Minimizing the Two-Round Even-Mansour Cipher*

Shan Chen**, Rodolphe Lampe***, Jooyoung Lee†, Yannick Seurin‡, and John Steinberger**

June 9, 2014

Abstract. The r-round (iterated) *Even-Mansour cipher* (also known as *key-alternating cipher*) defines a block cipher from r fixed public n-bit permutations $P_1, \ldots, P_r$ as follows: given a sequence of n-bit round keys $k_0, \ldots, k_r$, an n-bit plaintext x is encrypted by xoring round key k_0, applying permutation P_1, xoring round key k_1, etc. The (strong) pseudorandomness of this construction in the random permutation model (i.e., when the permutations $P_1, \ldots, P_r$ are public random permutation oracles that the adversary can query in a black-box way) was studied in a number of recent papers, culminating with the work of Chen and Steinberger (EUROCRYPT 2014), who proved that the r-round Even-Mansour cipher is indistinguishable from a truly random permutation up to $\mathcal{O}(2^{\frac{rn}{r+1}})$ queries of any adaptive adversary (which is an optimal security bound since it matches a simple distinguishing attack). All results in this entire line of work share the common restriction that they only hold under the assumption that *the round keys $k_0, \ldots, k_r$ and the permutations $P_1, \ldots, P_r$ are independent*. In particular, for two rounds, the current state of knowledge is that the block cipher $E(x) = k_2 \oplus P_2(k_1 \oplus P_1(k_0 \oplus x))$ is provably secure up to $\mathcal{O}(2^{2n/3})$ queries of the adversary, when k_0, k_1, and k_2 are three independent n-bit keys, and P_1 and P_2 are two independent random n-bit permutations. In this paper, we ask whether one can obtain a similar bound for the two-round Even-Mansour cipher *from just one n-bit key and one n-bit permutation*. Our answer is positive: when the three n-bit round keys k_0, k_1, and k_2 are adequately derived from an n-bit master key k, and the same permutation P is used in place of P_1 and P_2, we prove a qualitatively similar $\widetilde{\mathcal{O}}(2^{2n/3})$ security bound (in the random permutation model). To the best of our knowledge, this is the first "beyond the birthday bound" security result for AES-like ciphers that does not assume independent round keys.

Keywords: generalized Even-Mansour cipher, key-alternating cipher, indistinguishability, pseudorandom permutation, random permutation model, sum-capture problem

** Tsinghua University, P.R. China. E-mail: dragoncs16@gmail.com, jpsteinb@gmail.com. These authors were supported by National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 61033001, 61361136003, and by the China Ministry of Education grant number 20121088050.

*** University of Versailles, France. E-mail: rodolphe.lampe@gmail.com. This author was supported by the French Direction Générale de l'Armement and the French National Agency of Research through the PRINCE project (contract ANR-10-SEGI-015).

† Sejong University, Seoul, Korea. E-mail: jlee05@sejong.ac.kr. This author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2007488).

‡ 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).

Table of Contents

1 Introduction

BACKGROUND. An elementary way to construct a block cipher with message space $\{0,1\}^n$ from r fixed and public n-bit permutations $P_1, \ldots P_r$ is to encrypt a plaintext x by computing

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

where $(k_0, \ldots, k_r)$ is a sequence of n-bit round keys which are usually derived from some master key K. This construction, which captures the high-level structure of (most) block cipher designs known as Substitution-Permutation Networks (SPNs), such as AES [DR02], PRESENT [BKL+07], or LED [GPPR11] to name a few, was coined a *key-alternating cipher* by Daemen and Rijmen [DR05].

For concrete designs, where permutations $P_1, \ldots, P_r$ are fixed, the current state of art of provable security only allows to upper bound the success probability of very specific attacks such as differential or linear attacks. On the other hand, it is possible to obtain broader provable security results by working in the random permutation model for $P_1, \ldots, P_r$, i.e., by viewing permutations $P_1, \ldots, P_r$ as public random permutation oracles, to which the adversary can only make black-box queries (both in the forward and backward direction). This is a very strong model, but this allows to upper bound the advantage of any (even computationally unbounded) adversary as a function of the number of queries it makes. It also heuristically indicates that any adversary willing to beat the proven security bound cannot be "generic" and must somehow take advantage of some particular property of the permutations used in any concrete block cipher.

Such results in the random permutation model were first obtained for $r = 1$ round by Even and Mansour [EM97], who showed that the block cipher encrypting x into $k_1 \oplus P_1(k_0 \oplus x)$, where k_0 and k_1 are independent n-bit keys, and P_1 is a random permutation oracle, is secure up to $\mathcal{O}(2^{n/2})$ queries of the adversary.[1] For this reason, this construction is often referred to as the *Even-Mansour cipher*, though this is somehow a misnomer since this is rather a framework in which one can conveniently analyze the security of the family of one-round key-alternating ciphers. In the following, we will perpetuate this unfortunate terminology and use the naming *r-round iterated Even-Mansour cipher* to designate the "ideal" r-round key-alternating cipher where $P_1, \ldots, P_r$ are public and perfectly random permutation oracles. Curiously, the general construction with $r > 1$ remained unstudied for a long while until a paper by Bogdanov *et al.* [BKL+12], who showed that for $r \geq 2$, security is guaranteed up to $\mathcal{O}(2^{2n/3})$ queries of the adversary. They also conjectured that the security should be $\mathcal{O}(2^{\frac{rn}{r+1}})$ for general r, which matches a simple distinguishing attack. Progress towards solving this conjecture was rather quick: Steinberger [Ste12] proved security up to $\mathcal{O}(2^{3n/4})$ queries for $r \geq 3$, Lampe *et al.* [LPS12] proved security up to $\mathcal{O}(2^{\frac{rn}{r+2}})$ queries for any even r, and finally Chen and Steinberger [CS14] resolved the conjecture and proved the $\mathcal{O}(2^{\frac{rn}{r+1}})$-security bound for any r. We stress that *all these results* only hold assuming that the $r+1$ round keys and the r permutations are independent. Actually, this is not perfectly accurate: one only needs the $r+1$ round keys $(k_0, \ldots, k_r)$ to be r-wise independent [CS14], which can be obtained from only an rn-bit long master key, the most simple example being round keys of the form $(k'_1, k'_1 \oplus k'_2, k'_2 \oplus k'_3, \ldots, k'_{r-1} \oplus k'_r, k'_r)$, in which case the resulting iterated Even-Mansour cipher is exactly the cascade of r single-key one-round Even-Mansour ciphers $x \mapsto k'_i \oplus P_i(k'_i \oplus x)$.

[1] Actually it is not very hard to prove that a similar result holds when using $k_0 = k_1$, see [DKS12].

Our Problem. Let us quickly recapitulate existing provable security results on the Even-Mansour cipher for a low number of rounds. For $r = 1$, we know that the single-key Even-Mansour cipher $x \mapsto k \oplus P(k \oplus x)$ ensures security up to $\mathcal{O}(2^{n/2})$ queries of the adversary. As pointed out by Dunkelman *et al.* [DKS12], this construction is "minimal" in the sense that if one removes any component (either the addition of one of the keys, or the permutation P), the construction becomes trivially breakable. For the two-round Even-Mansour cipher, the best provable security result we have so far requires two independent n-bit permutations P_1 and P_2, and two independent n-bit keys (k, k') to construct three pairwise independent round keys, for example $(k, k' \oplus k, k')$. Concretely, the block cipher $x \mapsto k' \oplus P_2((k' \oplus k) \oplus P_1(k \oplus x))$ ensures security up to $\mathcal{O}(2^{2n/3})$ queries of the adversary. In this paper, we tackle the following question:

> *Can we obtain a $\mathcal{O}(2^{2n/3})$-security bound similar to the one proven for the two-round Even-Mansour cipher with (pairwise) independent round keys and independent permutations, from just one n-bit key k and one n-bit random permutation P?*

This question is natural since in most (if not all) SPN block ciphers, round keys are derived from an n-bit master key (or more generally an ℓ-bit master key, where $\ell \in [n, 2n]$ is small compared with the total length of the round keys), and the same permutation, or very similar ones, are used at each round. It is therefore fundamental to determine whether security can actually benefit from the iterative structure and increase beyond the birthday bound, even though one does not use more key material nor more permutations than in the single-key one-round Even-Mansour cipher.

Our Results. We answer positively to the question above. Our main theorem states sufficient conditions on the way to derive three n-bit round keys (k_0, k_1, k_2) from one n-bit master key k so that the two-round Even-Mansour cipher defined from a single permutation

$$x \mapsto k_2 \oplus P(k_1 \oplus P(k_0 \oplus x))$$

is secure up to $\widetilde{\mathcal{O}}(2^{2n/3})$ queries of the adversary, where the $\widetilde{\mathcal{O}}(\cdot)$ notation hides logarithmic (in $N = 2^n$) factors. In particular, such a good key-schedule $k \mapsto (k_0, k_1, k_2)$ can be constructed from any (fixed) linear orthomorphism of $\mathbb{F}_2^n$. A permutation π of $\{0,1\}^n$ is called an orthomorphism if $x \mapsto x \oplus \pi(x)$ is also a permutation. The good cryptographic properties of orthomorphisms have already been noticed in a number of papers [Mit95, GGM99], and are in particular used in Lai-Massey schemes [LM90, Vau99] such as the block ciphers IDEA [LM90] and FOX [JV04]. Our main theorem is as follows.

Theorem (Informal). *Let π be any (fixed) linear orthomorphism of $\mathbb{F}_2^n$, and let P be a public random n-bit permutation oracle. Then the block cipher with message space and key space $\{0,1\}^n$ defined as (see Figure 1, top)*

$$\mathsf{EM}_k^P(x) = k \oplus P(\pi(k) \oplus P(k \oplus x)) \qquad (\star)$$

is secure against any adversary making up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries to EM_k^P and P. (Queries can be adaptive and are allowed in both directions for EM_k^P and P).

We remark that if one omits π in construction $(\star)$, i.e., if one adds the same round key k each time, security drops back to $\mathcal{O}(2^{n/2})$ queries. More generally, if round keys are all equal

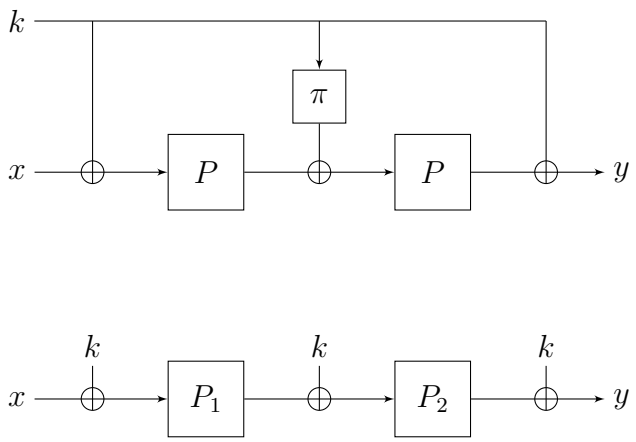

Fig. 1. Two constructions of "minimal" two-round Even-Mansour ciphers provably secure up to $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries of any (adaptive) adversary. Top: π is a (fixed) linear orthomorphism of $\mathbb{F}_2^n$, and P is a public random permutation oracle. Bottom: P_1 and P_2 are two independent public random permutation oracles.

and the same permutation P is used at each round of the iterated Even-Mansour cipher, security caps at $\mathcal{O}(2^{n/2})$ queries of the adversary, independently of the number r of rounds. This seems to be known as a folklore result about slide attacks [BW99, BW00], but since we could not find a detailed exposition in the literature, we precisely describe and analyze this attack (as well as a simple extension for two rounds when the key-schedule simply consists in xoring constants to the master key) in this paper. Hence, construction ($\star$) can be regarded as a "minimal" two-round Even-Mansour cipher delivering security beyond the birthday bound, since removing any component causes security to drop back to $\mathcal{O}(2^{n/2})$ queries at best (for π this follows from the slide attack just mentioned, while removing any instance of permutation P brings us back to a one-round Even-Mansour cipher). Additionally, we show that when using two independent public random permutations P_1 and P_2, the trivial key-schedule is sufficient: adding the same round key k at each round (see Figure 1, bottom) also yields a $\widetilde{\mathcal{O}}(2^{2n/3})$-security bound.

To the best of our knowledge, these are the first results proving "beyond the birthday bound" security for key-alternating ciphers such as AES that do not rely on the assumption that round keys are independent. This sheds some light on which exact properties are required from the key-schedule in order to lift the round keys independence assumption in provable security results. In particular, this seems to point out that a *pseudorandom* key-schedule is not needed (we remind the reader that our results come with the usual caveat that they are only proved in the very strong Random Permutation Model, and hence can only be taken as a heuristic security insurance once the inner permutation(s) are instantiated).

Overview of Our Techniques. In order to prove our results, we use the indistinguishability framework, namely we consider a distinguisher which must tell apart two worlds: the "real" world where it interacts with (EM_k^P, P), where EM_k^P is the Even-Mansour cipher instantiated with permutation P and a random key k, and the "ideal" world where it interacts with (E, P) where E is a random permutation independent from P. The distinguisher can make at most q_e queries to EM_k^P/E and at most q_p queries to P (all queries are adaptive and

can be forward or backward, and we work in the information-theoretic setting, i.e., the adversary is computationally unbounded). In order to upper bound the distinguishing advantage of this attacker, we use, as already done in [CS14], the H-coefficient method of Patarin [Pat08]. In a nutshell, this technique consists in partitioning the set of all possible transcripts of the interaction between the distinguisher and the tuple of permutations into a set $\mathcal{T}_1$ of "good" transcripts and a set $\mathcal{T}_2$ of "bad" transcripts. Good transcripts $\tau \in \mathcal{T}_1$ have the property that the ratio of the probabilities to obtain τ in the real and in the ideal world is greater that $1 - \varepsilon_1$ for some small $\varepsilon_1 > 0$, while the probability to obtain any bad transcript $\tau \in \mathcal{T}_2$ (in the ideal world) is less than some small $\varepsilon_2 > 0$. Then the advantage of the distinguisher can be upper bounded by $\varepsilon_1 + \varepsilon_2$.

In order to get intuition about what hides behind good and bad transcripts, it helps to first look at an example of how an adversary might "get lucky" during an attack. Specifically, we focus on the following attack scenario (we assume that $q_e = q_p = q$ for simplicity). The distinguisher (adversary) $\mathcal{D}$ starts by making q arbitrary queries to EM_k^P/E, resulting in a set of q pairs $\mathcal{Q}_E = \{(x_1, y_1), \ldots, (x_q, y_q)\}$; then $\mathcal{D}$ determines the pair of sets (U, V) with $|U| = |V| = q$ and $U, V \subseteq \{0,1\}^n$, that maximizes the size of the set

$$\mathcal{K}(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} \{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ s.t. } x_i \oplus k' \in U, y_i \oplus k' \in V\} \subseteq \{0,1\}^n, \quad (1)$$

and $\mathcal{D}$ queries $P(u)$, $P^{-1}(v)$ for all $u \in U$, $v \in V$. (This makes $2q$ queries to P instead of q, but this small constant factor is unimportant for the sake of intuition.) Note that if $\mathcal{D}$ is in the real world and if the real key k is in the set $\mathcal{K}(\mathcal{Q}_E, U, V)$ defined in (1), then $\mathcal{D}$ can see that one of its EM_k^P/E-queries is compatible with two of its P-queries with respect to k (in more detail, there exists a value i and queries (u, v), (u', v') to P such that $x_i \oplus k = u$, $v \oplus \pi(k) = u'$, and $v' \oplus k = y_i$). Elementary probabilistic considerations show that such a "complete cycle" will occur for at most a handful of keys in $\mathcal{K}(\mathcal{Q}_E, U, V)$, so that "false alerts" can be quickly weeded out and the correct key k validated in a few extra queries, all assuming $k \in \mathcal{K}(\mathcal{Q}_E, U, V)$. Moreover, heuristic considerations indicate that k will be in $\mathcal{K}(\mathcal{Q}_E, U, V)$ with probability $|\mathcal{K}(\mathcal{Q}_E, U, V)|/2^n$. In particular, thus, it becomes necessary to show that $|\mathcal{K}(\mathcal{Q}_E, U, V)|$ is significantly smaller than 2^n with high probability over $\mathcal{Q}_E$, i.e., that

$$\max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ s.t. } x_i \oplus k' \in U, y_i \oplus k' \in V\}| \quad (2)$$

is significantly smaller than 2^n with high probability over $\mathcal{Q}_E$, in order to show that $\mathcal{D}$ has small advantage at q queries. One of the criteria that can make a transcript "bad" in our proof happens to be, precisely, if the set of queries $\mathcal{Q}_E$ to EM_k^P/E contained within the transcript is such that (2) is larger than desirable. (Jumping ahead, $\mathcal{K}(\mathcal{Q}_E, U, V)$ will be re-baptized BadK_1 in Definitions 1 and 2 of a bad transcript).

