Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing

Benoît Cogliati* and Yannick Seurin**

Abstract. The iterated Even-Mansour construction defines a block cipher from a tuple of public n-bit permutations $(P_1, \ldots, P_r)$ by alternatively xoring some n-bit round key k_i, $i = 0, \ldots, r$, and applying permutation P_i to the state. The *tweakable* Even-Mansour construction generalizes the conventional Even-Mansour construction by replacing the n-bit round keys by n-bit strings derived from a master key *and a tweak*, thereby defining a tweakable block cipher. Constructions of this type have been previously analyzed, but they were either secure only up to the birthday bound, or they used a nonlinear mixing function of the key and the tweak (typically, multiplication of the key and the tweak seen as elements of some finite field) which might be costly to implement. In this paper, we tackle the question of whether it is possible to achieve beyond-birthday-bound security for such a construction by using only linear operations for mixing the key and the tweak into the state. We answer positively, describing a 4-round construction with a $2n$-bit master key and an n-bit tweak which is provably secure in the Random Permutation Model up to roughly $2^{2n/3}$ adversarial queries.

Keywords: tweakable block cipher, iterated Even-Mansour cipher, key-alternating cipher, beyond-birthday-bound security

1 Introduction

Background. A block cipher with key space $\mathcal{K}$ and message space $\mathcal{M}$ is a family of permutations of $\mathcal{M}$ indexed by the key $\mathbf{k} \in \mathcal{K}$. A *tweakable* block cipher (TBC) takes an additional (potentially public) input parameter $\mathbf{t} \in \mathcal{T}$ called a *tweak* aiming at providing inherent variability in about the same way an IV or nonce brings variability to an encryption scheme. Some block ciphers such as the Hasty Pudding Cipher [35], Mercy [10], or Threefish (the block cipher underlying the Skein hash function [15]) were designed so as to natively support tweaks. The syntax and security requirements for tweakable block ciphers were formally articulated in a seminal paper by Liskov, Rivest and Wagner [24]. Since then, TBCs have found multiple applications such as (tweakable) length-preserving encryption modes [18, 19], online ciphers [33, 1], and authenticated encryption modes [24, 32, 31].

* University of Versailles, France. E-mail: benoitcogliati@hotmail.fr
** ANSSI, Paris, France. E-mail: yannick.seurin@m4x.org

Liskov *et al.* [24] also proposed two generic constructions of a TBC from a standard block cipher, achieving security up to the so-called birthday bound, i.e., when the adversary is allowed at most roughly $2^{n/2}$ queries to the encryption or decryption oracle, where n is the block size (that is, the message space of the TBC is $\mathcal{M} = \{0,1\}^n$). The "black-box" design strategy (i.e., building a TBC on top of an existing standard block cipher, in a black-box way) has since then been the main avenue of research. Earlier proposals, such as XEX [31] and variants [26, 4] were related to the second of the two original proposals of Liskov *et al.*, and were limited to birthday-bound security as well. Recently, a number of constructions achieving beyond-birthday-bound security have emerged, such as Minematsu's construction [27], the CLRW construction [23, 22, 30], and two constructions by Mennink [25]. All those constructions enjoy a security proof in the standard model (i.e., assuming that the underlying block cipher is a pseudorandom permutation), except for Mennink's constructions that were analyzed in the ideal cipher model.

Tweaking Even-Mansour Ciphers. Unfortunately, none of the currently known black-box TBC constructions with beyond-birthday-bound security can be deemed truly practical (even though some of them might come close to it [25]). Hence, it might be beneficial to "open the hood" and to study how to build a TBC from some lower level primitive than a full-fledged conventional block cipher, e.g., a pseudorandom function or a public permutation. For example, Goldenberg *et al.* [16] investigated how to include a tweak in Feistel ciphers. This was extended to generalized Feistel ciphers by Mitsuda and Iwata [28]. Recently, a similar study was undertaken for the second large class of block ciphers besides Feistel ciphers, namely key-alternating ciphers [11], a super-class of Substitution-Permutation Networks (SPNs). An r-round key-alternating cipher based on a tuple of public n-bit permutations $(P_1, \ldots, P_r)$ maps a plaintext $x \in \{0,1\}^n$ to the ciphertext defined as

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

where the n-bit round keys $k_0, \ldots, k_r$ are either independent or derived from a master key $\mathbf{k}$. When the P_i's are modeled as public permutation oracles, construction (1) is also referred to as the (iterated) Even-Mansour construction, in reference to Even and Mansour who pioneered the analysis of this construction in the Random Permutation Model [13]. While Even and Mansour limited themselves to proving birthday-bound security in the case $r = 1$, larger numbers of rounds were studied in subsequent works [3, 36, 21]. The general case has been recently (tightly) settled by Chen and Steinberger [6], who proved that the r-round iterated Even-Mansour cipher with r-wise independent round keys ensures security up to roughly $2^{\frac{rn}{r+1}}$ adversarial queries.

In order to incorporate a tweak $\mathbf{t}$ in the iterated Even-Mansour construction, it is tantalizing to generalize (1) by replacing round keys k_i by some function $f_i(\mathbf{k}, \mathbf{t})$ of the master key $\mathbf{k}$ *and* the tweak $\mathbf{t}$ (see Figure 1). We will refer to such a construction as a *Tweakable Even-Mansour* (TEM) construction.[1] This is exactly

[1] We warn that the naming *Tweakable Even-Mansour* construction was previously used by the designers of Minalpher [34], a candidate to the CAESAR competition,

the spirit of the TWEAKEY framework introduced by Jean *et al.* [20]. In fact, these authors go one step further and propose to unify the key and tweak inputs into what they dub the *tweakey*. The main topic of this paper being provable security (in the traditional model where the key is secret and the tweak is chosen by the adversary), we will not make such a bold move here, since we are not aware of any formal security model adequately capturing what Jean *et al.* had in mind.

The investigation of the theoretical soundness of this design strategy was initiated in three recent papers. First, Cogliati and Seurin [8], and independently Farshim and Procter [14], analyzed the simple case of an n-bit key k and an n-bit tweak t simply xored together at each round, i.e., $f_i(k,t) = k \oplus t$ for each $i = 0, \ldots, r$.[2] They gave attacks up to two rounds, and proved birthday-bound security for three rounds. In fact, the security of this construction caps at $2^{n/2}$ queries independently of the number of rounds. Indeed, it can be written $\widetilde{E}(k,t,x) = E(k \oplus t, x)$, where E is the conventional iterated Even-Mansour cipher with the trivial key-schedule (i.e., the same round key is xored between each round), and by a result of Bellare and Kohno [2, Corollary 5.7], a tweakable block cipher of this form can never offer more than $\kappa/2$ bits of security, where κ is the key-length of E (i.e., $\kappa = n$ in the case at hand). Hence, if we want beyond-birthday-bound security, we have no choice but to consider more complex functions f_i (at the bare minimum, these functions, even if linear, should prevent the TBC construction from being of the form $E(k \oplus t, x)$ for some block cipher E with n-bit keys).

This was undertaken by Cogliati, Lampe, and Seurin [7], who considered nonlinear ways of mixing the key and the tweak. More specifically, they studied the case where $f_i(\mathbf{k}, t) = H_{k_i}(t)$, where the family of functions (H_k) is uniform and almost XOR-universal, and the master key is $\mathbf{k} = (k_0, \ldots, k_r)$. A classical example is multiplication-based hashing, i.e., $f_i(\mathbf{k}, t) = k_i \otimes t$, where $\otimes$ denotes the multiplication in the finite field $\mathbb{F}_{2^n}$, the tweak $t = 0$ being forbidden. Cogliati *et al.* showed that one round is secure up to the birthday bound, and that two rounds are secure up to roughly $2^{2n/3}$ adversarial queries.[3] They also provided a (non-tight) asymptotic security bound improving as the number of rounds grows. However, implementing a xor-universal hash function might be costly, and linear functions f_i's would be highly preferable for obvious efficiency reasons.

---

to designate a permutation-based variant of Rogaway's XEX construction [31], i.e., a 1-round Even-Mansour construction where the derivation functions f_0 and f_1 applied to $(\mathbf{k}, \mathbf{t})$ are allowed to depend on the internal permutation P_1 (something we do not consider in this paper).

[2] Actually, the results of [8, 14] were stated in terms of xor-induced related-key security of the (conventional) iterated Even-Mansour cipher, but in this case this is equivalent to standard (i.e., single-key) security of the corresponding tweakable construction.

[3] More precisely, the birthday-bound result applies to the variant of the construction were the same key is used before and after permutation P_1, and the $2^{2n/3}$-security bound applies to the cascade of this construction with two independent keys and two independent permutations.

Our Results. In this paper, we ask whether it is possible to come with a tweakable Even-Mansour construction achieving both:

1. a linear mixing of the tweak and the key to the state;
2. beyond-birthday-bound security.

We answer positively, by providing a construction with $2n$-bit keys and n-bit tweaks. The starting point is the 4-round iterated Even-Mansour construction with a $2n$-bit master key (k_0, k_1), k_0 and k_1 being both n bits, and what we call the "alternating" key schedule, namely round keys are k_0, k_1, k_0, etc. This is for example how LED-128 is designed [17]. To turn this block cipher into a tweakable Even-Mansour construction, we simply add the n-bit tweak t between each permutation (see Figure 2). In other words, if we denote $E((k_0, k_1), x)$ the conventional Even-Mansour cipher with alternating round keys, the tweakable construction that we consider can be written

$$\widetilde{E}((k_0, k_1), t, x) = E((k_0 \oplus t, k_1 \oplus t), x).$$

We prove that this construction is secure up to roughly $2^{2n/3}$ adversarial queries. Unsurprisingly, and as in many previous works, our proof uses Patarin's H-coefficients technique [29, 6]. In particular, we rely on a key lemma by Cogliati *et al.* [7] to analyze so-called good transcripts.

