\leq \sum_{i \leq l} \Pr[H_{k_{j+1}}(t_i) \oplus H_{k_{j+1}}(t_{l+1}) = z_i^j \oplus z_{l+1}^j] \\
&\quad + \sum_{i \leq l} \Pr[H_{k_{j+1}}(t_i) \oplus H_{k_{j+1}}(t_{l+1}) = x_i^j \oplus x_{l+1}^j] \\
&\quad + \sum_{u_{j+1} \in U_{j+1}} \Pr[H_{k_{j+1}}(t_{l+1}) = z_{l+1}^j \oplus u_{j+1}] \\
&\quad + \sum_{u_{j+1} \in U_{j+1}} \Pr[H_{k_{j+1}}(t_{l+1}) = x_{l+1}^j \oplus u_{j+1}] \\
&\leq 2l\varepsilon + \frac{2q_p}{N},
\end{aligned}$$

where the last inequality comes from the ε-AXU property of $\mathcal{H}$ (note that when $t_{l+1} = t_j$, necessarily $z_{l+1}^j \neq z_i^j$ and $x_{l+1}^j \neq x_i^j$ since $\mathcal{D}$ never makes pointless queries, so that the probability is zero) and from the uniformity of $\mathcal{H}$. Since the keys k_j are independent, we have:

$$\Pr\left[\bigcap_{i=0}^{r-1} F_i\right] \leq \left(2l\varepsilon + \frac{2q_p}{N}\right)^r. \tag{34}$$

Using the Coupling Lemma and the fact that $z_i^r = x_i^r$ for all $i \leq l$, we have:

$$\|\mu'_{l+1} - \mu'_l\| \leq \Pr\left[(z_1^r, \ldots, z_{l+1}^r) \neq (x_1^r, \ldots, x_{l+1}^r)\right] \leq \Pr\left[z_{l+1}^r \neq x_{l+1}^r\right]. \tag{35}$$

If we succeed to couple the last query at some round $j \leq r-1$, we know that $z_{l+1}^{j'}$ and $x_{l+1}^{j'}$ remain equal in the subsequent rounds so that:

$$\Pr\left[z_{l+1}^r \neq x_{l+1}^r\right] \leq \Pr\left[\bigcap_{i=0}^{r-1} F_i\right]. \tag{36}$$

Using (34), (35) and (36), we have:

$$\|\mu'_{l+1} - \mu'_l\| \leq \left(2l\varepsilon + \frac{2q_p}{N}\right)^r \leq \left(2q_c\varepsilon + \frac{2q_p}{N}\right)^r. \tag{37}$$

Finally, using (32) and (37), we get:

$$\|\mu_{\mathbf{t},\mathbf{x},\mathcal{Q}_\mathbf{P}} - \mu^*_\mathbf{t}\| \leq q_c \left(2q_c\varepsilon + \frac{2q_p}{N}\right)^r. \qquad \square$$

Concluding. By combining Lemmas 9 and 10, we get the proof of Theorem 3.

4.3 From Non-Adaptive to Adaptive Distinguishers

In this section, we consider the case of CCA-distinguishers, and prove the following result.

Theorem 4. *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:*

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

For odd r, we have $\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,r,\mathcal{H}]} \leq \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,r-1,\mathcal{H}]}$, 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.

To prove Theorem 4, we will rely on Lemma 1 in the special case where all transcripts are good ($\varepsilon_2 = 0$). For this, we will derive an appropriate bound ε_1 by doubling the number of rounds of the construction and using Lemma 8. Note that in this subsection, contrary to Section 3, we only consider attainable queries transcripts $\tau' = (\mathcal{Q}_C, \mathcal{Q}_\mathbf{P})$ without giving the key $\mathbf{k}$ to the adversary at the end of the attack. We still denote T_{re} and T_{id} random variables distributed according to the probability distributions of the query transcript τ' induced by the real (resp. the ideal) world.