To elaborate a little more on this, note that

$$\begin{aligned} |\mathcal{K}(\mathcal{Q}_E, U, V)| &\leq |\{(k', u, v) \in \{0,1\}^n \times U \times V : k' \oplus u = x_i, k' \oplus v = y_i \text{ for some } 1 \leq i \leq q\}| \\ &= |\{(i, u, v) \in \{1, \ldots, q\} \times U \times V : x_i \oplus y_i = u \oplus v\}|. \end{aligned}$$

Also note that the set of values $\{x_i \oplus y_i : (x_i, y_i) \in \mathcal{Q}_E\}$ is essentially a random set since if the i-th query to EM_k^P/E is forward then y_i comes at random from a large set, whereas otherwise

x_i comes at random from a large set. Moreover, as a matter of fact, the problem of upper bounding

$$\mu(A) \stackrel{\text{def}}{=} \max_{\substack{U,V \subseteq \{0,1\}^n \\ |U|=|V|=q}} |\{(a,u,v) \in A \times U \times V : a = u \oplus v\}$$

for a *truly random* set $A \subseteq \{0,1\}^n$ of size q has already been studied before [Bab89, Hay05, AKKR08, KPS13, Ste13], being dubbed[2] the *sum-capture problem* in [Ste13]. One of the main known results [Bab89, Ste13] on the sum-capture problem is that $\mu(A)$ is upper bounded by roughly $q^{3/2}$ for $q \leq 2^{2n/3}$. Surprisingly enough, this bound is exactly sufficient for our application, since $q^{3/2} \ll 2^n$ for $q \ll 2^{2n/3}$. (Implying, thus, that (2) is far from 2^n as long as q remains beneath $2^{2n/3}$, as desired.) Our own setting is, of course, slightly different, since the set $\{x_i \oplus y_i : (x_i, y_i) \in \mathcal{Q}_E\}$ isn't, unlike A, a purely random set of size q. Other complications also arise: in the general case where the three round keys (k_0, k_1, k_2) are derived from the n-bit master key k using non-trivial (bijective) key derivation functions $\gamma_i : k \mapsto k_i$, $\mathcal{K}(\mathcal{Q}_E, U, V)$ takes the more complicated form

$$\{k' \in \{0,1\}^n : \exists (x_i, y_i) \in \mathcal{Q}_E \text{ s.t. } x_i \oplus \gamma_0(k') \in U, y_i \oplus \gamma_2(k') \in V\},$$

so that we have to upper bound

$$|\{(i,u,v) \in \{1,\ldots,q\} \times U \times V : x_i \oplus u = \gamma_0 \circ \gamma_2^{-1}(y_i \oplus v)\}|.$$

All this means that we have to carefully adapt (and to some degree significantly extend) the Fourier-analytic techniques used in [Bab89, Ste13].

Once the probability to obtain a bad transcript has been upper bounded, the second part of the proof is to show that the ratio between the probabilities to obtain any good transcript in the real and the ideal world is close to 1. This part is in essence a permutation counting argument. When the two permutations are independent (Figure 1, bottom), the counting argument is not overly complicated. While we could, in principle, re-use the general results of [CS14], we expose it in Section 5 (see Lemma 9) since it constitutes a good warm-up for the reader before the more complicated counting in the subsequent section. For the single-permutation case, things become much more involved: first, we need to consider more conditions defining bad transcripts; and second, the permutation counting itself becomes much more intricate. Interestingly, this part is related to the following simple to state (yet to the best of our knowledge unexplored) problem: how many queries are needed to distinguish a random squared permutation $P \circ P$ (where P is uniformly random) from a uniformly random permutation E?

Related Work. Two recent papers analyzed a stronger security property of the iterated Even-Mansour cipher than mere pseudorandomness, namely indifferentiability from an ideal cipher [ABD+13, LS13]. Aside with provable security results already mentioned, a number of papers explored attacks on the (iterated) Even-Mansour cipher for one round [Dae91, BW00, DKS12], two rounds [NWW13], three rounds [DDKS13], and four rounds [BCD+13].

A distinct yet related line of work considers the security of the so-called "Xor-Cascade" construction [Gaz13, Lee13], a key-length extension method which generalizes the DESX construction [KR01] in the same way the Generalized Even-Mansour construction generalizes

[2] The terminology is attributed to Mario Szegedy.

the original (one-round) Even-Mansour cipher. Given a block cipher E with message space $\{0,1\}^n$ and key space $\{0,1\}^\kappa$, the r-round Xor-Cascade construction XC^E defines a new block cipher with message space $\{0,1\}^n$ and key space $\{0,1\}^{\kappa+(r+1)n}$ as follows: given a plaintext $x \in \{0,1\}^n$ and a key $(z, k_0, \ldots, k_r) \in \{0,1\}^{\kappa+(r+1)n}$, the ciphertext y is computed as

$$y = k_r \oplus E_{z_r}(k_{r-1} \oplus E_{z_{r-1}}(\cdots E_{z_2}(k_1 \oplus E_{z_1}(k_0 \oplus x))\cdots)),$$

where $(z_1, \ldots, z_r)$ is a sequence of sub-keys deterministically derived from z in a way such that for any z, the z_i's are pairwise distinct (note that this imposes $r \leq 2^\kappa$). Some authors considered minor variants of this construction where the last whitening key k_r is omitted [Gaz13] or where the sub-keys $(z_1, \ldots, z_r)$ are drawn uniformly at random [Lee13]. Directly relevant to our work, Gazi and Tessaro [GT12] considered a construction they named 2XOR, which is the two-round variant of Xor-Cascade where the whitening keys are identical (and the last whitening key is omitted), namely

$$\mathsf{2XOR}^E_{z,k}(x) = E_{z_2}(k \oplus E_{z_1}(k \oplus x)),$$

where (z_1, z_2) are pairwise distinct sub-keys derived from z. They showed that, when the underlying block cipher E is modeled as an ideal cipher, this construction is secure up to $\mathcal{O}(2^{\kappa+n/2})$ queries to E, even when the adversary can make all possible 2^n queries to the permutation oracle (which, in the indistinguishability experiment, is either $\mathsf{2XOR}^E_{z,k}$ or an independent random permutation). Considering a block cipher E with key-length $\kappa = 1$, one obtains a construction which is similar to the two-round Even-Mansour cipher of Figure 1, bottom, where the last key addition would be omitted.[3] Hence, the Gazi-Tessaro result says that this construction is secure for $q_e = 2^n$ and $q_p = \mathcal{O}(2^{n/2})$.[4] Our own results are incomparable with the one of [GT12]. First, the third key addition is omitted in the 2XOR construction. Second, our bounds are more general: they hold for any value of q_e and q_p as long as $q_e < 2^{2n/3}$ and $q_p < 2^{2n/3}$. Though our bounds become meaningless for $q_e = 2^n$, they show that when $q_e < 2^{2n/3}$ (an interesting case in practice since an attacker will not always have access to the entire codebook), security is ensured up to $\mathcal{O}(2^{2n/3})$ queries to the internal permutations (something that cannot be derived from the result of [GT12]).

Open Questions. Currently, our results only apply when the key derivation functions mapping the master key to the round keys are *linear* bijective functions of $\mathbb{F}_2^n$. This is due to the fact that the proof of our sum-capture theorem in Section 3 requires linear mappings. It is an open question whether this theorem can be extended to nonlinear (bijective) mappings as well. A second tantalizing yet challenging open problem is of course to generalize our results to larger numbers of rounds. Namely, for $r > 2$, can we find sufficient conditions on the key-schedule such that the r-round single-permutation Even-Mansour cipher ensures security up

[3] There is a slight subtlety here: in the 2XOR construction used with a block cipher with key-length $\kappa = 1$, i.e., a pair of permutations (P_1, P_2), there is an additional key bit z (hidden to the distinguisher) which tells in which order the two permutations are called.

[4] This is in fact very closely related to the security result for the single-key one-round Even-Mansour cipher up to $\mathcal{O}(2^{n/2})$ queries to the inner and outer permutations [DKS12]. In the Gazi-Tessaro case with $\kappa = 1$, the adversary is given an arbitrary permutation E, and must distinguish, given access to (P_1, P_2), whether P_1 and P_2 are independent, or whether $P_2(k \oplus P_1(k \oplus x)) = E(x)$ for some random key k. In the single-key one-round Even-Mansour case, the adversary must distinguish, given access to (P_1, P_2), whether P_1 and P_2 are independent, or whether $k \oplus P_1(k \oplus x) = P_2(x)$, i.e., $P_2^{-1}(k \oplus P_1(k \oplus x)) = x$. These are very similar problems, the latter being (up to changing P_2 into P_2^{-1}) a special case of the former with E the identity.

to $\widetilde{\mathcal{O}}(2^{\frac{rn}{r+1}})$ queries of the adversary? We stress that even the simpler case where permutations are independent and round keys are identical seems hard to tackle for $r > 2$: we currently have no idea of how to extend our sum-capture result in order to upper bound the probability of bad transcripts even in the case $r = 3$.

It would also be interesting to reduce the *time* complexity of attacks against the two-round Even-Mansour cipher (potentially down to $\mathcal{O}(2^{2n/3})$). Currently, the best known attack (for the case of independent permutations and identical round keys) has time complexity $\mathcal{O}(2^{n-\log_2 n})$ [DKS12]. Since our focus in this paper is on query complexity, we have not investigated whether this attack applies to the single-permutation variant ($\star$) as well.

Organization. We start in Section 2 by setting the notation, giving the necessary background on the H-coefficient technique, and proving some helpful lemmas. In Section 3, which is self-contained, we prove our new sum-capture result, which might be of independent interest. In Section 4, we detail slide attacks against the iterated Even-Mansour cipher. Sections 5 and 6 contain our two provable security results for the two "minimized" variants of the two-round Even-Mansour cipher of Figure 1. In Section 5, we first deal with the case where the two permutations are independent and the three round keys are identical. The permutation counting argument in this section (Lemma 9) serves as a good exercise before the corresponding one of the subsequent section (Lemma 10). Section 6, which contains our main theorem, deals with the case of a single permutation.

2 Preliminaries

2.1 Notation

Permutations. In all the following, we fix an integer $n \geq 1$, and we write $N = 2^n$. The set of all permutations on $\{0,1\}^n$ will be denoted $\mathcal{P}_n$. For integers $1 \leq s \leq t$, we will write $(t)_s = t(t-1)\cdots(t-s+1)$ and $(t)_0 = 1$ by convention. Given $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q))$, where the x_i's are pairwise distinct n-bit strings and the y_i's are pairwise distinct n-bit strings, and a permutation $P \in \mathcal{P}_n$, we say that P extends $\mathcal{Q}$, denoted $P \vdash \mathcal{Q}$, if $P(x_i) = y_i$ for $i = 1, \ldots, q$. Let $X = \{x \in \{0,1\}^n : (x, y) \in \mathcal{Q}\}$ and $Y = \{y \in \{0,1\}^n : (x, y) \in \mathcal{Q}\}$. We call X and Y respectively the *domain* and the *range* of $\mathcal{Q}$. By an abuse of notation, we will sometimes denote $\mathcal{Q}$ the bijection from X to Y such that $\mathcal{Q}(x_i) = y_i$ for $i = 1, \ldots, q$. Thus, for any $X' \subseteq X$ we have $\mathcal{Q}(X') = \{y \in \{0,1\}^n : (x, y) \in \mathcal{Q} \wedge x \in X'\}$, and for any $Y' \subseteq Y$ we have $\mathcal{Q}^{-1}(Y') = \{x \in \{0,1\}^n : (x, y) \in \mathcal{Q} \wedge y \in Y'\}$. We will often use the following simple fact: given $\mathcal{Q}$ of size q and $\mathcal{Q}'$ of size q' whose respective domains X and X' and respective ranges Y and Y' satisfy $X \cap X' = \emptyset$ and $Y \cap Y' = \emptyset$, one has

$$\Pr\left[P \leftarrow_{\$} \mathcal{P}_n : P \vdash \mathcal{Q}' \,\middle|\, P \vdash \mathcal{Q}\right] = \frac{1}{(N-q)_{q'}}.$$

When two sets A and B are disjoint, we denote $A \sqcup B$ their (disjoint) union.

Vector Space $\mathbb{F}_2^n$. We denote $\mathbb{F}_2 \simeq \{0,1\}$ the field with two elements, and $\mathbb{F}_2^n$ the vector space of dimension n over $\mathbb{F}_2$. Given two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, we denote $x \cdot y = \sum_{i=1}^n x_i y_i \bmod 2$ the inner product of x and y. The general linear group of degree n over $\mathbb{F}_2$, i.e., the set of all automorphisms (linear bijective mappings) of $\mathbb{F}_2^n$, will be denoted $\mathsf{GL}(n)$. Given $\Gamma \in \mathsf{GL}(n)$, we denote Γ^* the adjoint of Γ, i.e., the unique automorphism satisfying $x \cdot \Gamma(y) = \Gamma^*(x) \cdot y$ for all $x, y \in \mathbb{F}_2^n$.

2.2 The Generalized Even-Mansour Cipher

Fix integers $n, r, m, \ell \geq 1$. Let $\phi : \{1, \ldots, r\} \to \{1, \ldots, m\}$ be an arbitrary function, and $\boldsymbol{\gamma} = (\gamma_0, \ldots, \gamma_r)$ be a $(r+1)$-tuple of functions from $\{0,1\}^\ell$ to $\{0,1\}^n$. The r-round Generalized Even-Mansour construction $\mathsf{EM}[n, r, m, \ell, \phi, \boldsymbol{\gamma}]$ specifies, from any m-tuple $\boldsymbol{P} = (P_1, \ldots, P_m)$ of permutations on $\{0,1\}^n$, a block cipher with message space $\{0,1\}^n$ and key space $\{0,1\}^\ell$, simply denoted $\mathsf{EM}^{\boldsymbol{P}}$ in the following (parameters $[n, r, m, \ell, \phi, \boldsymbol{\gamma}]$ are implicit and will always be clear from the context), which maps a plaintext $x \in \{0,1\}^n$ and a key $K \in \{0,1\}^\ell$ to the ciphertext defined by (see Figure 2):

$$\mathsf{EM}^{\boldsymbol{P}}(K, x) = \gamma_r(K) \oplus P_{\phi(r)}(\gamma_{r-1}(K) \oplus P_{\phi(r-1)}(\cdots P_{\phi(2)}(\gamma_1(K) \oplus P_{\phi(1)}(\gamma_0(K) \oplus x)) \cdots)).$$

We denote $\mathsf{EM}^{\boldsymbol{P}}_K : x \mapsto \mathsf{EM}^{\boldsymbol{P}}(K, x)$ the Even-Mansour cipher instantiated with key K (hence, syntactically, $\mathsf{EM}^{\boldsymbol{P}}_K$ is a permutation on $\{0,1\}^n$).

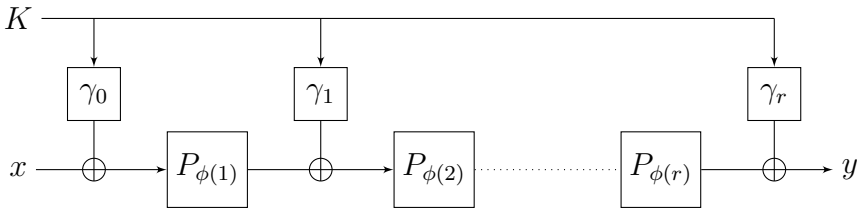

Fig. 2. The r-round Generalized Even-Mansour cipher.

For example, AES-128 is a Generalized Even-Mansour cipher where $n = 128$, $r = 10$, $m = 2$, $\ell = 128$, the function ϕ is defined by $\phi(i) = 1$ for $i = 1, \ldots, 9$ and $\phi(10) = 2$, each key derivation function γ_i is a 128-bit (non-linear for $i \geq 1$) permutation, and the two permutations P_1 and P_2 are defined as:

$$P_1 = \mathsf{MixColumns} \circ \mathsf{ShiftRows} \circ \mathsf{SubBytes}$$
$$P_2 = \mathsf{ShiftRows} \circ \mathsf{SubBytes}.$$

All previous work about the indistinguishability of the Even-Mansour cipher [BKL+12, LPS12, Ste12, CS14] considered the case where all permutations and all round keys are independent, namely $m = r$, ϕ is the identity function, $\ell = (r+1)n$, and γ_i simply selects the i-th n-bit string of $K = (k_0, \ldots, k_r)$.

In the following, we will focus in particular on two special cases:

– the case where permutations are independent and the same n-bit key k is used at each round, namely $m = r$, ϕ is the identity function, $\ell = n$, and all γ_i's are the identity function, in which case we will simply denote $\mathsf{EMIP}[n, r]$ the resulting construction. Hence, for an r-tuple of permutations $\boldsymbol{P} = (P_1, \ldots, P_r)$, the block cipher $\mathsf{EMIP}^{\boldsymbol{P}}$ maps a plaintext $x \in \{0,1\}^n$ and a key $k \in \{0,1\}^n$ to the ciphertext defined by:

$$\mathsf{EMIP}^{\boldsymbol{P}}(k, x) = k \oplus P_r(k \oplus P_{r-1}(\cdots P_2(k \oplus P_1(k \oplus x)) \cdots)).$$

– the case where a single permutation P is used at each round, namely $m = 1$ and $\phi(i) = 1$ for $i = 1, \ldots, r$, in which case we will simply denote $\mathsf{EMSP}[n, r, \ell, \boldsymbol{\gamma}]$ the resulting construction. Hence, for a permutation P, the block cipher EMSP^P maps a plaintext $x \in \{0,1\}^n$ and a key $K \in \{0,1\}^\ell$ to the ciphertext defined by:

$$\mathsf{EMSP}^P(K, x) = \gamma_r(K) \oplus P(\gamma_{r-1}(K) \oplus P(\cdots P(\gamma_1(K) \oplus P(\gamma_0(K) \oplus x)) \cdots)).$$

When additionally $\ell = n$ (namely the master key length is equal to the block length), we overload the notation and simply denote $\mathsf{EMSP}[n, r, \boldsymbol{\gamma}]$ the resulting construction.

2.3 Security Definition

To study the indistinguishability of the Generalized Even-Mansour cipher (in the Random Permutation Model), we consider a distinguisher $\mathcal{D}$ which interacts with a set of $m+1$ permutation oracles on n bits that we denote generically $(P_0, P_1 \ldots, P_m) = (P_0, \boldsymbol{P})$. The goal of $\mathcal{D}$ is to distinguish whether it is interacting with $(\mathsf{EM}_K^{\boldsymbol{P}}, \boldsymbol{P})$, where $\boldsymbol{P} = (P_1, \ldots, P_m)$ are random and independent permutations and K is randomly chosen from $\{0,1\}^\ell$ (we will informally refer to this case as the "real" world), or with $(E, \boldsymbol{P})$, where E is a random n-bit permutation independent from $\boldsymbol{P}$ (the "ideal" world). Note that in the latter case the distinguisher is simply interacting with $m+1$ independent random permutations. We sometimes refer to the first permutation P_0 as the *outer* permutation, and to permutations $P_1, \ldots, P_m$ as the *inner* permutations. The distinguisher is adaptive, and can make both forward and backward queries to each permutation oracle, which corresponds to the notion of adaptive chosen-plaintext and ciphertext security (CCA). We consider computationally unbounded distinguishers, and we assume *wlog* that the distinguisher is deterministic and never makes useless queries (which means that it never repeats a query, nor makes a query $P_i^{-1}(y)$ if it received y as the answer to a previous query $P_i(x)$, or vice-versa).