Application to Related-Key Security. Our result can be rephrased in terms of related-key security [2] of the conventional Even-Mansour cipher: the 4-round conventional Even-Mansour cipher with the alternating key-schedule is secure up to roughly $2^{2n/3}$ adversarial queries against related-key attacks for the set of related-key deriving functions

$$\Phi^{2-\oplus} \stackrel{\text{def}}{=} \{(k_0, k_1) \mapsto (k_0 \oplus \Delta, k_1 \oplus \Delta) : \Delta \in \{0,1\}^n\}.$$

Note that this set is more restrictive than the set $\Phi^{\oplus}$ that would allow to xor an arbitrary $2n$-bit string to the master key (k_0, k_1). It remains an open problem (already stated in [8]) to find an Even-Mansour construction provably secure beyond the birthday bound against $\Phi^{\oplus}$-related-key attacks.

Open Problems. We propose three challenging open problems, the first two being restricted to the case of n-bit tweaks. First, what would be the analogue of the Chen-Steinberger result [6] in the tweakable setting? In more details, we know how to deliver $n/2$ bits of security with an n-bit master key [8, 14] and this paper shows how to reach $2n/3$ bits of security with a $2n$-bit master key. Hence, it is natural to ask whether one can obtain $rn/(r+1)$ bits of security from an rn-bit master key for $r > 2$, and what would be the adequate number of rounds and the corresponding (linear) "tweak-and-key" schedule. Second, Chen *et al.* [5] showed that the 2-round conventional Even-Mansour construction can provably deliver $2n/3$ bits of security even with an n-bit master key (for example, when the two inner permutations are independent, the trivial key-schedule is

sufficient). Again, what would be the analogue of this result in the tweakable setting? Can we design a TEM construction with an n-bit master key and an n-bit tweak delivering $2n/3$ bits of security, or even more? Finally, it is natural to ask whether one can extend the construction of this paper to handle larger tweaks, in particular $2n$-bit tweaks. We show in the full version of this paper [9] that the naive way of proceeding, namely adding alternatively t_0 and t_1, is insecure for four rounds. Hence, this seems to require at least five rounds.

We also remark that attacks against the (conventional) iterated Even-Mansour cipher with the alternating key-schedule have been investigated by Dinur *et al.* [12]. It would be interesting to study whether these attacks can be adapted (and potentially improved) in the tweakable setting.

Organization. In Section 2, we introduce the notation, the security definitions, and give some background on the H-coefficients technique. Our main result is proved in Section 3.

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 $\mathsf{P}(n)$.

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 $\{0,1\}^n$.

Tweakable Even-Mansour Constructions. Fix integers $n, r \geq 1$. Let $\mathcal{K}$ and $\mathcal{T}$ be two sets, and let $\mathbf{f} = (f_0, \ldots, f_r)$ be a $(r+1)$-tuple of functions from $\mathcal{K} \times \mathcal{T}$ to $\{0,1\}^n$. The r-round tweakable Even-Mansour construction $\mathsf{TEM}[n,r,\mathbf{f}]$ 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 $\mathcal{K}$, tweak space $\mathcal{T}$, and message space $\{0,1\}^n$, simply denoted $\mathsf{TEM}^{\mathbf{P}}$ in the following (parameters $[n,r,\mathbf{f}]$ will always be clear from the context) which maps a key $\mathbf{k} \in \mathcal{K}$, a tweak $\mathbf{t} \in \mathcal{T}$, and a plaintext $x \in \{0,1\}^n$ to the ciphertext defined as (see Figure 1):

$$\mathsf{TEM}^{\mathbf{P}}(\mathbf{k},\mathbf{t},x) = f_r(\mathbf{k},\mathbf{t}) \oplus P_r(f_{r-1}(\mathbf{k},\mathbf{t}) \oplus P_{r-1}(\cdots P_1(f_0(\mathbf{k},\mathbf{t}) \oplus x)\cdots)).$$

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

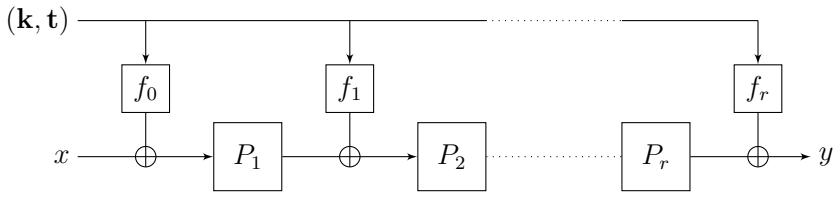

Fig. 1. The r-round tweakable Even-Mansour construction based on a tuple of public permutations $(P_1, \ldots, P_r)$.

We will mostly be interested in the case where $\mathcal{K} = (\{0,1\}^n)^a$ and $\mathcal{T} = (\{0,1\}^n)^b$ for integers $a, b \geq 1$. In this setting, we will denote $\mathbf{k} = (k_0, \ldots, k_{a-1})$ and $\mathbf{t} = (t_0, \ldots, t_{b-1})$, all k_i's and t_j's being n-bit strings, or simply $\mathbf{k} = k$, resp. $\mathbf{t} = t$ when $a = 1$, resp. $b = 1$. When all f_i's are linear over $(\{0,1\}^n)^{a+b}$, we say that the construction has *linear tweak and key mixing*.

Previously Studied Constructions. Two types of TEM constructions have already been studied. In [8], Cogliati and Seurin considered the simplest case where $a = b = 1$ (n-bit keys and n-bit tweaks) and $f_i(k,t) = k \oplus t$ for each $i = 0, \ldots, r$. This construction has linear tweak and key mixing, and is secure up to $2^{n/2}$ adversarial queries starting from $r = 3$. (The results of [8] were formulated in terms of xor-induced related-key attacks against the conventional iterated Even-Mansour construction, but in this simple case the two security notions are in fact equivalent.) In [7], Cogliati, Lampe, and Seurin studied a large class of nonlinear mixing functions, in particular, for n-bit tweaks, finite field multiplication-based ones, i.e., $f(k,t) = k \otimes t$, or more generally, for bn-bit tweaks, polynomial hashing-based functions, i.e., $f(k, (t_0, \ldots, t_{b-1})) = \sum_{i=0}^{b-1} k^{i+1} \otimes t_i$.

2.2 Security Definitions

Fix some family of functions $\mathbf{f} = (f_0, \ldots, f_r)$ from $\mathcal{K} \times \mathcal{T}$ to $\{0,1\}^n$. To study the security of the construction $\mathsf{TEM}[n, r, \mathbf{f}]$ in the Random Permutation Model, we consider a distinguisher $\mathcal{D}$ which interacts with $r+1$ oracles that we denote generically $(\widetilde{P}_0, P_1, \ldots, P_r)$, where syntactically $\widetilde{P}_0$ is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\{0,1\}^n$, and $P_1, \ldots, P_r$ are permutations of $\{0,1\}^n$. The goal of $\mathcal{D}$ is to distinguish two "worlds": the so-called *real world*, where $\mathcal{D}$ interacts with $(\mathsf{TEM}_{\mathbf{k}}^{\mathbf{P}}, \mathbf{P})$, where $\mathbf{P} = (P_1, \ldots, P_r)$ is a tuple of public random permutations and the key $\mathbf{k}$ is drawn uniformly at random from $\mathcal{K}$, 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*.

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

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

where the first probability is taken over the random choice of $\mathbf{k}$ and $\mathbf{P}$, and the second probability is taken over the random choice of $\widetilde{P}_0$ and $\mathbf{P}$. In all the following, we consider computationally unbounded distinguishers, and hence we can assume *wlog* that they are deterministic. We also assume that they never make pointless queries (i.e., queries whose answers can be unambiguously deduced from previous answers). The distinguisher is allowed to query all oracles adaptively in both directions; this corresponds to adaptive chosen-plaintext and ciphertext attacks (CCA).

For non-negative integers q_c and q_p, we define the insecurity of the $\mathsf{TEM}[n, r, \mathbf{f}]$ construction against CCA-attacks as

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

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

2.3 The H-Coefficients Technique

As in many previous works [6, 5, 8, 7], our security proof will use the H-coefficients technique [29], which we explain here.

Transcript. Recall that the distinguisher $\mathcal{D}$ interacts with a tuple of $r+1$ oracles denoted $(\widetilde{P}_0, P_1, \ldots, P_r)$. In the real world, the construction oracle $\widetilde{P}_0$ is $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{k}}$ where $\mathbf{P} = (P_1, \ldots, P_r)$ and $\mathbf{k}$ is random, whereas in the ideal world it is a random tweakable permutation independent from $(P_1, \ldots, P_r)$. From the interaction of $\mathcal{D}$ with these oracles, we define the *queries transcript* $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ of the attack as follows. The list $\mathcal{Q}_C$ records the queries to the construction oracle: if $\mathcal{D}$ made either a direct query $(\mathbf{t}, x)$ to the construction oracle $\widetilde{P}_0$ which was answered by y, or an inverse query $(\mathbf{t}, y)$ which was answered by x, then the triple $(\mathbf{t}, x, y) \in \mathcal{T} \times \{0,1\}^n \times \{0,1\}^n$ is added to $\mathcal{Q}_C$. 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 $\mathcal{D}$ made either a direct query u to permutation P_i which was answered by v, or an inverse query v which was answered by u. Note that queries are recorded in a directionless and unordered way, but by our assumption that the distinguisher is deterministic, the raw interaction of $\mathcal{D}$ with its oracles can unambiguously be reconstructed from the queries transcript (see e.g. [6] 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 $\mathcal{Q}_{P_i}$. Moreover, since we assume that the distinguisher always makes the maximal number of allowed queries to each oracle, one has $|\mathcal{Q}_C| = q_c$ and $|\mathcal{Q}_{P_i}| = q_p$ for $1 \leq i \leq r$. 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, $1 \leq i \leq m$, ordering the tweaks arbitrarily. Note that one always has $\sum_{i=1}^{m} q_i = q_c$, even though m may depend on the answers received from the oracles.