Lemma 11. *Let r be an even integer and $r' = r/2$. Let q_c, q_p be positive integers. We denote:*

$$\alpha = 2^{r'}\frac{q_c(N\varepsilon q_c + q_p)^{r'}}{N^{r'}}.$$

Then for any attainable queries transcript τ', one has

$$\frac{\Pr[T_{\mathrm{re}} = \tau']}{\Pr[T_{\mathrm{id}} = \tau']} \geq 1 - 4\sqrt{\alpha}.$$

Proof. Fix any attainable queries transcript $\tau' = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$. As usual, we write $\mathbf{P} \vdash \mathcal{Q}_\mathbf{P}$ for the event $\wedge_{i=1}^r (P_i \vdash \mathcal{Q}_{P_i})$. We denote $\mathbf{P} = (P_1, \ldots, P_r)$, $\mathbf{P}'_1 = (P_1, \ldots, P_{r'})$ and $\mathbf{P}'_2 = (P_{r'+1}, \ldots, P_r)$. Similarly, $\mathbf{k}'_1 = (k_1, \ldots, k_{r'})$ and $\mathbf{k}'_2 = (k_{r'+1}, \ldots, k_r)$. We define the events:

$$\mathbf{P}'_1 \vdash \mathcal{Q}_{\mathbf{P}'_1} = \wedge_{i=1}^{r'} (P_i \vdash \mathcal{Q}_{P_i}),$$
$$\mathbf{P}'_2 \vdash \mathcal{Q}_{\mathbf{P}'_2} = \wedge_{i=r'+1}^{r} (P_i \vdash \mathcal{Q}_{P_i}).$$

Let also $\mathcal{Q}_C = ((t_1, x_1, y_1), \ldots, (t_{q_c}, x_{q_c}, y_{q_c}))$, $\mathbf{t} = (t_1, \ldots, t_{q_c})$, $\mathbf{x} = (x_1, \ldots, x_{q_c})$ and $\mathbf{y} = (y_1, \ldots, y_{q_c})$. Then, for every $i = 1, \ldots, q_c$,

$$\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}(t_i, x_i) = \mathsf{TEM}_{\mathbf{k}_2'}^{\mathbf{P}_2'}\Big(t_i, \mathsf{TEM}_{\mathbf{k}_1'}^{\mathbf{P}_1'}(t_i, x_i)\Big).$$

We will apply Lemma 8 independently to each half of the cipher $\mathsf{TEM}_{\mathbf{k}_1'}^{\mathbf{P}_1'}$ and $\mathsf{TEM}_{\mathbf{k}_2'}^{\mathbf{P}_2'}$. Consider the first half $\mathsf{TEM}_{\mathbf{k}_1'}^{\mathbf{P}_1'}$. By Lemma 10, we have $\|\mu^1_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}_1'}} - \mu^*_{\mathbf{t}}\| \leq \alpha$, where $\mu^1_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}_1'}}$ is the distribution of $\mathsf{TEM}_{\mathbf{k}_1'}^{\mathbf{P}_1'}(\mathbf{t}, \mathbf{x})$ conditioned on $\mathbf{P}_1' \vdash \mathcal{Q}_{\mathbf{P}_1'}$. Hence Lemma 8 ensures that there is a subset $S_{\mathbf{x}} \subset \Omega_{\mathbf{t}}$ of size at least $(1 - \sqrt{\alpha})|\Omega_{\mathbf{t}}|$ such that for all $\mathbf{z} \in S_{\mathbf{x}}$:

$$\mu^1_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}_1'}}(\mathbf{z}) \geq \frac{1 - \sqrt{\alpha}}{|\Omega_{\mathbf{t}}|}. \tag{38}$$

Applying a similar reasoning to the distribution $\mu^2_{\mathbf{t},\mathbf{y},\mathcal{Q}_{\mathbf{P}_2'}}$ of $(\mathsf{TEM}_{\mathbf{k}_2'}^{\mathbf{P}_2'})^{-1}(\mathbf{t}, \mathbf{y})$ conditioned on $\mathbf{P}_2' \vdash \mathcal{Q}_{\mathbf{P}_2'}$, we see that there exists a subset $S_{\mathbf{y}} \subset \Omega_{\mathbf{t}}$ of size at least $(1 - \sqrt{\alpha})|\Omega_{\mathbf{t}}|$ such that for all $\mathbf{z} \in S_{\mathbf{y}}$:

$$\mu^2_{\mathbf{t},\mathbf{y},\mathcal{Q}_{\mathbf{P}_2'}}(\mathbf{z}) \geq \frac{1 - \sqrt{\alpha}}{|\Omega_{\mathbf{t}}|}. \tag{39}$$