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

$$\mathbf{Adv}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{\mathsf{EM}_K^{\boldsymbol{P}}, \boldsymbol{P}} = 1\right] - \Pr\left[\mathcal{D}^{E, \boldsymbol{P}} = 1\right] \right|,$$

where the first probability is taken over the random choice of K and $\boldsymbol{P}$, and the second probability is taken over the random choice of E and $\boldsymbol{P}$. We recall that, even though this is not apparent from the notation, the distinguisher can make both forward and backward queries to each permutation oracle.

For q_e, q_p non-negative integers, we define the insecurity of the ideal[5] Generalized Even-Mansour cipher with parameters $(n, r, m, \ell, \phi, \boldsymbol{\gamma})$ as:

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EM}[n,r,m,\ell,\phi,\boldsymbol{\gamma}]}(q_e, q_p) = \max_{\mathcal{D}} \mathbf{Adv}(\mathcal{D}),$$

where the maximum is taken over all distinguishers $\mathcal{D}$ making exactly q_e queries to the outer permutation and exactly q_p queries to each inner permutation. The notation is adapted naturally for the two special cases EMIP and EMSP defined in Section 2.2.

2.4 The H-Coefficient Technique

We give here all the necessary background on the H-coefficient technique [Pat08, CS14] that we will use throughout this paper.

[5] By ideal, we mean that this insecurity measure is defined in the Random Permutation Model for $P_1, \ldots, P_m$.

TRANSCRIPT. All the information gathered by the distinguisher when interacting with the system of $m+1$ permutations can be summarized in what we call the *transcript* of the interaction, which is the ordered list of queries and answers received from the system (i, b, z, z'), where $i \in \{0, \ldots, m\}$ names the permutation being queried, b is a bit indicating whether this is a forward or backward query, $z \in \{0,1\}^n$ is the actual value queried and z' the answer. We say that a transcript is *attainable* (with respect to some fixed distinguisher $\mathcal{D}$) if there exists a tuple of permutations $(P_0, \ldots, P_m) \in (\mathcal{P}_n)^{m+1}$ such that the interaction of $\mathcal{D}$ with $(P_0, \ldots, P_m)$ yields this transcript (said otherwise, the probability to obtain this transcript in the "ideal" world is non-zero). In fact, an attainable transcript can be represented in a more convenient way that we will use in all the following. Namely, from the transcript we can build $m+1$ lists of directionless queries

$$\begin{aligned}
\mathcal{Q}_E &= ((x_1, y_1), \ldots, (x_{q_e}, y_{q_e})),\\
\mathcal{Q}_{P_1} &= ((u_{1,1}, v_{1,1}), \ldots, (u_{1,q_p}, v_{1,q_p})),\\
&\vdots\\
\mathcal{Q}_{P_m} &= ((u_{m,1}, v_{m,1}), \ldots, (u_{m,q_p}, v_{m,q_p}))
\end{aligned}$$

as follows. For $j = 1, \ldots, q_e$, let $(0, b, z, z')$ be the j-th query to P_0 in the transcript: if this was a forward query then we set $x_j = z$ and $y_j = z'$, otherwise we set $x_j = z'$ and $y_j = z$. Similarly, for each $i = 1, \ldots, m$, and $j = 1, \ldots, q_p$, let (i, b, z, z') be the j-th query to P_i in the transcript: if this was a forward query then we set $u_{i,j} = z$ and $v_{i,j} = z'$, otherwise we set $u_{i,j} = z'$ and $v_{i,j} = z$. A moment of thinking should make it clear that for attainable transcripts there is a one-to-one mapping between these two representations. (Essentially this follows from the fact that the distinguisher is deterministic). Moreover, though we defined $\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}$ as ordered lists, the order is unimportant (our formalization keeps the natural order induced by the distinguisher).

For convenience, and following [CS14], we will be generous with the distinguisher by providing it, at the end of its interaction, with the actual key K when it is interacting with $(\mathsf{EM}_K^{\boldsymbol{P}}, \boldsymbol{P})$, or with a dummy key K selected uniformly at random when it is interacting with $(E, \boldsymbol{P})$. This is without loss of generality since the distinguisher is free to ignore this additional information. Hence, all in all a transcript τ is a tuple $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}, K)$. We refer to $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m})$ (without the key) as the *permutation transcript*, and we say that a transcript τ is attainable if the corresponding permutation transcript is attainable. We denote $\mathcal{T}$ the set of attainable transcripts. (Thus $\mathcal{T}$ depends on $\mathcal{D}$, as the notion of attainability depends on $\mathcal{D}$.) 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.

MAIN LEMMA. In order to upper bound the advantage of the distinguisher, we will repeatedly use the following strategy: we will partition the set of attainable transcripts $\mathcal{T}$ into a set of "good" transcripts $\mathcal{T}_1$ such that the probabilities to obtain some transcript $\tau \in \mathcal{T}_1$ are close in the real and in the ideal world, and a set $\mathcal{T}_2$ of "bad" transcripts such that the probability to obtain any $\tau \in \mathcal{T}_2$ is small in the ideal world. More precisely, we will use the following result.

Lemma 1. *Fix a distinguisher $\mathcal{D}$. Let $\mathcal{T} = \mathcal{T}_1 \sqcup \mathcal{T}_2$ be a partition of the set of attainable transcripts. Assume that there exists ε_1 such that for any $\tau \in \mathcal{T}_1$, one has*[6]

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

and that there exists ε_2 such that

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \varepsilon_2.$$

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

Proof. The proof is standard, but we sketch it here for completeness. Since the distinguisher's output is a (deterministic) function of the transcript, its distinguishing advantage is upper bounded by the statistical distance between T_{id} and T_{re}, namely

$$\mathbf{Adv}(\mathcal{D}) \leq \|T_{\mathrm{re}} - T_{\mathrm{id}}\| \stackrel{\mathrm{def}}{=} \frac{1}{2} \sum_{\tau \in \mathcal{T}} \left| \Pr[T_{\mathrm{re}} = \tau] - \Pr[T_{\mathrm{id}} = \tau] \right|.$$

Moreover we have:

$$\begin{aligned}
\|T_{\mathrm{re}} - T_{\mathrm{id}}\| &= \sum_{\substack{\tau \in \mathcal{T} \\ \Pr[T_{\mathrm{id}}=\tau] > \Pr[T_{\mathrm{re}}=\tau]}} \left(\Pr[T_{\mathrm{id}} = \tau] - \Pr[T_{\mathrm{re}} = \tau]\right) \\
&= \sum_{\substack{\tau \in \mathcal{T} \\ \Pr[T_{\mathrm{id}}=\tau] > \Pr[T_{\mathrm{re}}=\tau]}} \Pr[T_{\mathrm{id}} = \tau] \left(1 - \frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]}\right) \\
&\leq \sum_{\tau \in \mathcal{T}_1} \Pr[T_{\mathrm{id}} = \tau] \varepsilon_1 + \sum_{\tau \in \mathcal{T}_2} \Pr[T_{\mathrm{id}} = \tau] \\
&\leq \varepsilon_1 + \varepsilon_2.
\end{aligned}$$

□

The ratio $\Pr[T_{\mathrm{re}} = \tau] / \Pr[T_{\mathrm{id}} = \tau]$ takes a particularly simple form for the Even-Mansour cipher. (This is one of the reasons why we append the key K at the end of the transcript; otherwise, the ratio would take a more cumbersome form.)

Lemma 2. *Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m}, K) \in \mathcal{T}$ be an attainable transcript. Let*

$$\mathsf{p}(\tau) \stackrel{\mathrm{def}}{=} \Pr\left[P_1, \ldots, P_m \leftarrow_{\$} \mathcal{P}_n : \mathsf{EM}_K^{P_1,\ldots,P_m} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m})\right].$$

Then

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau).$$

Proof. One can easily check that the interaction of the distinguisher with any set of permutations $(P_0, P_1, \ldots, P_m)$ produces permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \ldots, \mathcal{Q}_{P_m})$ *iff*

$$(P_0 \vdash \mathcal{Q}_E) \wedge (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m}).$$

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

In the ideal world, the distinguisher interacts with $(E, P_1, \ldots, P_m)$ where E is independent from $P_1, \ldots P_m$, and the (dummy) key K is uniformly random and independent from the permutations. It follows easily that

$$\Pr[T_{\mathrm{id}} = \tau] = \frac{1}{2^\ell} \times \frac{1}{(N)_{q_e}} \times \left(\frac{1}{(N)_{q_p}}\right)^m.$$

In the real world, the distinguisher interacts with $(\mathsf{EM}_K^{P_1,\ldots,P_m}, P_1, \ldots, P_m)$, where the key K is uniformly random and independent from $(P_1, \ldots, P_m)$. It easily follows that

$$\begin{aligned}\Pr[T_{\mathrm{re}} = \tau] = \frac{1}{2^\ell} \times \left(\frac{1}{(N)_{q_p}}\right)^m \\ \times \Pr\left[P_1, \ldots, P_m \leftarrow_{\$} \mathcal{P}_n : \mathsf{EM}_K^{P_1,\ldots,P_m} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge \cdots \wedge (P_m \vdash \mathcal{Q}_{P_m})\right],\end{aligned}$$

hence the result. □

2.5 Useful Lemmas

We give two lemmas that will be useful throughout the paper.

Lemma 3. *Let N, a, b, c, d be positive integers such that $c + d = 2b$ and $2a + 2b \leq N$. Then*

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

Proof. Assume *wlog* that $c \geq d$. Note that this implies $c \geq b$. Then:

$$\begin{aligned}\frac{(N)_a (N-2b)_a}{(N-c)_a (N-d)_a} &= \frac{(N)_a (N-2b)_a}{((N-b)_a)^2} \times \frac{((N-b)_a)^2}{(N-c)_a (N-d)_a} \\ &= \prod_{i=N-a-b+1}^{N-b} \frac{(i+b)(i-b)}{i^2} \times \prod_{i=N-a-b+1}^{N-b} \frac{i^2}{(i-c+b)(i-d+b)} \\ &= \prod_{i=N-a-b+1}^{N-b} \left(1 - \frac{b^2}{i^2}\right) \times \underbrace{\prod_{i=N-a-b+1}^{N-b} \frac{i^2}{(i-(c-b))(i+(c-b))}}_{\geq 1} \\ &\geq \left(1 - \frac{b^2}{(N-a-b+1)^2}\right)^a \\ &\geq 1 - \frac{4ab^2}{N^2},\end{aligned}$$

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

Lemma 4. *Let N, q be positive integers and $M > 0$. Assume that $M \leq \frac{q}{2} \leq \frac{N}{6}$, and let*

$$C_{N,q,k} = \frac{(q)_{2k} (N-2q)_{q-2k} (N)_q}{k! (N)_{2q-k}}.$$

Then we have

$$\sum_{0 \leq k \leq M} C_{N,q,k} \geq 1 - \frac{2M^2}{q} - \frac{3q^2}{2MN}.$$

Proof. We take advantage of the fact that $C_{N,q,k}$ "looks like" (but is not exactly) the hypergeometric distribution. The hypergeometric distribution typically applies to sampling without replacement from a finite population whose elements can be classified into two mutually exclusive categories. The random variable, parameterized by N, p, and q, counts the number of elements selected from a certain subset of q "good" elements when p elements are selected from the universe of N elements without replacement. The probability that exactly k elements are selected from the subset of q "good" elements is

$$\mathsf{Hyp}_{N,p,q}(k) = \frac{\binom{q}{k}\binom{N-q}{p-k}}{\binom{N}{p}} = \frac{(p)_k(q)_k(N-q)_{p-k}}{k!(N)_p},$$

and the mean of this variable is pq/N.

For $k \le M$, we have

$$\begin{aligned}
C_{N,q,k} &= \frac{(q)_{2k}(N-2q)_{q-2k}(N)_q}{k!(N)_{2q-k}} \times \frac{k!(N-q)_q}{(q)_k(q)_k(N-2q)_{q-k}} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&= \frac{(q-k)_k}{(q)_k} \times \frac{(N-q)_q(N-2q)_{q-2k}}{(N-q)_{q-k}(N-2q)_{q-k}} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&= \prod_{i=0}^{k-1}\left(1-\frac{k}{q-i}\right) \times \underbrace{\frac{(N-2q+k)_k}{(N-3q+2k)_k}}_{\ge 1} \times \mathsf{Hyp}_{N-q,q,q}(k) \\
&\ge \left(1-\frac{k}{q-k+1}\right)^k \mathsf{Hyp}_{N-q,q,q}(k) \\
&\ge \left(1-\frac{k^2}{q-k+1}\right) \mathsf{Hyp}_{N-q,q,q}(k) \\
&\ge \left(1-\frac{2M^2}{q}\right) \mathsf{Hyp}_{N-q,q,q}(k),
\end{aligned}$$

where the last inequality follows from $k \le M \le q/2$. Therefore

$$\sum_{0\le k\le M} C_{N,q,k} \ge \left(1-\frac{2M^2}{q}\right) \sum_{0\le k\le M} \mathsf{Hyp}_{N-q,q,q}(k).$$

Since the mean of the hypergeometric distribution $\mathsf{Hyp}_{N-q,q,q}$ is $\frac{q^2}{N-q}$, we have

$$\sum_{k>M} \mathsf{Hyp}_{N-q,q,q}(k) \le \frac{q^2}{M(N-q)} \le \frac{3q^2}{2MN}$$

by Markov's inequality and using the assumption that $q \le N/3$. So it follows that

$$\begin{aligned}
\sum_{0\le k\le M} C_{N,q,k} &\ge \left(1-\frac{2M^2}{q}\right) \sum_{0\le k\le M} \mathsf{Hyp}_{N-q,q,q}(k) \\
&\ge \left(1-\frac{2M^2}{q}\right)\left(1-\frac{3q^2}{2MN}\right) \ge 1-\frac{2M^2}{q}-\frac{3q^2}{2MN}.
\end{aligned}$$

□

3 A Sum-Capture Theorem

In this section, we prove a variant of previous "sum-capture" results [Bab89, KPS13, Ste13]. Informally, such results typically state that when choosing a random subset A of $\mathbb{Z}_2^n$ (or more generally any abelian group) of size q, the value

$$\mu(A) = \max_{\substack{U,V \subseteq \mathbb{Z}_2^n \\ |U|=|V|=q}} |\{(a,u,v) \in A \times U \times V : a = u \oplus v\}|$$

is close to its expected value q^3/N (if A, U, V were chosen at random), except with negligible probability. Here, we prove a result of this type for the setting where A arises from the interaction of an adversary with a random permutation P, namely $A = \{x \oplus y : (x,y) \in \mathcal{Q}\}$, where $\mathcal{Q}$ is the transcript of the interaction between the adversary and P. In fact our result is even more general, the special case just mentioned corresponding to Γ being the identity in the theorem below.

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

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

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

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

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

Proof. The theorem follows directly from Lemmas 5 and 7 that are proven below. □

A Reminder on Fourier Analysis. We start by introducing some notation and recalling some classical results on Fourier analysis over the abelian group $\mathbb{Z}_2^n$. In the following, given a subset $S \subset \{0,1\}^n$, we denote $1_S : \{0,1\}^n \to \{0,1\}$ the characteristic functions of S, namely $1_S(x) = 1$ if $x \in S$ and $1_S(x) = 0$ if $x \notin S$. Given two functions $f, g : \{0,1\}^n \to \mathbb{R}$, we denote

$$\langle f,g \rangle = \mathbb{E}[fg] = \frac{1}{N}\sum_{x \in \{0,1\}^n} f(x)g(x)$$

the inner product of f and g, and, for all $x \in \{0,1\}^n$, we denote

$$(f * g)(x) = \sum_{y \in \{0,1\}^n} f(y)g(x \oplus y)$$

the convolution of f and g. Given $\alpha \in \{0,1\}^n$, we denote $\chi_\alpha : \{0,1\}^n \to \{\pm 1\}$ the *character* associated with α defined as

$$\chi_\alpha(x) = (-1)^{\alpha \cdot x}.$$

The all-one character χ_0 is called the *principal character*. All other characters $\chi \neq 1$ corresponding to $\alpha \neq 0$ are called *non-principal characters*. The set of all characters forms a group for the pointwise product operation $(\chi_\alpha \chi_\beta)(x) = \chi_\alpha(x)\chi_\beta(x)$ and one has $\chi_\alpha \chi_\beta = \chi_{\alpha \oplus \beta}$.