A queries transcript is said *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 $(\widetilde{P}_0, \mathbf{P})$ results in this transcript (in other words, the probability to obtain this transcript in the ideal world is non-zero). Moreover, in order to have a simple definition of bad transcripts, the actual key $\mathbf{k}$ is revealed to the adversary at the end of the experiment if we are in the real world, while in the ideal world, a "dummy" key $\mathbf{k} \leftarrow_{\$} \mathcal{K}$ is simply drawn uniformly at random independently from the answers of the oracle $\widetilde{P}_0$ (this is obviously without loss of generality since this can only help the distinguisher and increase its advantage). All in all, a transcript τ is a tuple $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r}, \mathbf{k})$, and we say that a transcript is attainable if the corresponding queries transcript $(\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ is attainable. We denote Θ the set of attainable transcripts. In all the following, we denote T_{re}, resp. T_{id}, the probability distribution of the transcript τ induced by the real world, resp. the ideal world (note that these two probability distributions depend on the distinguisher). By extension, we use the same notation to denote a random variable distributed according to each distribution. The main lemma of the H-coefficients technique is the following one (see e.g. [6, 5] for the proof).

Lemma 1. *Fix a distinguisher $\mathcal{D}$. Let $\Theta = \Theta_{\mathrm{good}} \sqcup \Theta_{\mathrm{bad}}$ be a partition of the set of attainable transcripts. Assume that there exists ε_1 such that for any $\tau \in \Theta_{\mathrm{good}}$, one has*[4]

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

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

Useful Observations. We end this section with some useful preliminary observations. First, we introduce some 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 transcripts $\mathcal{Q}_{\mathbf{P}} = (\mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_r})$ 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

$$\Pr[P \leftarrow_{\$} \mathsf{P}(n) : P \vdash \mathcal{Q}] = \frac{1}{(N)_{q_p}}. \tag{2}$$

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

$$\Pr[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n) : \widetilde{P} \vdash \widetilde{\mathcal{Q}}] = \prod_{i=1}^{m} \frac{1}{(N)_{q_i}}. \tag{3}$$

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

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 (2) and (3), the probability of getting any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{\mathbf{P}}, \mathbf{k})$ in the ideal world is

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

In the real world, the probability to obtain τ is

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

Let

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

Then we have

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = \mathsf{p}(\tau) \Big/ \prod_{i=1}^{m} \frac{1}{(N)_{q_i}}. \tag{4}$$

Hence, applying Lemma 1 will require three steps: first, define good and bad transcripts, then upper bound the probability of bad transcripts in the ideal world, and finally lower bound the real world probability $\mathsf{p}(\tau)$ when τ is good in order to use Eq. (4).

2.4 An Extended Sum-Capture Lemma

To upper bound the probability of getting a bad transcript in the ideal world, we will need a generalization of the sum-capture theorem from [5] (that applied to a random permutation) to the case of a *family* of random permutations (in other words, a random tweakable permutation).

We denote $\mathsf{GL}(n)$ the general linear group of degree n over $\mathbb{F}_2$, i.e., the set of all automorphisms (linear bijective mappings) of $\mathbb{F}_2^n$.

Lemma 2. *Fix an automorphism $\Gamma \in \mathsf{GL}(n)$ and a non-empty set $\mathcal{T}$. Let $\widetilde{P}$ be a uniformly random tweakable permutation in $\mathsf{TP}(\mathcal{T}, n)$, and let $\mathcal{A}$ be some probabilistic algorithm making exactly q (two-sided) adaptive queries to $\widetilde{P}$. Let $\widetilde{\mathcal{Q}} = ((t_1, x_1, y_1), \ldots, (t_q, x_q, y_q))$ denote the transcript of the interaction of $\mathcal{A}$ with $\widetilde{P}$. For any two subsets U and V of $\{0,1\}^n$, let*

$$\mu(\widetilde{\mathcal{Q}}, U, V) = |\{((t, x, y), u, v) \in \widetilde{\mathcal{Q}} \times U \times V \;:\; x \oplus u = \Gamma(y \oplus v)\}|.$$

Then, assuming $9n \leq q \leq N/2$, one has

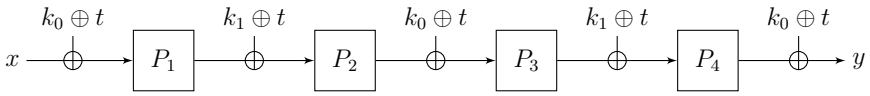

Fig. 2. The 4-round tweakable Even-Mansour construction with a $2n$-bit key (k_0, k_1) and an n-bit tweak t.

$$\Pr_{\widetilde{P},\omega}\left[\exists U, V \subseteq \{0,1\}^n \,:\, \mu(\widetilde{\mathcal{Q}}, U, V) \geq \frac{q|U||V|}{N} + \frac{2q^2\sqrt{|U||V|}}{N} + 3\sqrt{nq|U||V|}\right] \leq \frac{2}{N},$$

where the probability is taken over the random choice of $\widetilde{P}$ *and the random coins* ω *of* $\mathcal{A}$*.*

The proof of this lemma is a simple generalization of the one from [5] and can be found in the full version of this paper [9].

3 Beyond-Birthday-Bound Security

3.1 Statement of the Result and Discussion

In this section, we consider the 4-round tweakable Even-Mansour construction $\mathsf{TEM}[n, 4, \mathbf{f}]$ with $2n$-bit keys and n-bit tweaks depicted on Figure 2. The main result of this paper is the following one:

Theorem 1. *Let* $\mathbf{f} = (f_0, \ldots, f_4)$ *where* $f_i((k_0, k_1), t) = k_{i \bmod 2} \oplus t$*. Let* q_c, q_p *be two integers such that* $9n \leq q_c$ *and* $q_p + 3q_c + 1 \leq N/2$*. Then one has*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,4,\mathbf{f}]}(q_c, q_p) \leq \frac{44q_c^{3/2} + 38q_c\sqrt{q_p} + (30 + 3\sqrt{n})q_p\sqrt{q_c} + 4q_p^{3/2} + 2}{N}.$$

Hence, this construction ensures CCA-security as long as q_c and q_p are small compared to $2^{2n/3}$, up to logarithmic terms in $N = 2^n$.

The proof follows the H-coefficients method exposed in Section 2.3. In Section 3.2, we begin by describing the set of bad transcripts and upper bound the probability to get such a transcript in the ideal world. Then, for any good attainable transcript τ, we prove in Section 3.3 that the ratio between the probability to get τ in the real world and in the ideal world is close enough to 1.

3.2 Definition and Probability of Bad Transcripts

The first step is to define the set of bad transcripts. Let $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_4}, (k_0, k_1))$ be an attainable transcript, with $|\mathcal{Q}_C| = q_c$ and $|\mathcal{Q}_{P_i}| = q_p$ for

$i = 1, \ldots, 4$. In all the following, we let, for $i \in \{1, \ldots, 4\}$,

$$U_i = \{u_i \in \{0,1\}^n : (u_i, v_i) \in \mathcal{Q}_{P_i}\}$$
$$V_i = \{v_i \in \{0,1\}^n : (u_i, v_i) \in \mathcal{Q}_{P_i}\}$$

denote the domains and ranges of $\mathcal{Q}_{P_i}$ respectively. We also define three quantities characterizing the transcript,

$$\alpha_1 \stackrel{\text{def}}{=} |\{((t,x,y), u_1) \in \mathcal{Q}_C \times U_1 \,:\, x \oplus k_0 \oplus t = u_1\}|$$
$$\alpha_4 \stackrel{\text{def}}{=} |\{((t,x,y), v_4) \in \mathcal{Q}_C \times V_4 \,:\, y \oplus k_0 \oplus t = v_4\}|$$
$$\alpha_{2,3} \stackrel{\text{def}}{=} |\{((t,x,y), v_2, u_3) \in \mathcal{Q}_C \times V_2 \times U_3 \,:\, v_2 \oplus k_0 \oplus t = u_3\}|.$$

We also define two quantities depending respectively on $\mathcal{Q}_{P_2}$ and $\mathcal{Q}_{P_3}$:

$$\nu_2 \stackrel{\text{def}}{=} |\{((u_2, v_2), (u_2', v_2')) \in (\mathcal{Q}_{P_2})^2 \,:\, (u_2, v_2) \neq (u_2', v_2'),\, u_2 \oplus v_2 = u_2' \oplus v_2'\}|$$
$$\nu_3 \stackrel{\text{def}}{=} |\{((u_3, v_3), (u_3', v_3')) \in (\mathcal{Q}_{P_3})^2 \,:\, (u_3, v_3) \neq (u_3', v_3'),\, u_3 \oplus v_3 = u_3' \oplus v_3'\}|.$$

Definition 1. *We say that a transcript τ is bad if at least one of the following conditions is fulfilled:*

(B-1) there exists $(t,x,y) \in \mathcal{Q}_C$, $(u_1, v_1) \in \mathcal{Q}_{P_1}$, and $(u_4, v_4) \in \mathcal{Q}_{P_4}$ such that $k_0 \oplus t = x \oplus u_1 = v_4 \oplus y$;
(B-2) there exists $(t,x,y) \in \mathcal{Q}_C$, $(u_1, v_1) \in \mathcal{Q}_{P_1}$, and $(u_2, v_2) \in \mathcal{Q}_{P_2}$ such that $k_0 \oplus t = x \oplus u_1$ and $k_1 \oplus t = v_1 \oplus u_2$;
(B-3) there exists $(t,x,y) \in \mathcal{Q}_C$, $(u_3, v_3) \in \mathcal{Q}_{P_3}$, and $(u_4, v_4) \in \mathcal{Q}_{P_4}$ such that $k_1 \oplus t = v_3 \oplus u_4$ and $k_0 \oplus t = v_4 \oplus y$;
(B-4) $\alpha_1 \geq \sqrt{q_c}/2$;
(B-5) $\alpha_4 \geq \sqrt{q_c}/2$;
(B-6) $\alpha_{2,3} \geq q_p \sqrt{q_c}$;
(B-7) $\nu_2 \geq \sqrt{q_p}$;
(B-8) $\nu_3 \geq \sqrt{q_p}$.