Note that $|S_{\mathbf{x}} \cap S_{\mathbf{y}}| \geq (1 - 2\sqrt{\alpha})|\Omega_{\mathbf{t}}|$. Since the permutations $P_1, \ldots, P_r$ and the keys $k_1, \ldots, k_r$ are uniformly random and independent, one has

$$\begin{aligned}
\Pr[T_{\mathrm{re}} = \tau'] &\geq \sum_{\mathbf{z} \in S_{\mathbf{x}} \cap S_{\mathbf{y}}} \Pr\left[\mathsf{TEM}_{\mathbf{k}_1'}^{\mathbf{P}_1'}(\mathbf{t}, \mathbf{x}) = \mathbf{z} \wedge \mathbf{P}_1' \vdash \mathcal{Q}_{\mathbf{P}_1'}\right] \\
&\qquad \times \Pr\left[(\mathsf{TEM}_{\mathbf{k}_2'}^{\mathbf{P}_2'})^{-1}(\mathbf{t}, \mathbf{y}) = \mathbf{z} \wedge \mathbf{P}_2' \vdash \mathcal{Q}_{\mathbf{P}_2'}\right] \\
&\geq \sum_{\mathbf{z} \in S_{\mathbf{x}} \cap S_{\mathbf{y}}} \mu^1_{\mathbf{t},\mathbf{x},\mathcal{Q}'_{\mathbf{P}_1'}}(\mathbf{z}) \mu^2_{\mathbf{t},\mathbf{y},\mathcal{Q}_{\mathbf{P}_2'}}(\mathbf{z}) \Pr[\mathbf{P}_1' \vdash \mathcal{Q}_{\mathbf{P}_1'}] \Pr[\mathbf{P}_2' \vdash \mathcal{Q}_{\mathbf{P}_2'}] \\
&\geq \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \sum_{\mathbf{z} \in S_{\mathbf{x}} \cap S_{\mathbf{y}}} \mu^1_{\mathbf{t},\mathbf{x},\mathcal{Q}_{\mathbf{P}_1'}}(\mathbf{z}) \mu^2_{\mathbf{t},\mathbf{y},\mathcal{Q}_{\mathbf{P}_2'}}(\mathbf{z}).
\end{aligned}$$

Using (38) and (39), we get

$$\begin{aligned}
\Pr[T_{\mathrm{re}} = \tau'] &\geq \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \sum_{\mathbf{z} \in S_{\mathbf{x}} \cap S_{\mathbf{y}}} \frac{(1 - \sqrt{\alpha})^2}{|\Omega_{\mathbf{t}}|^2} \\
&\geq \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \frac{(1 - 2\sqrt{\alpha})|S_{\mathbf{x}} \cap S_{\mathbf{y}}|}{|\Omega_{\mathbf{t}}|^2} \\
&\geq \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \frac{(1 - 2\sqrt{\alpha})(1 - 2\sqrt{\alpha})}{|\Omega_{\mathbf{t}}|} \\
&\geq \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \frac{1 - 4\sqrt{\alpha}}{|\Omega_{\mathbf{t}}|}.
\end{aligned} \tag{40}$$

We next consider $\Pr[T_{\mathrm{id}} = \tau']$. Note that, in the ideal world, the r-tuple of permutations is independent from the tweakable permutation. Hence, one has

$$\Pr[T_{\mathrm{id}} = \tau'] = \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \Pr[\widetilde{P} \vdash \mathcal{Q}_C].$$

Denote m the number of different tweaks. Let q_i be the number of queries using the i-th tweak for some arbitrary ordering of the tweaks. Then $|\Omega_{\mathbf{t}}| = \prod_{i=1}^{m} (N)_{q_i}$. Finally, $\widetilde{P} \vdash \mathcal{Q}_C$ is equivalent to q_i constraints on the permutation associated with the i-th tweak, $i = 1, \ldots, m$. Then

$$\Pr[\widetilde{P} \vdash \mathcal{Q}_C] = \prod_{i=1}^{m} \frac{1}{(N)_{q_i}} = \frac{1}{|\Omega_{\mathbf{t}}|}$$

and

$$\Pr[T_{\mathrm{id}} = \tau'] = \Pr[\mathbf{P} \vdash \mathcal{Q}_{\mathbf{P}}] \frac{1}{|\Omega_{\mathbf{t}}|}. \tag{41}$$

Hence, by combining (40) and (41), we arrive at

$$\frac{\Pr[T_{\mathrm{re}} = \tau']}{\Pr[T_{\mathrm{id}} = \tau']} \geq 1 - 4\sqrt{\alpha}. \qquad \square$$

Concluding. Combining Lemmas 1 and 11 proves Theorem 4.