Given a function $f : \{0,1\}^n \to \mathbb{R}$ and $\alpha \in \{0,1\}^n$, the *Fourier coefficient* of f corresponding to α is

$$\widehat{f}(\alpha) \stackrel{\text{def}}{=} \langle f, \chi_\alpha \rangle = \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x)(-1)^{\alpha \cdot x}.$$

The coefficient corresponding to $\alpha = 0$ is called the *principal Fourier coefficient*, all the other ones are called *non-principal Fourier coefficients*. Note that for a set $S \subseteq \{0,1\}^n$ one has

$$\widehat{1_S}(0) = \frac{|S|}{N},$$

namely the principal Fourier coefficient of 1_S is equal to the relative size of the set. We will also use the following three classical results, holding for any functions $f, g, : \{0,1\}^n \to \mathbb{R}$, any $\alpha \in \{0,1\}^n$, and any $S \subseteq \{0,1\}^n$:

$$\sum_{x \in \{0,1\}^n} f(x)g(x) = N \sum_{\alpha \in \{0,1\}^n} \widehat{f}(\alpha)\widehat{g}(\alpha) \tag{3}$$

$$\widehat{(f * g)}(\alpha) = N \widehat{f}(\alpha)\widehat{g}(\alpha) \tag{4}$$

$$\sum_{\alpha \in \{0,1\}^n} |\widehat{1_S}(\alpha)|^2 = \frac{|S|}{N}. \tag{5}$$

First Step: the Cauchy-Schwarz Trick. As a preliminary step towards proving Theorem 1, we start by relating the quantity $\mu(\mathcal{Q}, U, V)$ with the maximal amplitude of (a subset of) non-principal Fourier coefficients of the characteristic function $\widehat{1_\mathcal{Q}}$ of the set $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q))$ seen as a subset of $\{0,1\}^{2n}$. This part is adapted from Babai [Bab89, Section 4] and Steinberger [Ste13], but in our setting we have to work over the product group $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ (in particular, Lemma 5 below is the analogue of Theorem 4.1 in [Bab89], which was independently rediscovered by Steinberger [Ste13]). In the following, we let, for any $\alpha \in \{0,1\}^n$, $\alpha \neq 0$,

$$\Phi_{\alpha,\Gamma}(\mathcal{Q}) \stackrel{\text{def}}{=} N^2 \left|\widehat{1_\mathcal{Q}}(\alpha, \Gamma^*(\alpha))\right| = \left| \sum_{(x,y) \in \mathcal{Q}} (-1)^{\alpha \cdot x \oplus \Gamma^*(\alpha) \cdot y} \right|$$

$$\Phi_\Gamma(\mathcal{Q}) \stackrel{\text{def}}{=} \max_{\alpha \neq 0} \Phi_{\alpha,\Gamma}(\mathcal{Q}).$$

Lemma 5. *For any subsets U and V of $\{0,1\}^n$, one has*

$$\mu(\mathcal{Q}, U, V) \leq \frac{q|U||V|}{N} + \Phi_\Gamma(\mathcal{Q})\sqrt{|U||V|}.$$

Proof. In the following, we denote

$$W = U \times V = \{(u, v) : u \in U, v \in V\}$$
$$K = \{(\Gamma(k), k) : k \in \{0,1\}^n\}.$$

Since $((x,y),u,v) \in \mathcal{Q} \times U \times V$ satisfies $x \oplus u = \Gamma(y \oplus v)$ *iff* there exists $k \in \{0,1\}^n$ such that

$$(x,y) \oplus (u,v) = (\Gamma(k), k),$$

it follows that we have

$$\begin{aligned}
\mu(\mathcal{Q},U,V) &= \sum_{\substack{(x,y)\in(\{0,1\}^n)^2 \\ (u,v)\in(\{0,1\}^n)^2}} 1_{\mathcal{Q}}(x,y)1_W(u,v)1_K(x\oplus u, y\oplus v) \\
&= \sum_{(x,y)\in(\{0,1\}^n)^2} 1_{\mathcal{Q}}(x,y) \sum_{(u,v)\in(\{0,1\}^n)^2} 1_W(u,v)1_K(x\oplus u, y\oplus v) \\
&= \sum_{(x,y)\in(\{0,1\}^n)^2} 1_{\mathcal{Q}}(x,y)(1_W * 1_K)(x,y) \\
&= N^2 \sum_{(\alpha,\beta)\in(\{0,1\}^n)^2} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{(1_W * 1_K)}(\alpha,\beta) \qquad \text{(by (3))} \\
&= N^4 \sum_{(\alpha,\beta)\in(\{0,1\}^n)^2} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta) \qquad \text{(by (4))}.
\end{aligned}$$

Separating the principal Fourier coefficient from non-principal ones in the last equality above, we get

$$\begin{aligned}
\mu(\mathcal{Q},U,V) &= N^4 \frac{|\mathcal{Q}|}{N^2}\frac{|W|}{N^2}\frac{|K|}{N^2} + N^4 \sum_{(\alpha,\beta)\neq(0,0)} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta) \\
&= \frac{q|U||V|}{N} + N^4 \sum_{(\alpha,\beta)\neq(0,0)} \widehat{1_{\mathcal{Q}}}(\alpha,\beta)\widehat{1_W}(\alpha,\beta)\widehat{1_K}(\alpha,\beta). \qquad (6)
\end{aligned}$$

(We note that equality (6) above holds in fact for any abelian group G and any fixed, non-necessarily linear, permutation $\Gamma : G \to G$, replacing the summation over $(\alpha,\beta) \neq (0,0)$ by the summation over all non-principal characters of the product group $G \times G$.) Moreover, we have

$$\begin{aligned}
\widehat{1_W}(\alpha,\beta) &= \frac{1}{N^2} \sum_{(u,v)\in(\{0,1\}^n)^2} 1_W(u,v)(-1)^{\alpha\cdot u \oplus \beta\cdot v} \\
&= \frac{1}{N^2} \sum_{(u,v)\in(\{0,1\}^n)^2} 1_U(u)1_V(v)(-1)^{\alpha\cdot u \oplus \beta\cdot v} \\
&= \frac{1}{N^2} \left(\sum_{u\in\{0,1\}^n} 1_U(u)(-1)^{\alpha\cdot u} \right) \left(\sum_{v\in\{0,1\}^n} 1_V(v)(-1)^{\beta\cdot v} \right) \\
&= \widehat{1_U}(\alpha)\widehat{1_V}(\beta),
\end{aligned}$$

and

$$\begin{aligned}
\widehat{1_K}(\alpha,\beta) &= \frac{1}{N^2} \sum_{(x,y)\in(\{0,1\}^n)^2} 1_K(x,y)(-1)^{\alpha\cdot x \oplus \beta\cdot y} \\
&= \frac{1}{N^2} \sum_{y\in\{0,1\}^n} (-1)^{\alpha\cdot \Gamma(y) \oplus \beta\cdot y}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{N^2} \sum_{y \in \{0,1\}^n} (-1)^{\Gamma^*(\alpha)\cdot y \oplus \beta \cdot y} \\
&= 0 \text{ if } \beta \neq \Gamma^*(\alpha) \\
&\quad \frac{1}{N} \text{ if } \beta = \Gamma^*(\alpha).
\end{aligned}
$$

Then, injecting the two observations above in (6), we obtain

$$
\begin{aligned}
\mu(\mathcal{Q}, U, V) &= \frac{q|U||V|}{N} + N^3 \sum_{\alpha \neq 0} \widehat{1_{\mathcal{Q}}}(\alpha, \Gamma^*(\alpha)) \widehat{1_U}(\alpha) \widehat{1_V}(\Gamma^*(\alpha)) \\
&\leq \frac{q|U||V|}{N} + N^3 \sum_{\alpha \neq 0} \left|\widehat{1_{\mathcal{Q}}}(\alpha, \Gamma^*(\alpha))\right| \cdot \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right| \\
&\leq \frac{q|U||V|}{N} + N \Phi_\Gamma(\mathcal{Q}) \sum_{\alpha \neq 0} \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right|,
\end{aligned}
$$

where the last inequality follows by noting that $|\widehat{1_{\mathcal{Q}}}(\alpha, \Gamma^*(\alpha))| \leq \Phi_\Gamma(\mathcal{Q})/N^2$ for any $\alpha \neq 0$ (by definition of $\Phi_\Gamma(\mathcal{Q})$). By Cauchy-Schwarz,

$$
\sum_{\alpha \neq 0} \left|\widehat{1_U}(\alpha)\right| \cdot \left|\widehat{1_V}(\Gamma^*(\alpha))\right| \leq \sqrt{\sum_{\alpha \in \{0,1\}^n} |\widehat{1_U}(\alpha)|^2} \sqrt{\sum_{\alpha \in \{0,1\}^n} |\widehat{1_V}(\Gamma^*(\alpha))|^2} = \frac{1}{N}\sqrt{|U||V|},
$$

where the last equality follows from (5), so that we finally obtain

$$
\mu(\mathcal{Q}, U, V) \leq \frac{q|U||V|}{N} + \Phi_\Gamma(\mathcal{Q}) \sqrt{|U||V|}. \qquad \square
$$

Upper Bounding Non-Principal Fourier Coefficients. Having established Lemma 5, it remains to find an upper bound on $\Phi_\Gamma(\mathcal{Q})$ holding with high probability over the random choice of P and the random coins of the adversary. For this, we will need the following extension of the Chernoff bound to "moderately dependent" random variables.

Lemma 6. *Let $0 \leq \varepsilon \leq 1/2$, and let $\boldsymbol{A} = (A_i)_{1 \leq i \leq q}$ be a sequence of random variables taking values in $\{\pm 1\}$. Assume that for any $1 \leq i \leq q$ and any sequence $(a_1, \ldots, a_{i-1}) \in \{\pm 1\}^{i-1}$, one has*

$$
\Pr\left[A_i = 1 \,|\, (A_1, \ldots, A_{i-1}) = (a_1, \ldots a_{i-1})\right] \leq \frac{1}{2} + \varepsilon.
$$

Then, for any $\delta \in [0, 1]$, one has

$$
\Pr\left[\sum_{i=1}^{q} A_i \geq q(2\varepsilon + \delta)\right] \leq e^{-\frac{q\delta^2}{12}}.
$$

Proof. Let $\boldsymbol{B} = (B_i)_{1 \leq i \leq q}$ be independent and identically distributed random variables such that

$$
\Pr[B_i = 1] = \frac{1}{2} + \varepsilon \quad \text{and} \quad \Pr[B_i = -1] = \frac{1}{2} - \varepsilon.
$$

We first show that for any r, we have

$$
\Pr\left[\sum_{i=1}^{q} A_i \geq r\right] \leq \Pr\left[\sum_{i=1}^{q} B_i \geq r\right]. \tag{7}
$$

We prove this with a coupling-like argument. Let Ber_p denote the ± 1 Bernoulli distribution of parameter p (which takes value 1 with probability p and -1 with probability $1-p$). Consider the following sampling process (we assume $\varepsilon < 1/2$ here, but this is *wlog* since the lemma trivially holds for $\varepsilon = 1/2$):

for $i = 1$ to q **do**
  $p \leftarrow \Pr[A_i = 1 \,|\, (A_1, \dots, A_{i-1}) = (u_1, \dots u_{i-1})]$
  $u_i \leftarrow \mathsf{Ber}_p$
  if $u_i = 1$ **then**
    $v_i \leftarrow 1$
  else
    $p' \leftarrow \frac{1/2+\varepsilon-p}{1-p}$
    $v_i \leftarrow \mathsf{Ber}_{p'}$
return $((u_1, \dots, u_q), (v_1, \dots, v_q))$

Then clearly $(u_1, \dots, u_q) \sim \boldsymbol{A}$. Moreover, $(v_1, \dots, v_q) \sim \boldsymbol{B}$. Indeed, for any $i = 1, \dots, q$, and any sequence $(v_1, \dots, v_{i-1}) \in \{\pm 1\}^{i-1}$, one has

$$\Pr[v_i = 1 | (v_1, \dots, v_{i-1})] = p + p'(1-p) = \frac{1}{2} + \varepsilon.$$

Note that during the sampling process, $u_i = 1$ implies $v_i = 1$, so that for any r,

$$\sum_{i=1}^{q} u_i \geq r \Longrightarrow \sum_{i=1}^{q} v_i \geq r,$$

which implies (7).

Fix now $\delta \in [0, 1]$, and let $(B'_i)_{1 \leq i \leq q}$ be defined as

$$B'_i = \frac{1 + B_i}{2},$$

so that

$$\Pr[B'_i = 1] = \frac{1}{2} + \varepsilon \quad \text{and} \quad \Pr[B'_i = 0] = \frac{1}{2} - \varepsilon.$$

Let $m = \mathbb{E}(\sum_{i=1}^{q} B'_i) = q(1/2 + \varepsilon)$. Then the Chernoff bound asserts that for any $0 \leq \delta' \leq 1$, one has

$$\Pr\left[\sum_{i=1}^{q} B'_i \geq (1 + \delta')m\right] \leq e^{\frac{-m\delta'^2}{3}}.$$

Substituting $\delta' = \frac{q\delta}{2m} = \frac{\delta}{1+2\varepsilon}$ in the inequality above yields (note that $\delta \in [0, 1] \Rightarrow \delta' \in [0, 1]$)

$$\Pr\left[\sum_{i=1}^{q} B_i \geq q(2\varepsilon + \delta)\right] = \Pr\left[\sum_{i=1}^{q} B'_i \geq \left(1 + \frac{q\delta}{2m}\right) m\right] \leq e^{-\frac{q^2\delta^2}{12m}} \leq e^{-\frac{q\delta^2}{12}}.$$

which combined with (7) concludes the proof. □

We are now ready to prove an adequate upper bound on $\Phi_\Gamma(\mathcal{Q})$.

Lemma 7. *Assume that $9n \le q \le N/2$. Fix $\Gamma \in \mathsf{GL}(n)$ and an adversary $\mathcal{A}$ making q queries to a random permutation P. Let $\mathcal{Q}$ denote the transcript of the interaction of $\mathcal{A}$ with P. Then*

$$\Pr_{P,\omega}\left[\Phi_\Gamma(\mathcal{Q}) \ge \frac{2q^2}{N} + 3\sqrt{nq}\right] \le \frac{2}{N},$$

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

Proof. In all this proof, $\Pr[\cdot]$ denotes $\Pr_{P,\omega}[\cdot]$. Fix $\alpha \in \{0,1\}^n$, $\alpha \neq 0$. Letting $\mathcal{Q} = ((x_1, y_1), \ldots, (x_q, y_q))$ following the natural ordering of the queries of $\mathcal{A}$, we define the sequence of random variables $(A_i)_{1\le i\le q}$ where $A_i = (-1)^{\alpha\cdot x_i \oplus \Gamma^*(\alpha)\cdot y_i}$. Then $\Phi_{\alpha,\Gamma}(\mathcal{Q}) = |\sum_{i=1}^q A_i|$. In order to apply Lemma 6, we will show that for $1 \le i \le q$, and any sequence $\boldsymbol{a} = (a_1, \ldots, a_{i-1}) \in \{\pm 1\}^{i-1}$, we have

$$p_i \stackrel{\text{def}}{=} \Pr\left[A_i = 1 \,|\, (A_1, \ldots, A_{i-1}) = (a_1, \ldots, a_{i-1})\right] \le \frac{1}{2} + \frac{q}{N}. \tag{8}$$

Let $\mathcal{Q}_i = ((x_1, y_1), \ldots, (x_i, y_i))$ denote the first i pairs of the transcript $\mathcal{Q}$. Let also $\Theta_{\boldsymbol{a}}$ denote the set of attainable partial transcript $\mathcal{Q}_{i-1}$ such that $(A_1, \ldots, A_{i-1}) = (a_1, \ldots, a_{i-1})$. Then, one has

$$\begin{aligned} p_i &= \frac{\Pr\left[A_i = 1 \wedge (A_1, \ldots, A_{i-1}) = (a_1, \ldots, a_{i-1})\right]}{\Pr[(A_1, \ldots, A_{i-1}) = (a_1, \ldots, a_{i-1})]} \\ &= \frac{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[A_i = 1 \wedge \mathcal{Q}_{i-1} = (x'_j, y'_j)_{1\le j\le i-1}\right]}{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr[\mathcal{Q}_{i-1} = (x'_j, y'_j)_{1\le j\le i-1}]} \\ &= \frac{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[A_i = 1 \middle| \mathcal{Q}_{i-1} = (x'_j, y'_j)_{1\le j\le i-1}\right] \Pr\left[\mathcal{Q}_{i-1} = (x'_j, y'_j)_{1\le j\le i-1}\right]}{\sum_{(x'_j,y'_j)_{1\le j\le i-1}\in\Theta_{\boldsymbol{a}}} \Pr\left[\mathcal{Q}_{i-1} = (x'_j, y'_j)_{1\le j\le i-1}\right]}. \end{aligned} \tag{9}$$

Fix now any partial transcript $((x'_1, y'_1), \ldots, (x'_{i-1}, y'_{i-1}))$. Assume that the i-th query of the adversary to P is a forward query x_i. Note that the answer y_i is distributed uniformly at random on a set of size $N - i + 1$. Also notice that, once x_i is fixed, there are exactly $N/2$ y_i's such that $(-1)^{\alpha\cdot x_i \oplus \Gamma^*(\alpha)\cdot y_i} = 1$ since $\Gamma^*(\alpha)$ is non-zero. Similarly, if the i-th query is a backward query y_i, then the answer x_i is is distributed uniformly at random on a set of size $N-i+1$, and once y_i is fixed, there are exactly $N/2$ x_i's such that $(-1)^{\alpha\cdot x_i \oplus \Gamma^*(\alpha)\cdot y_i} = 1$ since $\alpha \neq 0$. Hence, we have that

$$\begin{aligned} \Pr\left[A_i = 1 \middle| \mathcal{Q}_{i-1} = ((x'_1, y'_1), \ldots, (x'_{i-1}, y'_{i-1}))\right] &\le \frac{N/2}{N - i + 1} \\ &\le \frac{N}{2(N-q)} \le \frac{1}{2} + \frac{q}{2(N-q)} \le \frac{1}{2} + \frac{q}{N}, \end{aligned}$$

which implies that the same upper bound holds for p_i as well by (9), hence proving (8). We can now apply Lemma 6 with $\varepsilon = q/N$ and we obtain, for any $\delta \in [0, 1]$,

$$\Pr\left[\sum_{i=1}^q A_i \ge \frac{2q^2}{N} + q\delta\right] \le e^{-\frac{q\delta^2}{12}}.$$

Defining $A'_i = -A_i$, and applying exactly the same reasoning, we obtain

$$\Pr\left[\sum_{i=1}^{q} A_i \leq -\left(\frac{2q^2}{N} + q\delta\right)\right] \leq e^{-\frac{q\delta^2}{12}}.$$

Thus by a union bound we obtain:

$$\Pr\left[\Phi_{\alpha,\Gamma}(\mathcal{Q}) \geq \frac{2q^2}{N} + q\delta\right] \leq 2e^{-\frac{q\delta^2}{12}}.$$

Note that this holds for any $\alpha \neq 0$. Hence, if we choose $\delta = \sqrt{(12 \ln N)/q}$ (which, assuming $q \geq 9n$, implies $\delta \leq 1$), we finally obtain, using $\sqrt{12 \ln 2} \leq 3$,

$$\Pr_{P,\omega}\left[\Phi_{\Gamma}(\mathcal{Q}) \geq \frac{2q^2}{N} + 3\sqrt{nq}\right] \leq \frac{2}{N}. \qquad \square$$

4 Slide Attacks against the Even-Mansour Cipher

4.1 Slide Attack for Identical Round Keys and Identical Permutations

Consider the r-round Even-Mansour cipher with a single permutation P and identical round keys, which we simply denote EM_k^P here. We show that there is a slide attack against this cipher with query and time complexity $\mathcal{O}(2^{n/2})$, independently of the number r of rounds. This attack works as follows (we describe a distinguishing attack where the adversary $\mathcal{D}$ interacts with a pair of permutations (E, P), and must distinguish whether E is truly random, or whether this is EM_k^P for a random key k):

1. Fix a nonzero $c \in \{0,1\}^n$ and two subsets X, $U \subset \{0,1\}^n$ such that $|X| = |U| = 2^{\frac{n}{2}}$ and
$$X \oplus U = \{x \oplus u : x \in X, u \in U\} = \{0,1\}^n.$$
(For example, X consists of all strings whose last $n/2$ bits are zero, and U consists of all strings whose first $n/2$ bits are zero.)
2. $\mathcal{D}$ makes queries
   - $E(x)$ and $E(x \oplus c)$ for $x \in X$
   - $P(u)$ and $P(u \oplus c)$ for $u \in U$
3. Using the responses to the above queries, $\mathcal{D}$ further makes queries
   - $E(P(u))$ and $E(P(u \oplus c))$ for $u \in U$
   - $P(E(x))$ and $P(E(x \oplus c))$ for $x \in X$
4. If there are $x^* \in X$ and $u^* \in U$ such that
$$P(E(x^*)) \oplus E(P(u^*)) = P(E(x^* \oplus c)) \oplus E(P(u^* \oplus c)) = x^* \oplus u^* \tag{10}$$
then $\mathcal{D}$ outputs 1. Otherwise, $\mathcal{D}$ outputs 0.