Otherwise we say that τ is good.[5] *We denote Θ_{good}, resp. Θ_{bad} the set of good, resp. bad transcripts.*

We start by upper bounding the probability of getting bad transcripts in the ideal world.

Lemma 3. *Assume that $9n \leq q_c \leq N/2$ and $q_p \leq N/2$. Then one has*

$$\Pr\left[T_{\text{id}} \in \Theta_{\text{bad}}\right] \leq \frac{2q_c^2 q_p + 3q_c q_p^2}{N^2} + \frac{(5 + 3\sqrt{n})\sqrt{q_c} q_p + 4q_p^{3/2} + 2}{N}.$$

Proof. We upper bound the probability of each condition in turn. We denote Θ_i the set of attainable transcripts satisfying condition (B-i). Recall that in the ideal world, the key (k_0, k_1) is drawn independently from the queries transcript.

[5] We define conditions (B-4) and (B-5) using $\sqrt{q_c}/2$ rather than $\sqrt{q_c}$ in order to be able later to directly apply a previous result by Cogliati *et al.* [7].

Condition (B-1). Let BadK_1 be the set of keys k_0 such that there exists $(t, x, y) \in \mathcal{Q}_C$, $(u_1, v_1) \in \mathcal{Q}_{P_1}$, and $(u_4, v_4) \in \mathcal{Q}_{P_4}$ such that $k_0 \oplus t = x \oplus u_1 = y \oplus v_4$. Note that BadK_1 only depends on the queries transcript, hence for any constant C we have, since k_0 is uniformly random,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_1\right] \leq \Pr\left[\widetilde{P}_0 \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n), \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^4 \,:\, |\mathsf{BadK}_1| > C\right] + \frac{C}{N}. \quad (5)$$

Moreover, if we let

$$\mu(\mathcal{Q}_C, U_1, V_4) \stackrel{\mathrm{def}}{=} |\{((t, x, y), u_1, v_4) \in \mathcal{Q}_C \times U_1 \times V_4 \,:\, x \oplus u_1 = y \oplus v_4)\}|,$$

then one clearly has

$$|\mathsf{BadK}_1| \leq \mu(\mathcal{Q}_C, U_1, V_4).$$

Hence, we can use Lemma 2 in order to upper-bound $|\mathsf{BadK}_1|$ with overwhelming probability (we consider $\mathcal{D}$ with access to the inner permutations as a probabilistic algorithm $\mathcal{A}$ interacting with the tweakable permutation $\widetilde{P}_0$, resulting in the transcript $\mathcal{Q}_C$, and we let Γ be the identity mapping). For

$$C = \frac{q_c q_p^2}{N} + \frac{2 q_c^2 q_p}{N} + 3 q_p \sqrt{n q_c},$$

we obtain that

$$\Pr\left[\widetilde{P}_0 \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, n), \mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^4 \,:\, |\mathsf{BadK}_1| > C\right] \leq \frac{2}{N}.$$

Using (5) gives

$$\Pr\left[T_{\mathrm{id}} \in \Theta_1\right] \leq \frac{q_c q_p^2}{N^2} + \frac{2 q_c^2 q_p}{N^2} + \frac{3 q_p \sqrt{n q_c}}{N} + \frac{2}{N}.$$

Conditions (B-2) and (B-3). We consider (B-2). For each $(t, x, y) \in \mathcal{Q}_C$, $(u_1, v_1) \in \mathcal{Q}_{P_1}$, and $(u_2, v_2) \in \mathcal{Q}_{P_2}$, the probability, over the random draw of (k_0, k_1), that $k_0 \oplus t = x \oplus u_1$ and $k_1 \oplus t = v_1 \oplus u_2$ is $1/N^2$ since (k_0, k_1) is uniform and independent from the queries transcript. Summing over the $q_c q_p^2$ possibilities for (t, x, y), (u_1, v_1), and (u_2, v_2) yields

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

Similarly,

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

Conditions (B-4) and (B-5). We consider (B-4). Seeing α_1 as a random variable over the random draw of (k_0, k_1), one has

$$\mathbb{E}[\alpha_1] = \sum_{(t,x,y)\in\mathcal{Q}_C} \sum_{u_1\in U_1} \Pr\left[k_0 = x \oplus u_1 \oplus t\right] \leq \frac{q_c q_p}{N}.$$

Then, using Markov's inequality,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_4\right] = \Pr\left[\alpha_1 \geq \frac{\sqrt{q_c}}{2}\right] \leq \frac{2\mathbb{E}[\alpha_1]}{\sqrt{q_c}} \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Similarly,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_5\right] \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Condition (B-6). Again, we see $\alpha_{2,3}$ as a random variable over the random draw of k_0. Then

$$\mathbb{E}[\alpha_{2,3}] = \sum_{(t,x,y)\in\mathcal{Q}_C} \sum_{v_2\in V_2} \sum_{u_3\in U_3} \Pr\left[k_0 = v_2 \oplus u_3 \oplus t\right] \leq \frac{q_c q_p^2}{N}.$$

Then, using Markov's inequality,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_6\right] = \Pr\left[\alpha_{2,3} \geq q_p\sqrt{q_c}\right] \leq \frac{\mathbb{E}[\alpha_{2,3}]}{q_p\sqrt{q_c}} \leq \frac{q_p\sqrt{q_c}}{N}.$$

Conditions (B-7) and (B-8). Consider (B-7). We see the distinguisher combined with $\widetilde{P}_0$ and the inner permutations P_1, P_3, and P_4 as a probabilistic algorithm $\mathcal{A}$ interacting with P_2, and we see ν_2 as a random variable over the random choice of P_2 and the randomness of $\mathcal{A}$. One has

$$\mathbb{E}[\nu_2] = \sum_{\substack{(i,j)\\1\leq i\neq j\leq q_c}} \Pr\left[u_{2,i} \oplus v_{2,i} = u_{2,j} \oplus v_{2,j}\right],$$

where the queries to P_2 are ordered as they are issued by $\mathcal{A}$. Consider the i-th and the j-th query, and assume *wlog* that $i < j$. If the j-th is a direct query $u_{2,j}$, then $v_{2,j}$ is uniformly random in a set of size $N - j + 1$. Similarly, if this is a inverse query $v_{2,j}$, then $u_{2,j}$ is uniformly random in a set of size $N - j + 1$. In all cases, the probability that $u_{2,i} \oplus v_{2,i} = u_{2,j} \oplus v_{2,j}$ is at most $1/(N - q_p)$. Hence,

$$\mathbb{E}[\nu_2] \leq \frac{q_p(q_p - 1)}{N - q_p} \leq \frac{2q_p^2}{N}.$$

Using Markov's inequality,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_7\right] = \Pr\left[\nu_2 \geq \sqrt{q_p}\right] \leq \frac{2q_p^{3/2}}{N}.$$

Similarly,

$$\Pr\left[T_{\mathrm{id}} \in \Theta_8\right] \leq \frac{2q_p^{3/2}}{N}.$$

The result follows by a union bound over all cases. □

3.3 Analysis of Good Transcripts

In this section, we fix a good transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_4}, (k_0, k_1))$. By (4), we have to lower bound

$$\mathsf{p}(\tau) \stackrel{\text{def}}{=} \Pr\left[\mathbf{P} \leftarrow_{\$} (\mathsf{P}(n))^4 : \mathsf{TEM}^{\mathbf{P}}_{k_0,k_1} \vdash \mathcal{Q}_C \middle| P_1 \vdash \mathcal{Q}_{P_1} \wedge \ldots \wedge P_4 \vdash \mathcal{Q}_{P_4}\right].$$

The proof will proceed in two steps: first, we will lower bound the probability that permutations P_1 and P_4 satisfy some conditions given in the definition below, and then, assuming (P_1, P_4) is good, we will lower bound the probability, over the choice of P_2 and P_3, that $\mathsf{TEM}^{\mathbf{P}}_{k_0,k_1} \vdash \mathcal{Q}_C$. For this second step, we will directly appeal to a previous result by Cogliati *et al.* [7].

We start by giving the conditions defining good pairs of permutations (P_1, P_4). We stress that these conditions cannot be accommodated in the definition of bad transcripts since they depend on values of P_1 and P_4 which do *not* appear in the queries transcript, so that they cannot be defined from the transcript τ alone. We also warn the reader upfront that conditions (C-5) and (C-6) are "dummy" conditions that will easily be seen to be impossible to fulfill, yet will allow us to cleanly use the previous result of Cogliati *et al.* [7].