References

[ABD+13] Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the Indifferentiability of Key-Alternating Ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *LNCS*, pages 531–550. Springer, 2013. Full version available at http://eprint.iacr.org/2013/061.

[ABL+13] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and Authenticated Online Ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - Proceedings, Part I*, volume 8269 of *LNCS*, pages 424–443. Springer, 2013.

[ABM13] Elena Andreeva, Andrey Bogdanov, and Bart Mennink. Towards Understanding the Known-Key Security of Block Ciphers. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *LNCS*, pages 348–366. Springer, 2013.

[BK03] Mihir Bellare and Tadayoshi Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 491–506. Springer, 2003.

[BKL+12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 45–62. Springer, 2012.

[CLL+14] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the Two-Round Even-Mansour Cipher. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 (Proceedings, Part I)*, volume 8616 of *LNCS*, pages 39–56. Springer, 2014. Full version available at http://eprint.iacr.org/2014/443.

[Cro00] Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.

[CS14] Shan Chen and John Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.

[CS15] Benoît Cogliati and Yannick Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - Proceedings, Part I*, volume 9056 of *LNCS*, pages 584–613. Springer, 2015. Full version available at http://eprint.iacr.org/2015/069.

[DKS12] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 336–354. Springer, 2012.

[DR01] Joan Daemen and Vincent Rijmen. The Wide Trail Design Strategy. In Bahram Honary, editor, *Cryptography and Coding 2001*, volume 2260 of *LNCS*, pages 222–238. Springer, 2001.

[EM97] Shimon Even and Yishay Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *Journal of Cryptology*, 10(3):151–162, 1997.

[FLS+10] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. SHA3 Submission to NIST (Round 3), 2010.

[FP15] Pooya Farshim and Gordon Procter. 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.

[GHL+07] David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On Tweaking Luby-Rackoff Blockciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 342–356. Springer, 2007.

[HR03] Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.

[HR04] Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.

[HR10] Viet Tung Hoang and Phillip Rogaway. On Generalized Feistel Networks. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630. Springer, 2010.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - Proceedings, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 278–295. Springer, 2012.

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

[LS13a] Rodolphe Lampe and Yannick Seurin. How to Construct an Ideal Cipher from a Small Set of Public Permutations. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *LNCS*, pages 444–463. Springer, 2013. Full version available at http://eprint.iacr.org/2013/255.

[LS13b] Rodolphe Lampe and Yannick Seurin. Tweakable Blockciphers with Asymptotically Optimal Security. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *LNCS*, pages 133–151. Springer, 2013.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012. Full version available at http://eprint.iacr.org/2012/450.

[MI08] Atsushi Mitsuda and Tetsu Iwata. Tweakable Pseudorandom Permutation from Generalized Feistel Structure. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *ProvSec 2008*, volume 5324 of *LNCS*, pages 22–37. Springer, 2008.

[Min09] Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Orr Dunkelman, editor, *Fast Software Encryption - FSE 2009*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.

[MRS09] Ben Morris, Phillip Rogaway, and Till Stegers. How to Encipher Messages on a Small Domain. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *LNCS*, pages 286–302. Springer, 2009.

[NK92] Kaisa Nyberg and Lars R. Knudsen. Provable Security Against Differential Cryptanalysis. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92*, volume 740 of *LNCS*, pages 566–574. Springer, 1992.

[Pat08] Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.

[Pro14] Gordon Procter. A Note on the CLRW2 Tweakable Block Cipher Construction. IACR Cryptology ePrint Archive, Report 2014/111, 2014. Available at http://eprint.iacr.org/2014/111.

[RBB03] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.

[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.

[RZ11] Phillip Rogaway and Haibin Zhang. Online Ciphers from Tweakable Blockciphers. In Aggelos Kiayias, editor, *Topics in Cryptology - CT-RSA 2011*, volume 6558 of *LNCS*, pages 237–249. Springer, 2011.

[Sch98] Richard Schroeppel. The Hasty Pudding Cipher. AES submission to NIST, 1998.

[Sho96] Victor Shoup. On Fast and Provably Secure Message Authentication Based on Universal Hashing. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of *LNCS*, pages 313–328. Springer, 1996.

[STA+14] Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher v1. Submission to the CAESAR competition, 2014.

[Ste12] John Steinberger. Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance. IACR Cryptology ePrint Archive, Report 2012/481, 2012. Available at http://eprint.iacr.org/2012/481.