The numbers of E-queries and P-queries required for this attack are both at most $2^{2+\frac{n}{2}}$ (there might be redundant queries). Moreover this attack can easily be turned into a key-recovery attack, the key guess of the adversary being $k = x^* \oplus u^*$ for (x^*, u^*) satisfying Equation (10).

Let us analyze the success probability of this attack. When $\mathcal{D}$ is interacting with the real world (EM_k^P, P), then it always outputs 1 since the pair (x^*, u^*) such that $x^* \oplus u^* = k$, where k is the secret key, necessarily satisfies Equation (10). This can easily be seen for example from the following "commutativity" property, holding for all $x \in \{0,1\}^n$:

$$k \oplus P(\mathsf{EM}_k^P(x)) = \mathsf{EM}_k^P(P(k \oplus x)).$$

On the other hand, suppose that E is a random permutation that is independent of P. We will show that the probability of finding (x^*, u^*) satisfying (10) is small. Fix any pair $(x, u) \in X \times U$. For any tuple (y, y', v, v') of n-bit values such that $y \neq y'$ and $v \neq v'$, we define

$$\begin{aligned}\mathsf{p}(y, y', v, v') &\stackrel{\text{def}}{=} \Pr\left[(x,u) \text{ satisfies (10)} \;\middle|\; \begin{array}{l} E(x) = y \wedge E(x \oplus c) = y' \\ P(u) = v \wedge P(u \oplus c) = v' \end{array}\right] \\ &= \Pr\left[P(y) \oplus E(v) = P(y') \oplus E(v') = x \oplus u \;\middle|\; \begin{array}{l} E(x) = y \wedge E(x \oplus c) = y' \\ P(u) = v \wedge P(u \oplus c) = v' \end{array}\right].\end{aligned}$$

In order to upper bound $\mathsf{p}(y, y', v, v')$, we distinguish the following four cases:

1. If $(y \notin \{u, u \oplus c\}$ or $v \notin \{x, x \oplus c\})$ and $(y' \notin \{u, u \oplus c\}$ or $v' \notin \{x, x \oplus c\})$, then
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)(N-3)}.$$
2. If $(y \in \{u, u \oplus c\}$ and $v \in \{x, x \oplus c\})$ and $(y' \notin \{u, u \oplus c\}$ or $v' \notin \{x, x \oplus c\})$, then
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)}.$$
3. If $(y \notin \{u, u \oplus c\}$ or $v \notin \{x, x \oplus c\})$ and $(y' \in \{u, u \oplus c\}$ and $v' \in \{x, x \oplus c\})$, then
$$\mathsf{p}(y, y', v, v') \leq \frac{1}{(N-2)}.$$
4. If $y \in \{u, u \oplus c\}$, $v \in \{x, x \oplus c\}$, $y' \in \{u, u \oplus c\}$, and $v' \in \{x, x \oplus c\}$, then
$$\mathsf{p}(y, y', v, v') \leq 1.$$

It remains to upper bound the number of tuples (y, y', v, v') for each case, and we obtain:

$$\begin{aligned}\Pr\left[(x,u) \text{ satisfies (10)}\right] &\leq \frac{1}{N^2(N-1)^2} \sum_{(y,y',v,v')} \mathsf{p}(y, y', v, v') \\ &\leq \frac{1}{N^2(N-1)^2} \left(\underbrace{\frac{N^2(N-1)^2}{(N-2)(N-3)}}_{\text{case 1}} + 2 \cdot \underbrace{\frac{4(N-1)^2}{N-2}}_{\text{cases 2\&3}} + \underbrace{4}_{\text{case 4}} \right) \\ &\leq \frac{1}{(N-2)(N-3)} + \frac{8}{N^2(N-2)} + \frac{4}{N^2(N-1)^2}.\end{aligned}$$

Summing over $(x,u) \in X \times U$, we finally obtain

$$\Pr[\exists (x,u) \text{ satisfying (10)}] \leq \frac{N}{(N-2)(N-3)} + \frac{8}{N(N-2)} + \frac{4}{N(N-1)^2} = \mathcal{O}\left(\frac{1}{N}\right).$$

Hence, when interacting with the ideal world, $\mathcal{D}$ outputs 1 with probability close to zero for large N. Thus, we just proved the following theorem.

Theorem 2. *Consider the r-round iterated Even-Mansour construction with a single permutation and identical round keys $\mathsf{EMSP}[n, r, \ell = n, \boldsymbol{\gamma} = \mathbf{Id}]$. Then there exists a distinguishing attack against this cipher which makes at most $2^{2+\frac{n}{2}}$ queries both to the outer and to the inner permutation, and which has a distinguishing advantage $1 - \mathcal{O}(\frac{1}{N})$.*

4.2 Extension to Key-Schedules Based on Xoring Constants

We show that the slide attack of the previous section can be extended to the single-permutation two-round Even-Mansour cipher with a very basic key-schedule, namely when the three round keys are derived as $k_i = k \oplus t_i$, where k is the n-bit master key and (t_0, t_1, t_2) are three (public) n-bit constants. The distinguisher, interacting with a pair of permutations (E, P), proceeds as follows:

1. Fix a nonzero $c \in \{0,1\}^n$ and two subsets X, $U \subset \{0,1\}^n$ such that $|X| = |U| = 2^{\frac{n}{2}}$ and
$$X \oplus U = \{x \oplus u : x \in X, u \in U\} = \{0,1\}^n.$$
(For example, X consists of all strings whose last $n/2$ bits are zero, and U consists of all strings whose first $n/2$ bits are zero.)
2. $\mathcal{D}$ makes queries
   - $E(x)$ and $E(x \oplus c)$ for $x \in X$
   - $P(u)$ and $P(u \oplus c)$ for $u \in U$
3. Using the responses to the above queries, $\mathcal{D}$ further makes queries
   - $E(t_0 \oplus t_1 \oplus P(u))$ and $E(t_0 \oplus t_1 \oplus P(u \oplus c))$ for $u \in U$
   - $P(t_1 \oplus t_2 \oplus E(x))$ and $P(t_1 \oplus t_2 \oplus E(x \oplus c))$ for $x \in X$
4. If there are $x^* \in X$ and $u^* \in U$ such that
$$\begin{cases} P(t_1 \oplus t_2 \oplus E(x^*)) \oplus E(t_0 \oplus t_1 \oplus P(u^*)) = t_0 \oplus t_2 \oplus x^* \oplus u^* \\ P(t_1 \oplus t_2 \oplus E(x^* \oplus c)) \oplus E(t_0 \oplus t_1 \oplus P(u^* \oplus c)) = t_0 \oplus t_2 \oplus x^* \oplus u^* \end{cases} \tag{11}$$
then $\mathcal{D}$ outputs 1. Otherwise, $\mathcal{D}$ outputs 0.

The numbers of E-queries and P-queries required for this attack are both at most $2^{2+\frac{n}{2}}$ (there might be redundant queries). Moreover this attack can easily be turned into a key-recovery attack, the key guess of the adversary being $k = t_0 \oplus x^* \oplus u^*$ for (x^*, u^*) satisfying conditions (11).

Let us analyze the success probability of this attack. When $\mathcal{D}$ is interacting with the real world (EM_k^P, P), then it always outputs 1 since the pair (x^*, u^*) such that $x^* \oplus u^* = k \oplus t_0$, where k is the secret master key, necessarily satisfies conditions (11). This can easily be seen for example from the following "commutativity" property, holding for all $x \in \{0,1\}^n$:

$$k \oplus t_2 \oplus P(t_1 \oplus t_2 \oplus \mathsf{EM}_k^P(x)) = \mathsf{EM}_k^P(t_0 \oplus t_1 \oplus P(k \oplus t_0 \oplus x)).$$

When the distinguisher is interacting with the ideal world (E, P), where E is a random permutation that is independent from P, then if we set $P' = t_0 \oplus t_1 \oplus P$ and $E' = t_1 \oplus t_2 \oplus E$, Equation (11) simplifies into Equation (10) with E and P replaced by E' and P', so that we can use exactly the same analysis as for the original attack of Section 4.1. Hence $\mathcal{D}$ outputs 1 with probability $\mathcal{O}(\frac{1}{N})$. Thus, we have the following theorem.

Theorem 3. *Consider the two-round Even-Mansour construction* $\mathsf{EMSP}[n, 2, \ell = n, \boldsymbol{\gamma}]$ *with a single permutation and round keys* k_i *derived from the* n*-bit master key* k *as* $\gamma_i(k) = k \oplus t_i$*, for publicly specified constants* (t_0, t_1, t_2)*. Then there exists a distinguishing attack against this cipher which makes at most* $2^{2+\frac{n}{2}}$ *queries both to the outer and to the inner permutation, and which has a distinguishing advantage* $1 - \mathcal{O}(\frac{1}{N})$*.*

5 Security Proof for Independent Permutations and Identical Round Keys

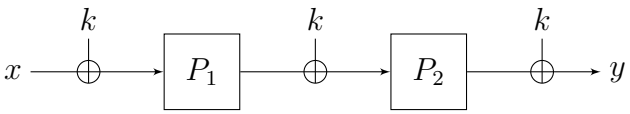

Fig. 3. The two-round Even-Mansour cipher with independent permutations and identical round keys.

In this section, we prove a $\widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$-security bound for the two-round Even-Mansour construction with two independent permutations and identical round keys $\mathsf{EMIP}[n, 2]$ (depicted on Figure 3). More precisely, we have the following theorem.

Theorem 4 (Independent permutations and identical round keys). *Consider the two-round Even-Mansour cipher with independent permutations and identical round keys* $\mathsf{EMIP}[n, 2]$*. Assume that* $9n \leq q_e, q_p \leq N/2$ *and* $2q_e + 2q_p \leq N$*. Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMIP}[n,2]}(q_e, q_p) \leq \frac{6}{N} + \frac{2q_e^2 q_p + 7q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e}}{N}.$$

Proof. The theorem directly follows from Lemma 1 and Lemmas 8 and 9 that are proven below. □

Letting $q = \max(q_e, q_p)$, the upper bound of Theorem 4 simplifies into

$$\frac{6}{N} + \frac{13q^3}{N^2} + \frac{9\sqrt{n}q^{\frac{3}{2}}}{N} = \frac{6}{2^n} + \frac{13q^3}{2^{2n}} + \frac{9q^{\frac{3}{2}}}{2^{n-\frac{1}{2}\log_2 n}}.$$

Hence, security is ensured up to $\mathcal{O}(2^{\frac{2n}{3}-\frac{1}{3}\log_2 n}) = \widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries of the adversary.

The remaining of this section is devoted to the proof of Theorem 4. Following the general methodology outlined in Section 2.4, our first task will be to define the set $\mathcal{T}_2$ of bad transcripts $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k)$, with $|\mathcal{Q}_E| = q_e$ and $|\mathcal{Q}_{P_1}| = |\mathcal{Q}_{P_2}| = q_p$. Informally, a transcript is bad if the key "connects" the set of queries too well. The formal definition follows.

Definition 1 (Bad transcript, independent permutations case). *We say that a transcript* $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k) \in \mathcal{T}$ *is* bad *if*

$$k \in \mathsf{BadK} = \bigcup_{1 \le i \le 3} \mathsf{BadK}_i$$

where:

$k \in \mathsf{BadK}_1 \Leftrightarrow k = x \oplus u_1 = v_2 \oplus y$ *for some* $(x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}$
$k \in \mathsf{BadK}_2 \Leftrightarrow k = x \oplus u_1 = v_1 \oplus u_2$ *for some* $(x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}$
$k \in \mathsf{BadK}_3 \Leftrightarrow k = v_1 \oplus u_2 = v_2 \oplus y$ *for some* $(x,y) \in \mathcal{Q}_E, (u_1,v_1) \in \mathcal{Q}_{P_1}, (u_2,v_2) \in \mathcal{Q}_{P_2}$.

Otherwise, τ *is said* good. *We denote* $\mathcal{T}_2$ *the set of bad transcripts, and* $\mathcal{T}_1 = \mathcal{T} \setminus \mathcal{T}_2$ *the set of good transcripts.*

We first upper bound the probability of obtaining a bad transcript in the ideal world.

Lemma 8. *Assume that* $9n \le q_e, q_p \le N/2$. *Then:*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \le \frac{6}{N} + \frac{2q_e^2 q_p + 3q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e}}{N}.$$

Proof. Note that in the ideal world, sets BadK_1, BadK_2 and BadK_3 only depend on the random permutations E, P_1, and P_2, and not on the key k, which is drawn uniformly at random at the end of the interaction of the distinguisher with (E, P_1, P_2). Hence, for any $C_1, C_2, C_3 > 0$, we can write

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \le \sum_{i=1,2,3} \Pr\left[E, P_1, P_2 \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_i| \ge C_i\right] + \frac{C_1 + C_2 + C_3}{N}.$$

Given a permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2})$, let:

$$\begin{aligned} X &= \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\}, & Y &= \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\}, \\ U_1 &= \{u_1 \in \{0,1\}^n : (u_1,v_1) \in \mathcal{Q}_{P_1}\}, & V_1 &= \{v_1 \in \{0,1\}^n : (u_1,v_1) \in \mathcal{Q}_{P_1}\}, \\ U_2 &= \{u_2 \in \{0,1\}^n : (u_2,v_2) \in \mathcal{Q}_{P_2}\}, & V_2 &= \{v_2 \in \{0,1\}^n : (u_2,v_2) \in \mathcal{Q}_{P_2}\} \end{aligned}$$

denote the domains and ranges of $\mathcal{Q}_E$, $\mathcal{Q}_{P_1}$, and $\mathcal{Q}_{P_2}$ respectively. Then one has

$$\begin{aligned} |\mathsf{BadK}_1| &\le \mu(\mathcal{Q}_E, U_1, V_2) \stackrel{\mathrm{def}}{=} |\{((x,y),u_1,v_2) \in \mathcal{Q}_E \times U_1 \times V_2 : x \oplus u_1 = v_2 \oplus y\}| \\ |\mathsf{BadK}_2| &\le \mu(\mathcal{Q}_{P_1}, X, U_2) \stackrel{\mathrm{def}}{=} |\{((u_1,v_1),x,u_2) \in \mathcal{Q}_{P_1} \times X \times U_2 : x \oplus u_1 = v_1 \oplus u_2\}| \\ |\mathsf{BadK}_3| &\le \mu(\mathcal{Q}_{P_2}, V_1, Y) \stackrel{\mathrm{def}}{=} |\{((u_2,v_2),v_1,y) \in \mathcal{Q}_{P_2} \times V_1 \times Y : v_1 \oplus u_2 = v_2 \oplus y\}|. \end{aligned}$$

We can now use Theorem 1 (with Γ the identity mapping) to upper bound $|\mathsf{BadK}_i|$ for $i = 1, 2, 3$, with high probability (note that in order to apply this theorem to upper bound, say, $|\mathsf{BadK}_1|$, we consider the combination of the distinguisher $\mathcal{D}$ and permutations P_1 and P_2 as a probabilistic adversary $\mathcal{A}$ interacting with permutation E, resulting in transcript $\mathcal{Q}_E$). We obtain that for

$$C_1 = \frac{q_e q_p^2}{N} + \frac{2q_e^2 q_p}{N} + 3q_p\sqrt{nq_e}$$

$$C_2 = C_3 = \frac{q_e q_p^2}{N} + \frac{2q_p^2\sqrt{q_e q_p}}{N} + 3q_p\sqrt{nq_e},$$

one has $\Pr[E, P_1, P_2 \leftarrow_\$ \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] \leq 2/N$ for each $i = 1, 2, 3$, which concludes the proof. □

In the second stage of the proof, we show that for any good transcript τ, the ratio between the probabilities to obtain τ in the ideal world and the real world is close to 1.