Definition 2. *A pair of permutations (P_1, P_4) such that $P_1 \vdash \mathcal{Q}_{P_1}$ and $P_4 \vdash \mathcal{Q}_{P_4}$ is said bad if at least one of the following conditions is fulfilled (see Figure 3 for a diagram of the first ten conditions):*

(C-1) there exists $(t, x, y) \in \mathcal{Q}_C$, $u_2 \in U_2$, and $v_3 \in V_3$ such that

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t = u_2 \\ P_4^{-1}(y \oplus k_0 \oplus t) \oplus k_1 \oplus t = v_3; \end{cases}$$

(C-2) there exists $(t, x, y) \in \mathcal{Q}_C$, $(u_2, v_2) \in \mathcal{Q}_{P_2}$, and $u_3 \in U_3$ such that

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t = u_2 \\ v_2 \oplus k_0 \oplus t = u_3; \end{cases}$$

(C-3) there exists $(t, x, y) \in \mathcal{Q}_C$, $(u_3, v_3) \in \mathcal{Q}_{P_3}$, and $v_2 \in V_2$ such that

$$\begin{cases} P_4^{-1}(y \oplus k_0 \oplus t) \oplus k_1 \oplus t = v_3 \\ u_3 \oplus k_0 \oplus t = v_2; \end{cases}$$

(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

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t' \\ P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y'' \oplus k_0 \oplus t'') \oplus t''; \end{cases}$$

(C-5) there exists $(t, x, y,) \neq (t', x', y') \in \mathcal{Q}_C$ such that

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t' \\ t = t'; \end{cases}$$

(C-6) there exists $(t,x,y,) \neq (t',x',y') \in \mathcal{Q}_C$ *such that*

$$\begin{cases} P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y' \oplus k_0 \oplus t') \oplus t' \\ t = t'; \end{cases}$$

(C-7) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ *and* $u_2 \in U_2$ *such that*

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t = u_2 \\ P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y' \oplus k_0 \oplus t') \oplus t'; \end{cases}$$

(C-8) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ *and* $v_3 \in V_3$ *such that*

$$\begin{cases} P_4^{-1}(y \oplus k_0 \oplus t) \oplus k_1 \oplus t = v_3 \\ P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'; \end{cases}$$

(C-9) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ *and* $(u_2,v_2),(u_2',v_2') \in \mathcal{Q}_{P_2}$ *such that*

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t = u_2 \\ P_1(x' \oplus k_0 \oplus t') \oplus k_1 \oplus t' = u_2' \\ v_2 \oplus t = v_2' \oplus t'; \end{cases}$$

(C-10) there exists $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ *and* $(u_3,v_3),(u_3',v_3') \in \mathcal{Q}_{P_3}$ *such that*

$$\begin{cases} P_4^{-1}(y \oplus k_0 \oplus t) \oplus k_1 \oplus t = v_3 \\ P_4^{-1}(y' \oplus k_0 \oplus t') \oplus k_1 \oplus t' = v_3' \\ u_3 \oplus t = u_3' \oplus t'; \end{cases}$$

(C-11) $\alpha_2 \geq \sqrt{q_c}$;
(C-12) $\alpha_3 \geq \sqrt{q_c}$;
(C-13) $\beta_2 \geq \sqrt{q_c}$;
(C-14) $\beta_3 \geq \sqrt{q_c}$;

where

$$\begin{aligned} \alpha_2 &\stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C \,:\, P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t \in U_2\}|, \\ \alpha_3 &\stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C \,:\, P_4^{-1}(y \oplus k_0 \oplus t) \oplus k_1 \oplus t \in V_3\}|, \\ \beta_2 &\stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C \,:\, \exists (t',x',y') \neq (t,x,y), \\ &\qquad P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'\}|, \\ \beta_3 &\stackrel{\text{def}}{=} |\{(t,x,y) \in \mathcal{Q}_C \,:\, \exists (t',x',y') \neq (t,x,y), \\ &\qquad P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y' \oplus k_0 \oplus t') \oplus t'\}|. \end{aligned}$$

Otherwise we say that (P_1,P_4) *is good. We denote* Π_{good}*, resp.* Π_{bad} *the set of good, resp. bad pairs of permutations* (P_1,P_4) *such that* $P_1 \vdash \mathcal{Q}_{P_1}$ *and* $P_4 \vdash \mathcal{Q}_{P_4}$.

In all the following, we denote Π the set of pairs of permutations (P_1,P_4) such that $P_1 \vdash \mathcal{Q}_{P_1}$ and $P_4 \vdash \mathcal{Q}_{P_4}$. The first step towards studying good transcripts will be to upper bound the probability that the pair (P_1,P_4) is bad.

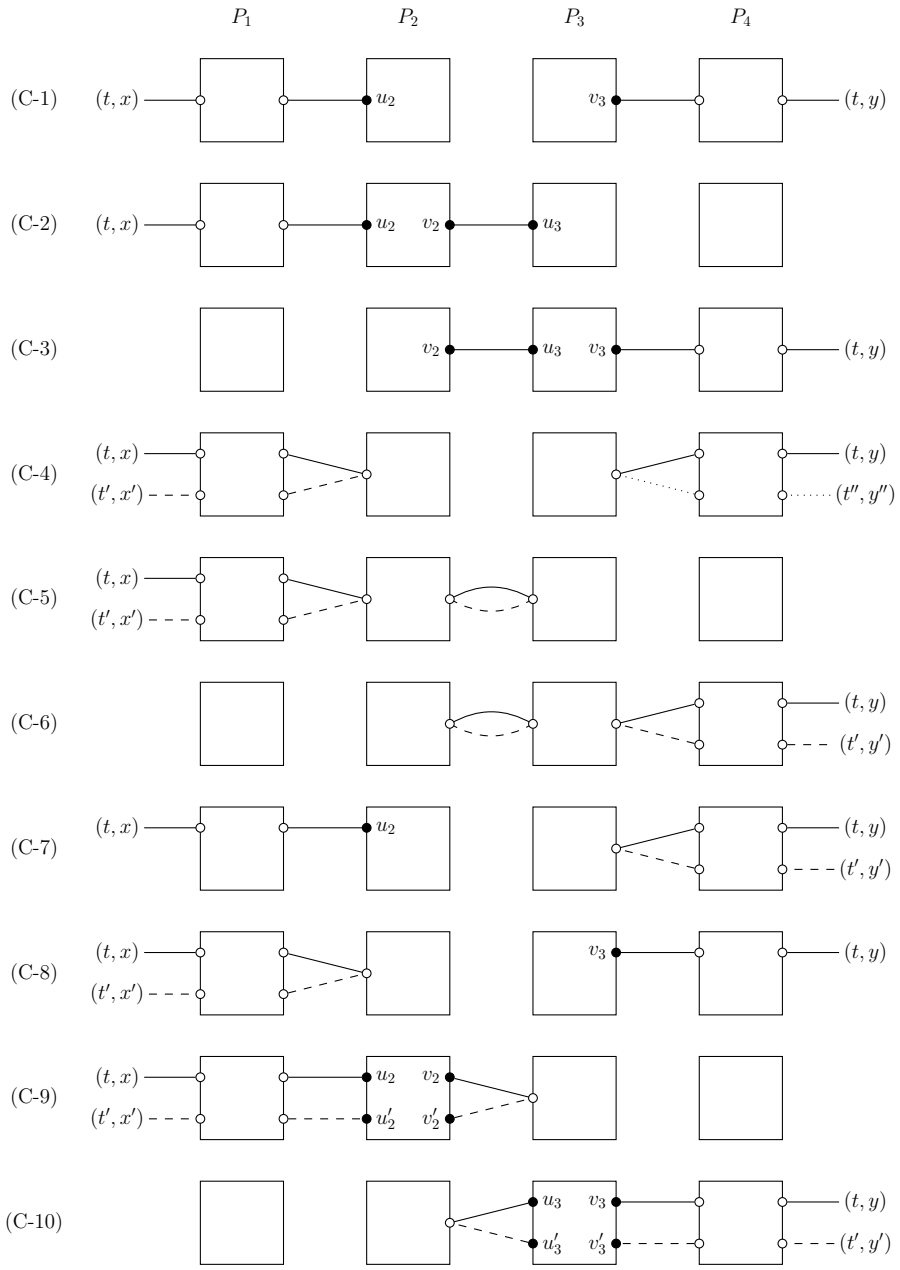

Fig. 3. The ten "collision" conditions characterizing a bad pair of permutations (P_1, P_4). Black dots correspond to pairs $(u_2, v_2) \in \mathcal{Q}_{P_2}$ or $(u_3, v_3) \in \mathcal{Q}_{P_3}$. Note that for (C-4) one might have $(t', x') = (t'', x'')$, and for (C-9) (resp. (C-10)) one might have $x \oplus t = x' \oplus t'$ (resp. $y \oplus t = y' \oplus t'$).

Lemma 4. *For any integers q_c and q_p such that $q_p + q_c + 1 \leq N/2$, one has*

$$\Pr[(P_1, P_4) \in \Pi_{\text{bad}}] \leq \frac{4q_c^3 + 16q_c^2 q_p + 4q_c q_p^2}{N^2} + \frac{10q_c^{3/2} + 4q_c\sqrt{q_p} + 10\sqrt{q_c}q_p}{N}$$

where the probability is taken over the uniformly random draw of (P_1, P_4) in Π.

Proof. We upper bound the probabilities of the fourteen conditions in turn. We denote Π_i the set of pairs of permutations $(P_1, P_4) \in \Pi$ satisfying condition (C-i).

Condition (C-1). Fix $(t, x, y) \in \mathcal{Q}_C$, $u_2 \in U_2$, and $v_3 \in V_3$. Note that if $x \oplus k_0 \oplus t = u_1$ for some $(u_1, v_1) \in \mathcal{Q}_{P_1}$, then $v_1 \oplus k_1 \oplus t$ cannot be equal to u_2 since otherwise τ would satisfy (B-2). Similarly, if $y \oplus k_0 \oplus t = v_4$ for some $(u_4, v_4) \in \mathcal{Q}_{P_4}$, then $u_4 \oplus k_1 \oplus t$ cannot be equal to v_3 since otherwise τ would satisfy (B-3). On the other hand, if $x \oplus k_0 \oplus t \notin U_1$ and $y \oplus k_0 \oplus t \notin V_4$, then the probability over $(P_1, P_4) \leftarrow_\$ \Pi$ that

$$\begin{cases} P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t \\ P_4^{-1}(y \oplus k_0 \oplus t) = v_3 \oplus k_1 \oplus t \end{cases}$$

is at most $1/(N - q_p)^2 \leq 4/N^2$. (In more details, if $u_2 \oplus k_1 \oplus t \in V_1$ or $v_3 \oplus k_1 \oplus t \in U_4$, then this probability is zero, whereas otherwise it is exactly $1/(N - q_p)^2$.) Summing over the at most $q_c q_p^2$ possibilities for (t, x, y), u_2, and v_3 yields

$$\Pr[(P_1, P_4) \in \Pi_1] \leq \frac{4q_c q_p^2}{N^2}.$$

Conditions (C-2) and (C-3). We consider (C-2), the reasoning for (C-3) is similar. Fix $(t, x, y) \in \mathcal{Q}_C$, $(u_2, v_2) \in \mathcal{Q}_{P_2}$, and $u_3 \in U_3$. Note first that for (C-2) to be satisfied, one must have $v_2 \oplus k_0 \oplus t = u_3$, and there are by definition at most $\alpha_{2,3}$ triplets $((t, x, y), v_2, u_3)$ satisfying this equality. If $x \oplus k_0 \oplus t = u_1$ for some $(u_1, v_1) \in \mathcal{Q}_{P_1}$, then $v_1 \oplus k_1 \oplus t$ cannot be equal to u_2 since otherwise τ would satisfy (B-2). On the other hand, if $x \oplus k_0 \oplus t \notin U_1$, then the probability that $P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t$ is at most $1/(N - q_p) \leq 2/N$ (it is zero if $u_2 \oplus k_1 \oplus t \in V_1$, and $1/(N - q_p)$ otherwise). Summing over the at most $\alpha_{2,3}$ possibilities for (t, x, y), (u_2, v_2), and u_3, with $\alpha_{2,3} \leq q_p\sqrt{q_c}$ since otherwise τ would satisfy (B-6), we obtain

$$\Pr[(P_1, P_4) \in \Pi_2] \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Similarly,

$$\Pr[(P_1, P_4) \in \Pi_3] \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Condition (C-4). Fix $(t,x,y),(t',x',y'),(t'',x'',y'') \in \mathcal{Q}_C$ with (t,x,y) distinct from (t',x',y') and from (t'',x'',y''). First, note that if $x \oplus k_0 \oplus t = x' \oplus k_0 \oplus t'$ or $y \oplus k_0 \oplus t = y'' \oplus k_0 \oplus t''$, then (C-4) cannot be satisfied. Hence, we assume that none of these two equalities holds. We consider three cases. Assume first that $x \oplus k_0 \oplus t = u_1$ for some $(u_1, v_1) \in \mathcal{Q}_{P_1}$. Note that there are at most α_1 possibilities for (t,x,y), and $\alpha_1 \leq \sqrt{q_c}/2$ since otherwise τ would satisfy (B-4). Moreover $y \oplus k_0 \oplus t \notin V_4$ since otherwise τ would satisfy (B-1). Hence, the probability that

$$P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y'' \oplus k_0 \oplus t'') \oplus t''$$

is at most $1/(N - q_p - 1) \leq 2/N$. (In more details, if $y'' \oplus k_0 \oplus t'' \in V_4$, then this probability is either zero if $P_4^{-1}(y'' \oplus k_0 \oplus t'') \oplus t \oplus t'' \in U_4$, or exactly $1/(N-q_p)$ otherwise, whereas if $y'' \oplus k_0 \oplus t'' \notin V_4$, then this probability is at most $1/(N-q_p-1)$.) Summing over the at most $\sqrt{q_c}/2 \times q_c$ possibilities for (t,x,y) and (t'',x'',y''), the probability of this first case is at most $q_c^{3/2}/N$. The second case where $y \oplus k_0 \oplus t \in V_4$ is handled similarly. Finally, consider the case where $x \oplus k_0 \oplus t \notin U_1$ and $y \oplus k_0 \oplus t \notin V_4$. Then the probability that

$$\begin{cases} P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t' \\ P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y'' \oplus k_0 \oplus t'') \oplus t''; \end{cases}$$

is at most $1/(N-q_p-1)^2 \leq 4/N^2$. Summing over the at most q_c^3 possibilities for (t,x,y), (t',x',y'), and (t'',x'',y''), the probability of this third case is at most $4q_c^3/N^2$. Overall, we obtain

$$\Pr[(P_1,P_4) \in \Pi_4] \leq \frac{4q_c^3}{N^2} + \frac{2q_c^{3/2}}{N}.$$

Conditions (C-5) and (C-6). These conditions cannot be satisfied. Indeed, assume that there exits $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ satisfying (C-5). Since $t = t'$, then $x \neq x'$ by the assumption that the distinguisher never makes pointless queries. This obviously implies that $P_1(x \oplus k_0 \oplus t) \oplus t \neq P_1(x' \oplus k_0 \oplus t') \oplus t'$, a contradiction. The reasoning is similar for (C-6). Hence,

$$\Pr[(P_1,P_4) \in \Pi_5] = \Pr[(P_1,P_4) \in \Pi_6] = 0.$$

Conditions (C-7) and (C-8). We consider condition (C-7). Fix queries $(t,x,y) \neq (t',x',y') \in \mathcal{Q}_C$ and $u_2 \in U_2$. We will consider two cases: first, the case where $y \oplus k_0 \oplus t \in V_4$, and then the case where $y \oplus k_0 \oplus t \notin V_4$. For both cases, note that if $x \oplus k_0 \oplus t = u_1$ for some $(u_1, v_1) \in \mathcal{Q}_{P_1}$, then $v_1 \oplus k_1 \oplus t$ cannot be equal to u_2 since otherwise τ would satisfy (B-2). Hence, we can assume that $x \oplus k_0 \oplus t \notin U_1$. It follows that the probability that

$$P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t = u_2$$

is at most $1/(N-q_p) \leq 2/N$ (it is zero if $u_2 \oplus k_1 \oplus t \in V_1$, and $1/(N-q_p)$ otherwise). Summing over the at most α_4 queries $(t,x,y) \in \mathcal{Q}_C$ such that $y \oplus k_0 \oplus t \in V_4$,

with $\alpha_4 \leq \sqrt{q_c}/2$ since otherwise τ would satisfy (B-5), and the q_p possibilities for u_2, we see that the first case happens with probability at most $q_p\sqrt{q_c}/N$. Assume now that $y \oplus k_0 \oplus t \notin V_4$. Then the probability that

$$P_4^{-1}(y \oplus k_0 \oplus t) \oplus t = P_4^{-1}(y' \oplus k_0 \oplus t') \oplus t'$$

is at most $1/(N - q_p - 1) \leq 2/N$. (In more details, if $y \oplus k_0 \oplus t = y' \oplus k_0 \oplus t'$, then it can easily be seen that it cannot hold, whereas if $y \oplus k_0 \oplus t \neq y' \oplus k_0 \oplus t'$, the equation holds with probability at most $1/(N - q_p - 1)$.) Summing over the at most $q_c^2 q_p$ possibilities for (t, x, y), (t', x', y'), and u_2, we see that the probability of the second case is at most $4q_c^2 q_p/N^2$. Overall,

$$\Pr\left[(P_1, P_4) \in \Pi_7\right] \leq \frac{q_p\sqrt{q_c}}{N} + \frac{4q_c^2 q_p}{N^2}.$$

Similarly, one has

$$\Pr\left[(P_1, P_4) \in \Pi_8\right] \leq \frac{q_p\sqrt{q_c}}{N} + \frac{4q_c^2 q_p}{N^2}.$$

Conditions (C-9) and (C-10). Consider condition (C-9). First note that, if the condition is satisfied, we have $x \oplus k_0 \oplus t \notin U_1$, $x' \oplus k_0 \oplus t' \notin U_1$, $u_2 \oplus k_1 \oplus t \notin V_1$ and $u_2' \oplus k_1 \oplus t' \notin V_1$, otherwise (B-2) is fulfilled. Moreover, if $(u_2, v_2) = (u_2', v_2')$, then $t = t'$, thus $x = x'$, which is impossible. Hence we must have $(u_2, v_2) \neq (u_2', v_2')$. The condition can be divided into two conditions:

9.1 there exists $(t, x, y) \neq (t', x', y') \in \mathcal{Q}_C$ and $(u_2, v_2) \neq (u_2', v_2') \in \mathcal{Q}_{P_2}$ such that $x \oplus t = x' \oplus t'$, $P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t$ and $P_1(x' \oplus k_0 \oplus t') = u_2' \oplus k_1 \oplus t'$ and $v_2 \oplus t = v_2' \oplus t'$;

9.2 there exists $(t, x, y) \neq (t', x', y') \in \mathcal{Q}_C$ and $(u_2, v_2) \neq (u_2', v_2') \in \mathcal{Q}_{P_2}$ such that $x \oplus t \neq x' \oplus t'$, $P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t$ and $P_1(x' \oplus k_0 \oplus t') = u_2' \oplus k_1 \oplus t'$ and $v_2 \oplus t = v_2' \oplus t'$.