Lemma 9. *Assume that $2q_e + 2q_p \leq N$. Then for any $\tau \in \mathcal{T}_1$, we have:*

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \geq 1 - \frac{4q_e q_p^2}{N^2}.$$

Proof. Fix a good transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, k) \in \mathcal{T}_1$. In the following, we let:

$$\mathsf{p}(\tau) \stackrel{\mathrm{def}}{=} \Pr\left[P_1, P_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{EMIP}_k^{P_1,P_2} \vdash \mathcal{Q}_E \,\middle|\, (P_1 \vdash \mathcal{Q}_{P_1}) \wedge (P_2 \vdash \mathcal{Q}_{P_2})\right],$$

so that, by Lemma 2,

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau). \tag{12}$$

Hence, we now have to lower bound $\mathsf{p}(\tau)$. First, we modify the inner permutations P_1, P_2 and the transcript in order to "get rid" of the key k. For this, we define:

$$\begin{aligned}
P_1' &= P_1 \oplus k \\
P_2' &= P_2 \oplus k \\
\mathcal{Q}_E' &= \{(x \oplus k, y) : (x, y) \in \mathcal{Q}_E\} \\
\mathcal{Q}_{P_1}' &= \{(u_1, v_1 \oplus k) : (u_1, v_1) \in \mathcal{Q}_{P_1}\} \\
\mathcal{Q}_{P_2}' &= \{(u_2, v_2 \oplus k) : (u_2, v_2) \in \mathcal{Q}_{P_2}\}.
\end{aligned}$$

Then, one clearly has:

$$\mathsf{p}(\tau) = \Pr\left[P_1', P_2' \leftarrow_\$ \mathcal{P}_n : P_2' \circ P_1' \vdash \mathcal{Q}_E' \,\middle|\, (P_1' \vdash \mathcal{Q}_{P_1}') \wedge (P_2' \vdash \mathcal{Q}_{P_2}')\right].$$

Let:

$$\begin{aligned}
X &= \{x' \in \{0,1\}^n : (x', y') \in \mathcal{Q}_E'\}, & Y &= \{y' \in \{0,1\}^n : (x', y') \in \mathcal{Q}_E'\}, \\
U_1 &= \{u_1' \in \{0,1\}^n : (u_1', v_1') \in \mathcal{Q}_{P_1}'\}, & V_1 &= \{v_1' \in \{0,1\}^n : (u_1', v_1') \in \mathcal{Q}_{P_1}'\}, \\
U_2 &= \{u_2' \in \{0,1\}^n : (u_2', v_2') \in \mathcal{Q}_{P_2}'\}, & V_2 &= \{v_2' \in \{0,1\}^n : (u_2', v_2') \in \mathcal{Q}_{P_2}'\}
\end{aligned}$$

denote the domains and ranges of $\mathcal{Q}_E'$, $\mathcal{Q}_{P_1}'$, and $\mathcal{Q}_{P_2}'$ respectively. We also define $\alpha_1 = |V_2 \cap Y|$ and $\alpha_2 = |X \cap U_1|$. We can now rewrite the fact that τ is good as follows (see Figure 4):

$k \notin \mathsf{BadK}_1 \Leftrightarrow \mathcal{Q}_E'(X \cap U_1)$ is disjoint from $V_2 \Leftrightarrow (\mathcal{Q}_E')^{-1}(V_2 \cap Y)$ is disjoint from U_1
$k \notin \mathsf{BadK}_2 \Leftrightarrow \mathcal{Q}_{P_1}'(X \cap U_1)$ is disjoint from U_2
$k \notin \mathsf{BadK}_3 \Leftrightarrow (\mathcal{Q}_{P_2}')^{-1}(V_2 \cap Y)$ is disjoint from V_1.

To see why the first equivalence holds, note that:

$$\begin{aligned}
&\mathcal{Q}'_E(X \cap U_1) \cap V_2 \neq \emptyset \\
\Leftrightarrow\ & x' = u'_1 \text{ and } y' = v'_2 \text{ for some } (x', y') \in \mathcal{Q}'_E, (u'_1, v'_1) \in \mathcal{Q}'_{P_1}, \text{ and } (u'_2, v'_2) \in \mathcal{Q}'_{P_2} \\
\Leftrightarrow\ & k = x \oplus u_1 \text{ and } k = v_2 \oplus y \text{ for some } (x, y) \in \mathcal{Q}_E, (u_1, v_1) \in \mathcal{Q}_{P_1}, \text{ and } (u_2, v_2) \in \mathcal{Q}_{P_2} \\
\Leftrightarrow\ & k \in \mathsf{BadK}_1.
\end{aligned}$$

The other cases are proved similarly.

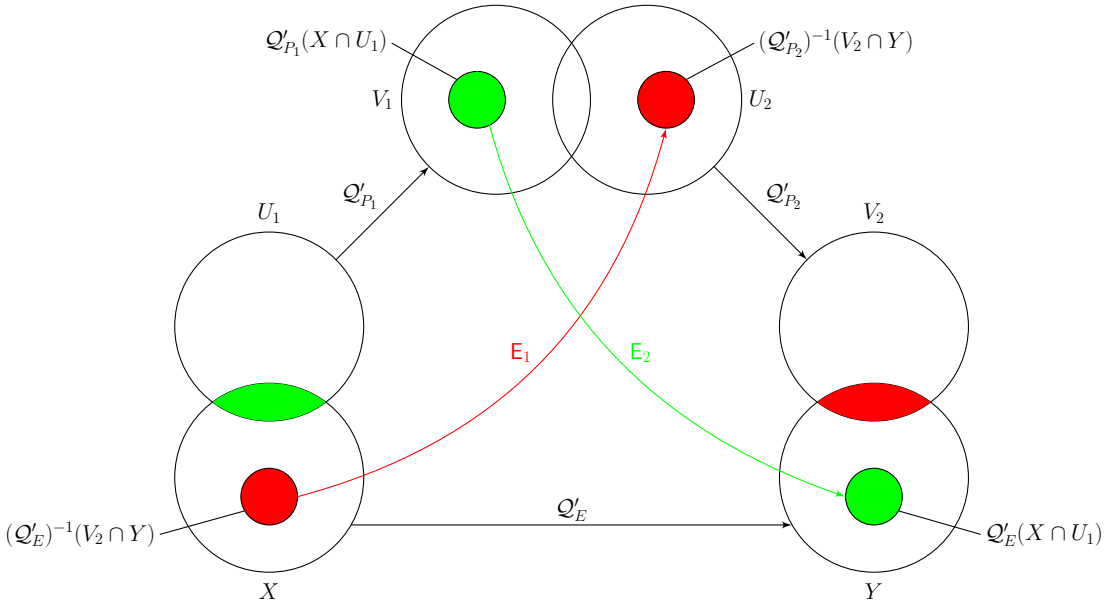

Fig. 4. Graphical help for the proof of Lemma 9. X and Y are of size q_e, while U_1, V_1, U_2, and V_2 are of size q_p. The red zones are of size α_1 and the green zones of size α_2.

This allows us to lower bound $\mathsf{p}(\tau)$ as follows. Let E_1 denote the event that $P'_1(x') = u'_2$ for each of the α_1 pairs of queries $((x', y'), (u'_2, v'_2)) \in \mathcal{Q}'_E \times \mathcal{Q}'_{P_2}$ such that $y' = v'_2$ (red arrow on Figure 4). Similarly, let E_2 be the event that $P'_2(v'_1) = y'$ for each of the α_2 pairs of queries $((x', y'), (u'_1, v'_1)) \in \mathcal{Q}'_E \times \mathcal{Q}'_{P_1}$ such that $x' = u'_1$ (green arrow on Figure 4). Since $P'_2 \circ P'_1 \vdash \mathcal{Q}'_E$ implies E_1 and E_2, we have

$$\begin{aligned}
\mathsf{p}(\tau) &= \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : (P'_2 \circ P'_1 \vdash \mathcal{Q}'_E) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right] \\
&= \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : P'_2 \circ P'_1 \vdash \mathcal{Q}'_E \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right] \\
&\quad \times \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right]. \qquad (13)
\end{aligned}$$

Moreover, since $(\mathcal{Q}'_E)^{-1}(V_2 \cap Y)$ is disjoint from U_1 and $(\mathcal{Q}'_{P_2})^{-1}(V_2 \cap Y)$ is disjoint from V_1, we have

$$\Pr\left[P'_1 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \middle| P'_1 \vdash \mathcal{Q}'_{P_1}\right] = \frac{1}{(N - q_p)_{\alpha_1}}.$$

Similarly, since $\mathcal{Q}'_{P_1}(X \cap U_1)$ is disjoint from U_2 and $\mathcal{Q}'_E(X \cap U_1)$ is disjoint from V_2, we have

$$\Pr\left[P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_2 | P'_2 \vdash \mathcal{Q}'_{P_2}\right] = \frac{1}{(N-q_p)_{\alpha_2}}.$$

Hence,

$$\Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 | (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2})\right] = \frac{1}{(N-q_p)_{\alpha_1} \cdot (N-q_p)_{\alpha_2}}. \quad (14)$$

Let $\alpha = \alpha_1 + \alpha_2$. Conditioned on event $(P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P'_1 is fixed on $q_p + \alpha_1$ points, P'_2 is fixed on $q_p + \alpha_2$ points, and $P'_2 \circ P'_1$ agrees with $\mathcal{Q}'_E$ on α pairs (x', y'). It remains to lower bound the probability p^* that $P'_2 \circ P'_1$ completes the remaining $q_e - \alpha$ evaluations needed to extend $\mathcal{Q}'_E$, namely

$$\mathsf{p}^* = \Pr\left[P'_1, P'_2 \leftarrow_\$ \mathcal{P}_n : P'_2 \circ P'_1 \vdash \mathcal{Q}'_E | (P'_1 \vdash \mathcal{Q}'_{P_1}) \wedge (P'_2 \vdash \mathcal{Q}'_{P_2}) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right].$$

Let S_1, resp. T_1, be the set of points for which P'_1, resp. $(P'_1)^{-1}$, has not been determined. More formally:

$$S_1 = \{0,1\}^n \setminus (U_1 \sqcup (\mathcal{Q}'_E)^{-1}(V_2 \cap Y))$$
$$T_1 = \{0,1\}^n \setminus (V_1 \sqcup (\mathcal{Q}'_{P_2})^{-1}(V_2 \cap Y)).$$

Similarly, let S_2, resp. T_2, be the set of points for which P'_2, resp. $(P'_2)^{-1}$, has not been determined. More formally:

$$S_2 = \{0,1\}^n \setminus (U_2 \sqcup \mathcal{Q}'_{P_1}(X \cap U_1))$$
$$T_2 = \{0,1\}^n \setminus (V_2 \sqcup \mathcal{Q}'_E(X \cap U_1).$$

Let also

$$X' = X \cap S_1 = X \setminus (U_1 \sqcup (\mathcal{Q}'_E)^{-1}(V_2 \cap Y))$$
$$Y' = Y \cap T_2 = Y \setminus (V_2 \sqcup \mathcal{Q}'_E(X \cap U_1)).$$

Then p^* is exactly the probability, over the choice of two random bijections $\overline{P'_1} : S_1 \to T_1$ and $\overline{P'_2} : S_2 \to T_2$, that $\overline{P'_2} \circ \overline{P'_1}(x') = y'$ for each $(x', y') \in \mathcal{Q}'_E$ such that $x' \in X'$ and $y' \in Y'$. We now lower bound p^*.

Note that $|X'| = |Y'| = q_e - \alpha$. Choose a set $W \subseteq \{0,1\}^n \setminus (V_1 \cup U_2)$ of size $q_e - \alpha$ (note that $N - 2q_p \geq q_e - \alpha$ by the assumption that $2q_e + 2q_p \leq N$) and a bijection $F : X' \to W$. The number of possibilities for the pair (W, F) is at least

$$\binom{N-2q_p}{q_e-\alpha}(q_e-\alpha)! = (N-2q_p)_{q_e-\alpha}.$$

For each choice of (W, F), the probability that random bijections $\overline{P'_1} : S_1 \to T_1$ and $\overline{P'_2} : S_2 \to T_2$, satisfy:

(1) $\overline{P'_1}(x') = F(x')$ for each $x' \in X'$,
(2) $\overline{P'_2} \circ \overline{P'_1}(x') = y'$ for each $(x', y') \in \mathcal{Q}'_E$ such that $x' \in X'$ and $y' \in Y'$

is exactly

$$\frac{1}{(N-q_p-\alpha_1)_{q_e-\alpha}(N-q_p-\alpha_2)_{q_e-\alpha}},$$

since condition (1) fixes $q_e-\alpha$ distinct equations on $\overline{P'_1}$ and condition (2) fixes $q_e-\alpha$ distinct equations on $\overline{P'_2}$. Hence, summing over all the possibilities for the pair (W,F), we obtain

$$\mathsf{p}^* \geq \frac{(N-2q_p)_{q_e-\alpha}}{(N-q_p-\alpha_1)_{q_e-\alpha}(N-q_p-\alpha_2)_{q_e-\alpha}}. \tag{15}$$

Gathering (12), (13), (14), and (15) finally yields:

$$\begin{aligned}
\frac{\Pr[T_{\mathrm{re}}=\tau]}{\Pr[T_{\mathrm{id}}=\tau]} &\geq \frac{(N)_{q_e}(N-2q_p)_{q_e-\alpha}}{(N-q_p)_{\alpha_1}(N-q_p-\alpha_1)_{q_e-\alpha}(N-q_p)_{\alpha_2}(N-q_p-\alpha_2)_{q_e-\alpha}} \\
&= \frac{(N)_{q_e}(N-2q_p)_{q_e-\alpha}}{(N-q_p)_{q_e-\alpha_2}(N-q_p)_{q_e-\alpha_1}} \\
&= \frac{(N)_{q_e}(N-2q_p)_{q_e}}{(N-q_p)_{q_e}(N-q_p)_{q_e}} \times \underbrace{\frac{(N-q_p-q_e+\alpha_2)_{\alpha_2}(N-q_p-q_e+\alpha_1)_{\alpha_1}}{(N-2q_p-q_e+\alpha)_{\alpha}}}_{\geq 1} \\
&\geq \frac{(N)_{q_e}(N-2q_p)_{q_e}}{((N-q_p)_{q_e})^2} \\
&\geq 1-\frac{4q_eq_p^2}{N^2},
\end{aligned}$$

where for the last inequality we used Lemma 3 with $a=q_e$ and $b=c=d=q_p$, and the assumption that $2q_e+2q_p\leq N$. This concludes the proof. □

6 Security Proof for the Single Permutation Case

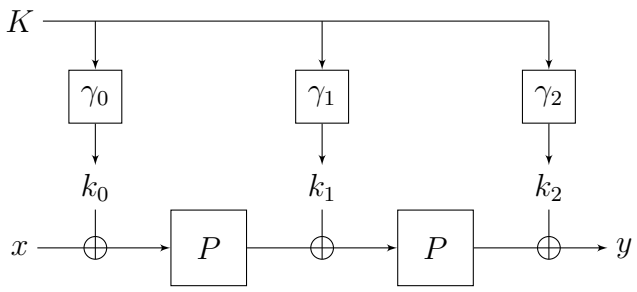

Fig. 5. The two-round Even-Mansour cipher with a single permutation and an arbitrary key-schedule.

In this section, we study the security of the two-round Even-Mansour construction where a single permutation P is used instead of two independent permutations, namely $\mathsf{EMSP}[n,r,\ell,\boldsymbol{\gamma}]$ (depicted on Figure 5). By the results of Section 4, we know that we cannot simply use the same n-bit key k at each round if we aim at proving security beyond the birthday bound, so

that some non-trivial key-schedule $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, with $\gamma_i : \{0,1\}^\ell \to \{0,1\}^n$, is needed (we remain as general as possible in a first phase, and will only specify the key-schedule later on). Given a key $K \in \{0,1\}^\ell$, we denote $k_0 = \gamma_0(K)$, $k_1 = \gamma_1(K)$, and $k_2 = \gamma_2(K)$, so that:

$$\mathsf{EMSP}_K^P(x) = P(P(x \oplus k_0) \oplus k_1) \oplus k_2.$$

6.1 Good Transcripts and Their Properties

Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K)$, with $|\mathcal{Q}_E| = q_e$, $|\mathcal{Q}_P| = q_p$, and $K \in \{0,1\}^\ell$ be an attainable transcript. As previously, we start by defining the set of bad transcripts. In all the following, we let

$$M = \frac{q_e}{N^{\frac{1}{3}}}.$$

Definition 2 (Bad transcript, single-permutation case). *We say that a transcript* $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}$ *is* bad *if*

$$K \in \mathsf{BadK} = \bigcup_{1 \le i \le 10} \mathsf{BadK}_i$$

where

$$\begin{aligned}
K \in \mathsf{BadK}_1 &\Leftrightarrow k_0 = x \oplus u \text{ and } k_2 = v' \oplus y \text{ for some } (x,y) \in \mathcal{Q}_E \text{ and } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_2 &\Leftrightarrow k_0 = x \oplus u \text{ and } k_1 = v \oplus u' \text{ for some } (x,y) \in \mathcal{Q}_E \text{ and } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_3 &\Leftrightarrow k_1 = v \oplus u' \text{ and } k_2 = v' \oplus y \text{ for some } (x,y) \in \mathcal{Q}_E \text{ and } (u,v),(u',v') \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_4 &\Leftrightarrow k_0 = x \oplus u \text{ and } k_0 \oplus k_1 = v \oplus x' \text{ for some } (x,y),(x',y') \in \mathcal{Q}_E, (u,v) \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_5 &\Leftrightarrow k_1 \oplus k_2 = y' \oplus u \text{ and } k_2 = v \oplus y \text{ for some } (x,y),(x',y') \in \mathcal{Q}_E, (u,v) \in \mathcal{Q}_P \\
K \in \mathsf{BadK}_6 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : x \oplus u = k_0\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_7 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : v \oplus y = k_2\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_8 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : x \oplus v = k_0 \oplus k_1\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_9 &\Leftrightarrow |\{((x,y),(u,v)) \in \mathcal{Q}_E \times \mathcal{Q}_P : u \oplus y = k_1 \oplus k_2\}| > \frac{M}{3} \\
K \in \mathsf{BadK}_{10} &\Leftrightarrow \left|\{((x,y),(x',y')) \in \mathcal{Q}_E \times \mathcal{Q}_E : x \oplus y' = k_0 \oplus k_1 \oplus k_2\}\right| > M.
\end{aligned}$$

Otherwise τ *is said* good. *We denote* $\mathcal{T}_2$ *the set of bad transcripts, and* $\mathcal{T}_1 = \mathcal{T} \setminus \mathcal{T}_2$ *the set of good transcripts.*

We postpone the discussion of the probability to obtain a bad transcript to the next section, and focus first on the properties of good transcripts. Namely, we will show the following lemma.