In the first case, one has

$$u_2 \oplus k_1 \oplus t = P_1(x \oplus k_0 \oplus t) = P_1(x' \oplus k_0 \oplus t') = u_2' \oplus k_1 \oplus t',$$

thus $u_2 \oplus u_2' = t \oplus t' = v_2 \oplus v_2'$. Hence the first condition implies the following one: there exists $(t, x, y) \in \mathcal{Q}_C$ and $(u_2, v_2) \neq (u_2', v_2') \in \mathcal{Q}_{P_2}$ such that $P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t$ and $u_2 \oplus u_2' = v_2 \oplus v_2'$, with $x \oplus k_0 \oplus t \notin U_1$ and $u_2 \oplus k_1 \oplus t \notin V_1$. Since $\nu_2 < \sqrt{q_p}$, the number of suitable $u_2 \in U_2$ is lower than $\sqrt{q_p}$, and the probability that this first condition is fulfilled is at most $\frac{q_c\sqrt{q_p}}{N - q_p} \leq \frac{2q_c\sqrt{q_p}}{N}$. For the second condition, fix any queries $(t, x, y) \neq (t', x', y') \in \mathcal{Q}_C$ such that $x \oplus t \neq x' \oplus t'$, $x \oplus k_0 \oplus t \notin U_1$, $x' \oplus k_0 \oplus t' \notin U_1$ and $(u_2, v_2) \in \mathcal{Q}_{P_2}$. If $v_2 \oplus t \oplus t' \notin V_2$, the condition cannot be fulfilled. Otherwise let $(u_2', v_2') \in \mathcal{Q}_{P_2}$ be the unique query such that $v_2 \oplus t = v_2' \oplus t'$. Then the probability that $P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t$ and $P_1(x' \oplus k_0 \oplus t') = u_2' \oplus k_1 \oplus t'$ is at most $\frac{1}{(N - q_p)(N - q_p - 1)}$. Finally, by summing

over every possible tuple of queries, and by taking into account the condition 9.1, one has

$$\Pr\left[(P_1, P_4) \in \Pi_9\right] \leq \frac{2q_c\sqrt{q_p}}{N} + \frac{4q_c^2 q_p}{N^2}.$$

Similarly,

$$\Pr\left[(P_1, P_4) \in \Pi_{10}\right] \leq \frac{2q_c\sqrt{q_p}}{N} + \frac{4q_c^2 q_p}{N^2}.$$

Conditions (C-11) and (C-12). We see α_2 (resp. α_3) as a random variable over the choice of P_1 (resp. P_4). Note that

$$\begin{aligned}\alpha_2 &= |\{(t,x,y) \in \mathcal{Q}_C \,:\, P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t \in U_2\}| \\ &= |\{(t,x,y) \in \mathcal{Q}_C \,:\, x \oplus k_0 \oplus t \notin U_1,\, P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t \in U_2\}|,\end{aligned}$$

because, if $x \oplus k_0 \oplus t \in U_1$ and $P_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t \in U_2$, then (B-2) is fulfilled. We denote $\mathcal{Q}_{C,1}$ the subset of queries $(t,x,y) \in \mathcal{Q}_C$ such that $x \oplus k_0 \oplus t \notin U_1$. Then

$$\begin{aligned}\mathbb{E}[\alpha_2] &= \sum_{(t,x,y)\in\mathcal{Q}_{C,1}} \sum_{u_2 \in U_2} \Pr\left[P_1(x \oplus k_0 \oplus t) = u_2 \oplus k_1 \oplus t\right] \\ &\leq \sum_{(t,x,y)\in\mathcal{Q}_{C,1}} \sum_{u_2 \in U_2} \frac{1}{N - q_p} \\ &\leq \frac{2q_c q_p}{N}.\end{aligned}$$

Using Markov's inequality, we get

$$\Pr\left[(P_1, P_4) \in \Pi_{11}\right] \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Similarly,

$$\Pr\left[(P_1, P_4) \in \Pi_{12}\right] \leq \frac{2q_p\sqrt{q_c}}{N}.$$

Conditions (C-13) and (C-14). Consider condition (C-13). Note that

$$\begin{aligned}\beta_2 &= |\{(t,x,y) \in \mathcal{Q}_C \,:\, \exists (t',x',y') \neq (t,x,y), \\ &\qquad P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'\}| \\ &\leq \alpha_1 + |\{(t,x,y) \in \mathcal{Q}_C \,:\, x \oplus k_0 \oplus t \notin U_1 \text{ and } \exists (t',x',y') \neq (t,x,y), \\ &\qquad P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'\}|.\end{aligned}$$

We denote β_2' the last term of this sum. Thus

$$\begin{aligned}\mathbb{E}[\beta_2'] &= \sum_{(t,x,y)\in\mathcal{Q}_{C,1}} \sum_{(t',x',y')\neq(t,x,y)} \Pr\left[P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'\right] \\ &\leq \frac{q_c^2}{N - q_p - 1} \leq \frac{2q_c^2}{N}.\end{aligned}$$

This inequality holds because, if $x \oplus t = x' \oplus t'$, then $t \neq t'$ since the distinguisher never makes pointless queries, thus $P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'$ cannot be fulfilled. Otherwise,

$$\Pr\left[P_1(x \oplus k_0 \oplus t) \oplus t = P_1(x' \oplus k_0 \oplus t') \oplus t'\right] \leq \frac{1}{N - q_p - 1}.$$

Finally, since (B-4) is not fulfilled, $\alpha_1 < \sqrt{q_c}/2$. Thus $\beta_2 \geq \sqrt{q_c}$ implies $\beta_2' \geq \sqrt{q_c}/2$. Hence, using Markov's inequality,

$$\Pr\left[(P_1, P_4) \in \mathit{\Pi}_{13}\right] \leq \Pr\left[\beta_2' \geq \sqrt{q_c}/2\right] \leq \frac{2\mathbb{E}[\beta_2']}{\sqrt{q_c}} \leq \frac{4q_c^{3/2}}{N}.$$

Similarly,

$$\Pr\left[(P_1, P_4) \in \mathit{\Pi}_{14}\right] \leq \frac{4q_c^{3/2}}{N}.$$

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

We are now ready for the second step of the reasoning.

Definition 3. *Fix any pair of permutations (P_1, P_4) such that $P_1 \vdash \mathcal{Q}_{P_1}$ and $P_4 \vdash \mathcal{Q}_{P_4}$. We define a new query transcript $\mathcal{Q}'_C$ depending on (P_1, P_4) as*

$$\mathcal{Q}'_C = \{(t, P_1(x \oplus k_0 \oplus t), P_4^{-1}(y \oplus k_0 \oplus t)) : (t, x, y) \in \mathcal{Q}_C\}.$$

We also denote

$$\tilde{\mathsf{p}}(\tau, P_1, P_4) = \Pr\left[P_2, P_3 \leftarrow_{\$} \mathsf{P}(n) : \mathsf{TEM}_{k_1,k_0}^{P_2,P_3} \vdash \mathcal{Q}'_C \,\middle|\, (P_2 \vdash \mathcal{Q}_{P_2}) \wedge (P_3 \vdash \mathcal{Q}_{P_3})\right].$$

Lemma 5. *One has*

$$\frac{\Pr\left[T_{\mathrm{re}} = \tau\right]}{\Pr\left[T_{\mathrm{id}} = \tau\right]} \geq \sum_{(P_1,P_4) \in \mathit{\Pi}_{\mathrm{good}}} \frac{\tilde{\mathsf{p}}(\tau, P_1, P_4)}{\left((N - q_p)!\right)^2 \prod_{i=1}^{m} 1/(N)_{q_i}}.$$

Proof. Clearly, once P_1 and P_4 are fixed, $\mathsf{TEM}_{k_0,k_1}^{P_1,P_2,P_3,P_4} \vdash \mathcal{Q}_C$ is equivalent to $\mathsf{TEM}_{k_1,k_0}^{P_2,P_3} \vdash \mathcal{Q}'_C$. Hence,

$$\begin{aligned}
\mathsf{p}(\tau) &= \sum_{(\bar{P}_1,\bar{P}_4) \in \mathit{\Pi}} \Pr\left[(P_1, P_4) \leftarrow_{\$} \mathit{\Pi} : (P_1 = \bar{P}_1) \wedge (P_4 = \bar{P}_4)\right] \tilde{\mathsf{p}}(\tau, \bar{P}_1, \bar{P}_4) \\
&\geq \sum_{(\bar{P}_1,\bar{P}_4) \in \mathit{\Pi}_{\mathrm{good}}} \frac{\tilde{\mathsf{p}}(\tau, \bar{P}_1, \bar{P}_4)}{((N - q_p)!)^2}.
\end{aligned}$$

The result follows from Eq. (4). □

We can now directly appeal to a previous result by Cogliati *et al.* [7].

Lemma 6. *Let q_c and q_p be two positive integers such that $q_p + 3q_c \leq N/2$. Fix any pair of permutations $(P_1, P_4) \in \Pi_{\text{good}}$. Then*

$$\frac{\tilde{\mathsf{p}}(\tau, P_1, P_4)}{\prod_{i=1}^{m} 1/(N)_{q_i}} \geq 1 - \left(\frac{4q_c(q_p + 2q_c)^2}{N^2} + \frac{14q_c^{3/2} + 4\sqrt{q_c}q_p}{N} \right).$$

Proof. One can check that the queries transcript $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$ satisfies exactly the conditions defining a good transcript as per [7, Definition 2]. Moreover, the ratio $\tilde{\mathsf{p}}(\tau, P_1, P_4)/\prod_{i=1}^{m} 1/(N)_{q_i}$ is exactly the ratio of the probabilities to get τ' in the real and in the ideal world once a good pair (P_1, P_4) is fixed. Hence, we can apply [7, Lemma 6] that directly yields the result.[6] □

We are now ready to prove the main lemma of this section.