Lemma 10. *Assume that* $N \ge 7^3$ *and* $4q_e + 2q_p \le N$. *Let* $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}_1$ *be a good transcript. Then*

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

where

$$\varepsilon_1 = \frac{4q_e(q_e+q_p)^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{20q_e}{N^{\frac{2}{3}}}.$$

Proof. Fix a good transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, K) \in \mathcal{T}_1$. In the following, we let:

$$\mathsf{p}(\tau) \stackrel{\text{def}}{=} \Pr\left[P \leftarrow_{\$} \mathcal{P}_n : \mathsf{EMSP}_K^P \vdash \mathcal{Q}_E \middle| P \vdash \mathcal{Q}_P\right],$$

so that, by Lemma 2,

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} = (N)_{q_e} \cdot \mathsf{p}(\tau). \tag{16}$$

Our goal is now to lower bound $\mathsf{p}(\tau)$. First, we modify the inner permutation P and the transcript in order to get rid of the round keys as follows:

$$\begin{aligned} P' &= P \oplus k_1, \\ \mathcal{Q}'_E &= \{(x \oplus k_0, y \oplus k_1 \oplus k_2) : (x, y) \in \mathcal{Q}_E\}, \\ \mathcal{Q}'_P &= \{(u, v \oplus k_1) : (u, v) \in \mathcal{Q}_P\}. \end{aligned}$$

Then we have

$$\mathsf{p}(\tau) = \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E | P' \vdash \mathcal{Q}'_P\right].$$

Let

$$\begin{aligned} X &= \{x' \in \{0,1\}^n : (x', y') \in \mathcal{Q}'_E\}, & Y &= \{y' \in \{0,1\}^n : (x', y') \in \mathcal{Q}'_E\}, \\ U &= \{u' \in \{0,1\}^n : (u', v') \in \mathcal{Q}'_P\}, & V &= \{v' \in \{0,1\}^n : (u', v') \in \mathcal{Q}'_P\} \end{aligned}$$

denote the domains and the ranges of $\mathcal{Q}'_E$ and $\mathcal{Q}'_P$, respectively. We also denote $\alpha_1 = |Y \cap V|$ and $\alpha_2 = |X \cap U|$. We can now rewrite the fact that the transcript is good as follows (see Figure 6):

$$K \notin \mathsf{BadK}_1 \Leftrightarrow \mathcal{Q}'_E(X \cap U) \text{ is disjoint from } V \Leftrightarrow (\mathcal{Q}'_E)^{-1}(Y \cap V) \text{ is disjoint from } U \tag{B.1}$$
$$K \notin \mathsf{BadK}_2 \Leftrightarrow \mathcal{Q}'_P(X \cap U) \text{ is disjoint from } U \tag{B.2}$$
$$K \notin \mathsf{BadK}_3 \Leftrightarrow (\mathcal{Q}'_P)^{-1}(Y \cap V) \text{ is disjoint from } V \tag{B.3}$$
$$K \notin \mathsf{BadK}_4 \Leftrightarrow \mathcal{Q}'_P(X \cap U) \text{ is disjoint from } X \tag{B.4}$$
$$K \notin \mathsf{BadK}_5 \Leftrightarrow (\mathcal{Q}'_P)^{-1}(Y \cap V) \text{ is disjoint from } Y \tag{B.5}$$
$$K \notin \mathsf{BadK}_6 \Leftrightarrow \alpha_2 = |X \cap U| \leq \frac{M}{3} \tag{B.6}$$
$$K \notin \mathsf{BadK}_7 \Leftrightarrow \alpha_1 = |Y \cap V| \leq \frac{M}{3} \tag{B.7}$$
$$K \notin \mathsf{BadK}_8 \Leftrightarrow |X \cap V| \leq \frac{M}{3} \tag{B.8}$$
$$K \notin \mathsf{BadK}_9 \Leftrightarrow |Y \cap U| \leq \frac{M}{3} \tag{B.9}$$
$$K \notin \mathsf{BadK}_{10} \Leftrightarrow |X \cap Y| \leq M. \tag{B.10}$$

Let E_1 denote the event that $P'(x') = u'$ for each of α_1 pairs of queries $((x', y'), (u', v')) \in \mathcal{Q}'_E \times \mathcal{Q}'_P$ such that $y' = v'$ (red arrows on Figure 6). Similarly, let E_2 be the event that $P'(v') = y'$ for each of α_2 pairs of queries $((x', y'), (u', v')) \in \mathcal{Q}'_E \times \mathcal{Q}'_P$ such that $x' = u'$ (green arrows on Figure 6). Since $P' \circ P' \vdash \mathcal{Q}'_E$ implies E_1 and E_2, we have

$$\mathsf{p}(\tau) = \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : (P' \circ P' \vdash \mathcal{Q}'_E) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| P' \vdash \mathcal{Q}'_P\right]$$

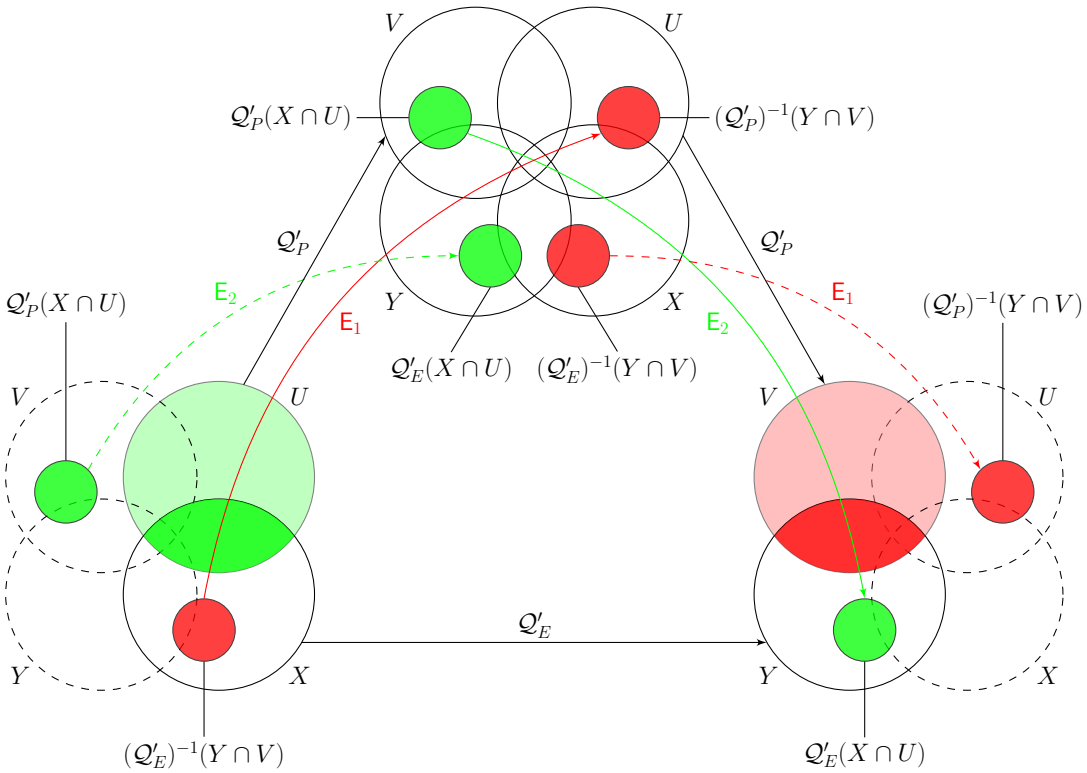

Fig. 6. Graphical help for the proof of Lemma 10. X and Y are of size q_e, while U and V are of size q_p. The red zones are of size α_1, and the green zones of size α_2. Conditioning on $(P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P' is defined on the zones which are colored on the left, while $(P')^{-1}$ is defined on the zones which are colored on the right.

$$= \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E \middle| (P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right]$$
$$\times \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| P' \vdash \mathcal{Q}'_P\right]. \tag{17}$$

Note that:

1. U, $\mathcal{Q}'_P(X \cap U)$, and $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ are pairwise disjoint since:
   - U and $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ are disjoint by (B.1),
   - U and $\mathcal{Q}'_P(X \cap U)$ are disjoint by (B.2),
   - $(\mathcal{Q}'_E)^{-1}(Y \cap V)$ is contained in X, and X and $\mathcal{Q}'_P(X \cap U)$ are disjoint by (B.4);
2. V, $\mathcal{Q}'_E(X \cap U)$, and $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ are pairwise disjoint since:
   - V and $\mathcal{Q}'_E(X \cap U)$ are disjoint by (B.1),
   - V and $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ are disjoint by (B.3),
   - $\mathcal{Q}'_E(X \cap U)$ is contained in Y, and Y and $(\mathcal{Q}'_P)^{-1}(Y \cap V)$ are disjoint by (B.5).

Therefore we have

$$\Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : \mathsf{E}_1 \wedge \mathsf{E}_2 \middle| P' \vdash \mathcal{Q}'_P\right] = \frac{1}{(N - q_p)_{\alpha_1 + \alpha_2}}. \tag{18}$$

Let $\alpha = \alpha_1 + \alpha_2$. Conditioned on event $(P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2$, P' is fixed on $q_p + \alpha$ points, and $P' \circ P'$ agrees with $\mathcal{Q}'_E$ on α pairs (x', y'). It remains to lower bound the probability p^* that $P' \circ P'$ completes the remaining $q_e - \alpha$ evaluations needed to extend $\mathcal{Q}'_E$, namely

$$\mathsf{p}^* = \Pr\left[P' \leftarrow_{\$} \mathcal{P}_n : P' \circ P' \vdash \mathcal{Q}'_E \middle| (P' \vdash \mathcal{Q}'_P) \wedge \mathsf{E}_1 \wedge \mathsf{E}_2\right].$$

Let $S \subseteq \{0,1\}^n$ denote the set of points for which P' has not been determined, more formally

$$S = \{0,1\}^n \setminus (U \sqcup \mathcal{Q}'_P(X \cap U) \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V)),$$

and let $T \subseteq \{0,1\}^n$ be the set of points for which $(P')^{-1}$ has not been determined, more formally

$$T = \{0,1\}^n \setminus (V \sqcup \mathcal{Q}'_E(X \cap U) \sqcup (\mathcal{Q}'_P)^{-1}(Y \cap V)).$$

Let also

$$X' = X \cap S = X \setminus (U \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V))$$
$$Y' = Y \cap T = Y \setminus (V \sqcup \mathcal{Q}'_E(X \cap U)).$$

(Note that $\mathcal{Q}'_E(X') = Y'$.) Then p^* is exactly the probability that $\overline{P'} \circ \overline{P'}(x') = y'$ for each $(x', y') \in \mathcal{Q}'_E$ such that $x' \in X'$ and $y' \in Y'$, over the random choice of bijection $\overline{P'} : S \to T$. Note that

1. $|S| = |T| = N - q_p - \alpha$;
2. $|X'| = |Y'| = q_e - \alpha$;
3. $|X' \cap Y'| \leq |X \cap Y| \leq M$ by (B.10);
4. $|X' \setminus T| \leq M$ since

$$\begin{aligned} X' \setminus T \subseteq X \setminus T &= X \cap \overline{T} \\ &= (X \cap V) \sqcup (X \cap \mathcal{Q}'_E(X \cap U)) \sqcup (X \cap (\mathcal{Q}'_P)^{-1}(Y \cap V)) \\ &\subseteq (X \cap V) \sqcup \mathcal{Q}'_E(X \cap U) \sqcup (\mathcal{Q}'_P)^{-1}(Y \cap V), \end{aligned}$$

and $|X \cap V|$, $|X \cap U|$, and $|Y \cap V|$ are at most $M/3$ by resp. (B.8), (B.6), and (B.7);

5. $|Y' \setminus S| \le M$ since

$$\begin{aligned} Y' \setminus S \subseteq Y \setminus S &= Y \cap \overline{S} \\ &= (Y \cap U) \sqcup (Y \cap \mathcal{Q}'_P(X \cap U)) \sqcup (Y \cap (\mathcal{Q}'_E)^{-1}(Y \cap V)) \\ &\subseteq (Y \cap U) \sqcup \mathcal{Q}'_P(X \cap U) \sqcup (\mathcal{Q}'_E)^{-1}(Y \cap V), \end{aligned}$$

and $|Y \cap U|$, $|X \cap U|$, and $|Y \cap V|$ are at most $M/3$ by resp. (B.9), (B.6), and (B.7).

At this point, let us recapitulate the problem of lower bounding p^*. We denote $q = q_e - \alpha$ and $q' = q_p + \alpha$.

Problem 1. Let N, q, q' be positive integers and $M > 0$. Let $S, T \subseteq \{0,1\}^n$, where $|S| = |T| = N - q'$. Let also $X' = \{x_1, \dots, x_q\} \subseteq S$ and $Y' = \{y_1, \dots, y_q\} \subseteq T$ be sets of size q. Assume that

$$|X' \cap Y'|, |X' \setminus T|, \text{ and } |Y' \setminus S| \le M, \tag{A.1}$$
$$6M \le q, \tag{A.2}$$
$$4q + 2q' \le N. \tag{A.3}$$

Find a lower bound on the probability p^* that a random bijection P from S to T satisfies $P(P(x_i)) = y_i$ for every $i = 1, \dots, q$. ◇

We will prove in Lemma 11 the lower bound

$$\mathsf{p}^* \ge \frac{1}{(N)_q} \left(1 - \frac{14M^2}{q} - \frac{3q^2}{MN} - \frac{4q(q+q')^2}{N^2}\right). \tag{19}$$

Before proving (19), let us finish the proof of Lemma 12. Note that assumptions (A.1), (A.2), and (A.3) needed to apply (19) are satisfied:

- assumption (A.1) is satisfied since we assume that τ is good;
- $\alpha \le M$ by (B.6) and (B.7) since τ is good, and by our original assumption that $N \ge 7^3$, we have $7M \le q_e$, so that $6M \le q_e - M \le q_e - \alpha = q$, and hence assumption (A.2) is satisfied;
- by our original assumption that $4q_e + 2q_p \le N$, assumption (A.3) is satisfied.

Therefore, combining (16), (17), (18), and (19), we have:

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \ge \frac{(N)_{q_e}}{(N)_{q_e-\alpha}(N-q_p)_\alpha} \left(1 - \frac{14M^2}{q_e - \alpha} - \frac{3(q_e-\alpha)^2}{MN} - \frac{4(q_e-\alpha)(q_e+q_p)^2}{N^2}\right).$$

Since

$$\frac{(N)_{q_e}}{(N)_{q_e-\alpha}(N-q_p)_\alpha} = \frac{(N-q_e+\alpha)_\alpha}{(N-q_p)_\alpha} \ge \frac{(N-q_e)_\alpha}{(N)_\alpha} \ge 1 - \frac{q_e\alpha}{N-\alpha+1} \ge 1 - \frac{Mq_e}{N-M},$$

we obtain

$$\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} \ge 1 - \frac{Mq_e}{N-M} - \frac{14M^2}{q_e - M} - \frac{3q_e^2}{MN} - \frac{4q_e(q_e+q_p)^2}{N^2}.$$

Substituting $M = q_e/N^{\frac{1}{3}}$, and noting that $N - M \geq N/2$ and $q_e - M \geq 6q_e/7$, we finally obtain

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

where

$$\varepsilon_1 = \frac{4q_e(q_e + q_p)^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{20q_e}{N^{\frac{2}{3}}}.$$

This concludes the proof. □

It remains to prove the answer to Problem 1, which we do in the following lemma.

Lemma 11. *Let N, q, q' be positive integers and $M > 0$. Let S, $T \subseteq \{0,1\}^n$, where $|S| = |T| = N - q'$. Let also $X' = \{x_1, \ldots, x_q\} \subseteq S$ and $Y' = \{y_1, \ldots, y_q\} \subseteq T$ be sets of size q. Assume that*

$$|X' \cap Y'|, |X' \setminus T|, \text{ and } |Y' \setminus S| \leq M, \tag{A.1}$$
$$6M \leq q, \tag{A.2}$$
$$4q + 2q' \leq N. \tag{A.3}$$

Let p^* be the probability that a random bijection P from S to T satisfies $P(P(x_i)) = y_i$ for every $i = 1, \ldots, q$.[7] Then

$$\mathsf{p}^* \geq \frac{1}{(N)_q}\left(1 - \frac{14M^2}{q} - \frac{3q^2}{MN} - \frac{4q(q+q')^2}{N^2}\right).$$

Proof. The reader might find helpful to refer to Figure 7 along the proof. A simple way to lower bound p^* would be to only count bijections P such that $P(X') \cap X' = \emptyset$. However, this is not good enough for our purpose since this only yields a q^2/N bound. Hence, we also need to count bijections P such that $|P(X') \cap X'| = k$ for k in some sufficiently large range. (Jumping ahead, $P(X') \cap X'$ will be X_2 in the proof below).