Lemma 7. *Let q_c and q_p be two positive integers such that $q_p + 3q_c + 1 \leq N/2$. One has*

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \frac{20q_c^3 + 32q_c^2 q_p + 8q_c q_p^2}{N^2} - \frac{24q_c^{3/2} + 4q_c\sqrt{q_p} + 14\sqrt{q_c}q_p}{N}.$$

Proof. From Lemmas 5 and 6, one has

$$\begin{aligned}
\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} &\geq \sum_{(P_1,P_4)\in\Pi_{\text{good}}} \frac{\tilde{\mathsf{p}}(\tau, P_1, P_4)}{((N-q_p)!)^2 \prod_{i=1}^{m} 1/(N)_{q_i}} \\
&\geq \left(1 - \frac{4q_c(q_p + 2q_c)^2}{N^2} - \frac{14q_c^{3/2} + 4\sqrt{q_c}q_p}{N}\right) \sum_{\Pi_{\text{good}}} \frac{1}{((N-q_p)!)^2} \\
&= \left(1 - \frac{4q_c(q_p + 2q_c)^2}{N^2} - \frac{14q_c^{3/2} + 4\sqrt{q_c}q_p}{N}\right) \frac{|\Pi_{\text{good}}|}{((N-q_p)!)^2} \\
&= \left(1 - \frac{4q_c(q_p + 2q_c)^2}{N^2} - \frac{14q_c^{3/2} + 4\sqrt{q_c}q_p}{N}\right) \Pr[(P_1, P_4) \in \Pi_{\text{good}}],
\end{aligned}$$

where the last probability is taken over the random draw of (P_1, P_4) from Π, the set of pairs of permutations satisfying $P_1 \vdash \mathcal{Q}_{P_1}$ and $P_4 \vdash \mathcal{Q}_{P_4}$. Using Lemma 4, one has

$$\begin{aligned}
\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} &\geq \left(1 - \frac{4q_c^3 + 16q_c^2 q_p + 4q_c q_p^2}{N^2} - \frac{10q_c^{3/2} + 4q_c\sqrt{q_p} + 10\sqrt{q_c}q_p}{N}\right) \\
&\quad \times \left(1 - \frac{4q_c(q_p + 2q_c)^2}{N^2} - \frac{14q_c^{3/2} + 4\sqrt{q_c}q_p}{N}\right) \\
&\geq 1 - \frac{20q_c^3 + 32q_c^2 q_p + 8q_c q_p^2}{N^2} - \frac{24q_c^{3/2} + 4q_c\sqrt{q_p} + 14\sqrt{q_c}q_p}{N}.
\end{aligned}$$

□

[6] Even though this might not be apparent to the reader unfamiliar with [7], the proof of Lemma 6 in that paper does not rely on the xor-universal hash functions h_1 and h_2 appearing in the definition of good transcripts of [7].

CONCLUDING. We are now ready to prove Theorem 1. Combining Lemmas 1, 3, and 7, one has

$$\begin{aligned}\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,4,\mathbf{f}]}(q_c,q_p) &\le \frac{2q_c^2q_p+3q_cq_p^2}{N^2}+\frac{(5+3\sqrt{n})\sqrt{q_c}q_p+4q_p^{3/2}+2}{N}\\ &\quad+\frac{20q_c^3+32q_c^2q_p+8q_cq_p^2}{N^2}+\frac{24q_c^{3/2}+4q_c\sqrt{q_p}+14\sqrt{q_c}q_p}{N}\\ &\le \frac{20q_c^3+34q_c^2q_p+11q_cq_p^2}{N^2}\\ &\quad+\frac{24q_c^{3/2}+4q_c\sqrt{q_p}+(19+3\sqrt{n})\sqrt{q_c}q_p+4q_p^{3/2}+2}{N}.\end{aligned}$$

Since the result holds trivially when $q_c^3 > N^2$, $q_c^2q_p > N^2$, or $q_cq_p^2 > N^2$, we can assume that $q_c^3 \le N^2$, $q_c^2q_p \le N^2$, and $q_cq_p^2 \le N^2$, so that

$$\frac{q_c^3}{N^2} \le \frac{q_c^{3/2}}{N}, \quad \frac{q_c^2q_p}{N^2} \le \frac{q_c\sqrt{q_p}}{N}, \quad \text{and} \quad \frac{q_cq_p^2}{N^2} \le \frac{\sqrt{q_c}q_p}{N}.$$

Thus

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{TEM}[n,4,\mathbf{f}]}(q_c,q_p) \le \frac{44q_c^{3/2}+38q_c\sqrt{q_p}+(30+3\sqrt{n})q_p\sqrt{q_c}+4q_p^{3/2}+2}{N},$$

which concludes the proof of Theorem 1.

Acknowledgment

We wish to thank the anonymous reviewers of ASIACRYPT 2015 for their useful suggestions.

References

[1] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, E. Tischhauser, and K. Yasuda. Parallelizable and Authenticated Online Ciphers. In *Advances in Cryptology - ASIACRYPT 2013 - Proceedings, Part I*, volume 8269 of *LNCS*, pages 424–443. Springer, 2013.

[2] M. Bellare and T. Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 491–506. Springer, 2003.

[3] A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. P. Steinberger, and E. Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 45–62. Springer, 2012.

[4] D. Chakraborty and P. Sarkar. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. In *Information Security and Cryptology - Inscrypt 2006*, volume 4318 of *LNCS*, pages 88–102. Springer, 2006.

[5] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. P. Steinberger. Minimizing the Two-Round Even-Mansour Cipher. In *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.

[6] S. Chen and J. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.

[7] B. Cogliati, R. Lampe, and Y. Seurin. Tweaking Even-Mansour Ciphers. In *Advances in Cryptology - CRYPTO 2015 - Proceedings, Part I*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015. Full version available at http://eprint.iacr.org/2015/539.

[8] B. Cogliati and Y. Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In *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.

[9] B. Cogliati and Y. Seurin. Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing. Full version of this paper. Available at http://eprint.iacr.org/2015/851.

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

[11] J. Daemen and V. Rijmen. The Wide Trail Design Strategy. In *Cryptography and Coding 2001*, volume 2260 of *LNCS*, pages 222–238. Springer, 2001.

[12] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir. Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. In *Advances in Cryptology - ASIACRYPT 2014 (Proceedings, Part I)*, volume 8873 of *LNCS*, pages 439–457. Springer, 2014. Full version available at http://eprint.iacr.org/2013/674.

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

[14] P. Farshim and G. Procter. The Related-Key Security of Iterated Even-Mansour Ciphers. In *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 342–363. Springer, 2015. Full version available at http://eprint.iacr.org/2014/953.

[15] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker. The Skein Hash Function Family. SHA3 Submission to NIST (Round 3), 2010.

[16] D. Goldenberg, S. Hohenberger, M. Liskov, E. C. Schwartz, and H. Seyalioglu. On Tweaking Luby-Rackoff Blockciphers. In *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 342–356. Springer, 2007.

[17] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED Block Cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.

[18] S. Halevi and P. Rogaway. A Tweakable Enciphering Mode. In *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.

[19] S. Halevi and P. Rogaway. A Parallelizable Enciphering Mode. In *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.

[20] J. Jean, I. Nikolic, and T. Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In *Advances in Cryptology - ASIACRYPT 2014 - Proceedings, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

[21] R. Lampe, J. Patarin, and Y. Seurin. An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 278–295. Springer, 2012.

[22] R. Lampe and Y. Seurin. Security Analysis of Key-Alternating Feistel Ciphers. In *Fast Software Encryption - FSE 2014*, volume 8540 of *LNCS*, pages 243–264. Springer, 2014.

[23] W. Landecker, T. Shrimpton, and R. S. Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012. Full version available at http://eprint.iacr.org/2012/450.

[24] M. Liskov, R. L. Rivest, and D. Wagner. Tweakable Block Ciphers. In *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

[25] B. Mennink. Optimally Secure Tweakable Blockciphers. In *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 428–448. Springer, 2015. Full version available at http://eprint.iacr.org/2015/363.

[26] K. Minematsu. Improved Security Analysis of XEX and LRW Modes. In *Selected Areas in Cryptography - SAC 2006*, volume 4356 of *LNCS*, pages 96–113. Springer, 2006.

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

[28] A. Mitsuda and T. Iwata. Tweakable Pseudorandom Permutation from Generalized Feistel Structure. In *ProvSec 2008*, volume 5324 of *LNCS*, pages 22–37. Springer, 2008.

[29] J. Patarin. The "Coefficients H" Technique. In *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.

[30] G. 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.

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

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

[33] P. Rogaway and H. Zhang. Online Ciphers from Tweakable Blockciphers. In *Topics in Cryptology - CT-RSA 2011*, volume 6558 of *LNCS*, pages 237–249. Springer, 2011.

[34] Y. Sasaki, Y. Todo, K. Aoki, Y. Naito, T. Sugawara, Y. Murakami, M. Matsui, and S. Hirose. Minalpher v1. Submission to the CAESAR competition, 2014.

[35] R. Schroeppel. The Hasty Pudding Cipher. AES submission to NIST, 1998.

[36] J. 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.