Let $Z \subseteq X'$ be defined as

$$\begin{aligned} Z &= \{x_i \in X' : x_i \in T \wedge x_i \notin Y' \wedge y_i \in S \wedge y_i \notin X'\} \\ &= X' \setminus (\overline{T} \cup Y' \cup \{x_i \in X' : y_i \in Y' \setminus S\} \cup \{x_i \in X' : y_i \in X' \cap Y'\}) \\ &= X' \setminus ((X' \setminus T) \cup (X' \cap Y') \cup \{x_i \in X' : y_i \in Y' \setminus S\} \cup \{x_i \in X' : y_i \in X' \cap Y'\}). \end{aligned}$$

Let $q'' = |Z|$. Since by assumption (A.1) we have $|X' \cap Y'|$, $|X' \setminus T|$, and $|Y' \setminus S| \leq M$, it follows that $q'' \geq q - 4\lfloor M \rfloor \geq 2\lfloor M \rfloor$, where the last inequality follows from assumption (A.2) which implies that $6\lfloor M \rfloor \leq q$.

For each $0 \leq k \leq M$, choose two disjoint subsets X_1, $X_2 \subset Z$ of size k. We will write

$$\begin{aligned} X_1 &= \{x_{i_1}, \ldots, x_{i_k}\} \\ X_2 &= \{x_{i_{k+1}}, \ldots, x_{i_{2k}}\} \\ X' \setminus (X_1 \cup X_2) &= \{x_{i_{2k+1}}, \ldots, x_{i_q}\} \end{aligned}$$

[7] If $P(x_i) \notin S$, then $P(P(x_i))$ is regarded as undefined.

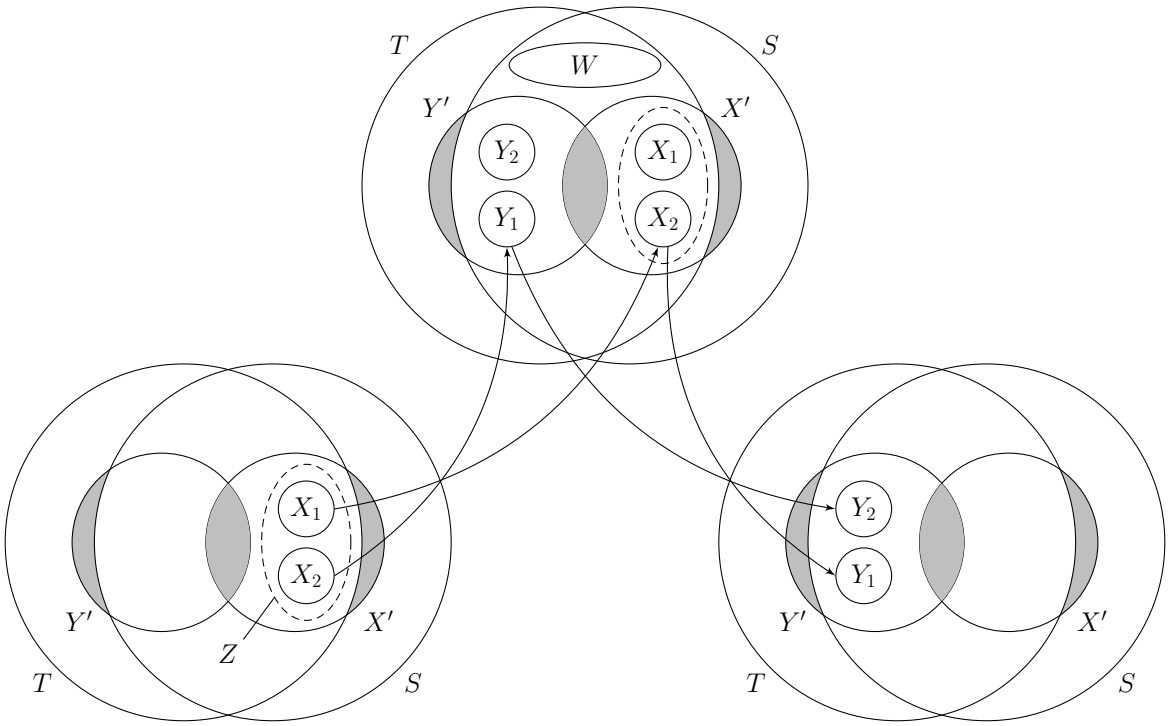

Fig. 7. Graphical help for the proof of Lemma 11. S and T are of size $N - q'$, while X' and Y' are of size q. The gray zones $X' \cap Y'$, $X' \setminus T$, and $Y' \setminus S$ are of size at most M. Sets X_1, X_2, Y_1, Y_2 are each of size k. The set W is of size $q - 2k$.

where $i_1 < \cdots < i_k$ and $i_{k+1} < \cdots < i_{2k}$ and $i_{2k+1} < \cdots < i_q$. Given (X_1, X_2), choose a bijection $F : X_1 \to X_2$ such that $F(X_1) = X_2$. The number of possibilities for (X_1, X_2, F) is

$$\binom{q''}{k}\binom{q''-k}{k}k! = \frac{(q'')_{2k}}{k!}. \tag{20}$$

For each pair of sets (X_1, X_2), let $Y_1 = \{y_{i_1}, \ldots, y_{i_k}\}$ and $Y_2 = \{y_{i_{k+1}}, \ldots, y_{i_{2k}}\}$. For a fixed pair of sets (X_1, X_2), we also choose

$$W \subset (S \cap T) \setminus (X' \cup Y')$$

such that $|W| = q - 2k$. This is possible (i.e., $(S \cap T) \setminus (X' \cup Y')$ is large enough) since by assumption (A.3), $N \geq 3q + 2q'$, so that for $0 \leq k \leq M$ we have

$$|(S \cap T) \setminus (X' \cup Y')| \geq |S \cap T| - |X' \cup Y'| \geq (N - 2q') - 2q \geq q - 2k.$$

For each choice of W, we also choose a bijection $G : X' \setminus (X_1 \cup X_2) \to W$. Then, the number of possibilities for the pair (W, G) is at least

$$\binom{N - 2q - 2q'}{q - 2k} \times (q - 2k)! = (N - 2q - 2q')_{q-2k}. \tag{21}$$

For each choice of (X_1, X_2, F, W, G), the probability that a random bijection $P : S \to T$ satisfies

(1) $P(x) = F(x)$ for each $x \in X_1$,
(2) $P(x) = G(x)$ for each $x \in X' \setminus (X_1 \cup X_2)$,
(3) $P(P(x_i)) = y_i$ for every $i = 1, \ldots, q$

is exactly

$$\frac{1}{(N - q')_{2q-k}}. \tag{22}$$

To see why this last claim holds, denote $\Pi : X' \to Y'$ the bijection such that $\Pi(x_i) = y_i$ for $i = 1, \ldots, q$. Then a bijection $P : S \to T$ satisfies (1), (2) and (3) above *iff* (see also Figure 7):

i) $P(x) = F(x)$ for each $x \in X_1$, which yields k equations;
ii) $P(x) = G(x)$ for each $x \in X' \setminus (X_1 \cup X_2)$, which yields $q - 2k$ additional equations;
iii) $P(z) = \Pi(F^{-1}(z))$ for each $z \in X_2$ (note that $X_2 \subseteq S$), so that $P(P(x)) = \Pi(x)$ for each $x \in X_1$; this yields k additional equations;
iv) $P(z) = \Pi(F(\Pi^{-1}(z)))$ for each $z \in Y_1$ (note that $Y_1 \subseteq S$), so that $P(P(x)) = \Pi(x)$ for each $x \in X_2$; this yields k additional equations since $Y_1 \cap X' = \emptyset$;
v) $P(z) = \Pi(G^{-1}(z))$ for each $z \in W$, so that $P(P(x)) = \Pi(x)$ for each $x \in X' \setminus (X_1 \cup X_2)$; this yields $q - 2k$ additional equations since W is disjoint from $X' \cup Y_1$.

In total this amounts to $(2q - k)$ equations, hence the claim. Gathering (20), (21), and (22), and since $q'' \geq q - 4\lfloor M \rfloor$, we have

$$\mathsf{p}^* \geq \sum_{0 \leq k \leq M} \frac{(q'')_{2k}(N - 2q - 2q')_{q-2k}}{k!(N - q')_{2q-k}}$$

$$\geq \sum_{0\leq k\leq M} \frac{(q)_{2k}(N-2q-q')_{q-2k}(N-q')_q}{k!(N-q')_{2q-k}} \times \frac{(q-4\lfloor M\rfloor)_{2k}(N-2q-2q')_{q-2k}}{(q)_{2k}(N-2q-q')_{q-2k}(N-q')_q}$$
$$\geq \frac{1}{(N)_q} \sum_{0\leq k\leq M} C_{N-q',q,k} \times \underbrace{\frac{(q-4\lfloor M\rfloor)_{2k}}{(q)_{2k}}}_{A} \times \underbrace{\frac{(N)_q(N-2q-2q')_{q-2k}}{(N-q')_q(N-2q-q')_{q-2k}}}_{B},$$

where the quantity $C_{N,q,k}$ was defined in Lemma 4, Section 2.5. Moreover, for any $0 \leq k \leq M$, we have

$$A \geq \frac{(q-4\lfloor M\rfloor)_{2\lfloor M\rfloor}}{(q)_{2\lfloor M\rfloor}} \geq \left(1-\frac{4\lfloor M\rfloor}{q-2\lfloor M\rfloor+1}\right)^{2\lfloor M\rfloor} \geq 1-\frac{8\lfloor M\rfloor^2}{q-2\lfloor M\rfloor+1} \geq 1-\frac{12\lfloor M\rfloor^2}{q},$$

where for the last inequality we used assumption (A.2) which implies $q-2\lfloor M\rfloor \geq 2q/3$, and

$$B \geq \frac{(N)_q(N-2q-2q')_q}{(N-q')_q(N-2q-q')_q} \geq 1-\frac{4q(q+q')^2}{N^2},$$

where we applied Lemma 3 with $a=q$, $b=q+q'$, $c=q'$, and $d=2q+q'$ (note that $2a+2b \leq N$ by assumption (A.3)).

Hence, we finally obtain, using Lemma 4 (note that the condition $M \leq q/2 \leq (N-q')/6$ needed to apply Lemma 4 holds by assumptions (A.2) and (A.3)),

$$\mathsf{p}^* \geq \frac{1}{(N)_q}\left(1-\frac{2M^2}{q}-\frac{3q^2}{2M(N-q')}-\frac{12M^2}{q}-\frac{4q(q+q')^2}{N^2}\right)$$
$$\geq \frac{1}{(N)_q}\left(1-\frac{14M^2}{q}-\frac{3q^2}{MN}-\frac{4q(q+q')^2}{N^2}\right),$$

where for the last inequality we used assumption (A.3) which implies $N-q' \geq N/2$. □

6.2 Probability of Bad Transcripts for Non-Independent Round Keys

In this section, we focus on the case where $\ell = n$, namely the master key length is equal to the block length (and hence to the round keys length). We treat the (simpler) cases where the three round keys are independent, or derived from two independent n-bit keys, respectively in Appendices A and B. First, we specify conditions on the key-schedule that will allow us to upper bound the probability to obtain a bad transcript (in the ideal world).

Definition 3 (Good key-schedule). *We say that a key-schedule* $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, *where* $\gamma_i : \{0,1\}^n \to \{0,1\}^n$, *is* good *if it satisfies the following conditions:*

(i) $\gamma_0, \gamma_1, \gamma_2 \in \mathsf{GL}(n)$ *(i.e., each* γ_i *is a linear bijective map of* $\mathbb{F}_2^n$*);*
(ii) $\gamma_0 \oplus \gamma_1 \in \mathsf{GL}(n)$ *and* $\gamma_1 \oplus \gamma_2 \in \mathsf{GL}(n)$*;*
(iii) $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ *is a permutation over* $\{0,1\}^n$ *(non-necessarily linear over* $\mathbb{F}_2^n$*).*

A simple way to build a good key-schedule is to take for γ_0 and γ_2 the identity, and $\gamma_1 = \pi$, where π is a linear orthomorphism of $\mathbb{F}_2^n$ (recall that a permutation π of $\{0,1\}^n$ is an orthomorphism if $x \mapsto x \oplus \pi(x)$ is also a permutation), so that the sequence of round keys is $(k, \pi(k), k)$. We give two simple examples of linear orthomorphisms which are attractive from an implementation point of view:

– When n is even, and $k = (k_L, k_R)$ where k_L and k_R are respectively the left and right halves of k, then
$$\pi : (k_L, k_R) \mapsto (k_R, k_L \oplus k_R)$$
is a linear orthomorphism.
– Fix an irreducible polynomial p of degree n over $\mathbb{F}_2$ and identify $\mathbb{F}_2^n$ and the extension field $\mathbb{F}_{2^n}$ defined by p in the canonical way. Then, for any $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, $k \mapsto c \odot k$ (where $\odot$ denotes the extension field multiplication) is a linear orthomorphism.

Lemma 12. *Let $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$ be a good key-schedule. Assume that $9n \leq q_e, q_p \leq N/2$. Then*
$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{10}{N} + \frac{4q_e^2 q_p + 7q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{9q_p\sqrt{nq_e} + 6q_e\sqrt{nq_p}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}.$$

Proof. In the ideal world, sets BadK_i only depend on the random permutations E and P, and not on the key k, which is drawn uniformly at random at the end of the interaction of the distinguisher with (E, P). Moreover, the size of BadK_i for $i = 6$ to 10 can be upper bounded independently of E, P. Indeed, since γ_0, γ_2, $\gamma_0 \oplus \gamma_1$, $\gamma_1 \oplus \gamma_2$, and $\gamma_0 \oplus \gamma_1 \oplus \gamma_2$ are all permutations of $\{0,1\}^n$, one has, for any permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$,
$$|\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| \leq \frac{3q_e q_p}{M},$$
$$|\mathsf{BadK}_{10}| \leq \frac{q_e^2}{M},$$
so that
$$\Pr\left[k \leftarrow_{\$} \{0,1\}^n : k \in \bigcup_{i=6}^{10} \mathsf{BadK}_i\right] \leq \frac{12q_e q_p}{NM} + \frac{q_e^2}{NM} \leq \frac{q_e + 12q_p}{N^{\frac{2}{3}}}.$$
On the other hand, in order to upper bound $|\mathsf{BadK}_i|$ for $i = 1$ to 5, we need to appeal to the sum-capture theorem of Section 3. For a permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$, let
$$X = \{x \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\}, \qquad Y = \{y \in \{0,1\}^n : (x, y) \in \mathcal{Q}_E\},$$
$$U = \{u \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\}, \qquad V = \{v \in \{0,1\}^n : (u, v) \in \mathcal{Q}_P\}$$
denote the domains and the ranges of $\mathcal{Q}_E$ and $\mathcal{Q}_P$, respectively. Then one has
$$|\mathsf{BadK}_1| \leq \mu(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} |\{((x, y), u, v) \in \mathcal{Q}_E \times U \times V : x \oplus u = \gamma_0 \circ \gamma_2^{-1}(y \oplus v)\}|$$
$$|\mathsf{BadK}_2| \leq \mu(\mathcal{Q}_P, X, U) \stackrel{\text{def}}{=} |\{((u, v), x, u') \in \mathcal{Q}_P \times X \times U : x \oplus u = \gamma_0 \circ \gamma_1^{-1}(v \oplus u')\}|$$
$$|\mathsf{BadK}_3| \leq \mu(\mathcal{Q}_P, V, Y) \stackrel{\text{def}}{=} |\{((u', v'), v, y) \in \mathcal{Q}_P \times V \times Y : v \oplus u' = \gamma_1 \circ \gamma_2^{-1}(v' \oplus y)\}|$$
$$|\mathsf{BadK}_4| \leq \mu(\mathcal{Q}_P, X, X) \stackrel{\text{def}}{=} |\{((u, v), x, x') \in \mathcal{Q}_P \times X \times X : x \oplus u = \gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}(v \oplus x')\}|$$
$$|\mathsf{BadK}_5| \leq \mu(\mathcal{Q}_P, Y, Y) \stackrel{\text{def}}{=} |\{((u, v), y, y') \in \mathcal{Q}_P \times Y \times Y : y' \oplus u = (\gamma_1 \oplus \gamma_2) \circ \gamma_2^{-1}(v \oplus y)\}|.$$
By our assumption that the key-schedule is good, we have that $\gamma_0 \circ \gamma_2^{-1}$, $\gamma_0 \circ \gamma_1^{-1}$, $\gamma_1 \circ \gamma_2^{-1}$, $\gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}$, and $\gamma_0 \circ (\gamma_0 \oplus \gamma_1)^{-1}$ are all automorphisms of $\mathbb{F}_2^n$. Hence, we can apply Theorem 1 (note that in order to apply this theorem to upper bound, say, $|\mathsf{BadK}_1|$, we consider

the combination of the distinguisher $\mathcal{D}$ and permutation P as a probabilistic adversary $\mathcal{A}$ interacting with permutation E, resulting in transcript $\mathcal{Q}_E$). Thus, if we set

$$C_1 = \frac{q_e q_p^2}{N} + \frac{2q_e^2 q_p}{N} + 3q_p\sqrt{nq_e}$$
$$C_2 = C_3 = \frac{q_e q_p^2}{N} + \frac{2q_p^2\sqrt{q_e q_p}}{N} + 3q_p\sqrt{nq_e}$$
$$C_4 = C_5 = \frac{q_e^2 q_p}{N} + \frac{2q_e q_p^2}{N} + 3q_e\sqrt{nq_p},$$

one has $\Pr[E, P \leftarrow_\$ \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] \leq 2/N$ for each $i = 1$ to 5. Since

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \sum_{i=1}^{5} \Pr[E, P \leftarrow_\$ \mathcal{P}_n : |\mathsf{BadK}_i| \geq C_i] + \frac{\sum_{i=1}^{5} C_i}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}},$$

we get the final result. □

Combining Lemmas 1, 10, and 12, we obtain the main theorem of this paper.

Theorem 5 (Single permutation and non-independent round keys). *Consider the single-permutation two-round Even-Mansour cipher* $\mathsf{EMSP}[n, 2, \boldsymbol{\gamma}]$ *with a good key-schedule* $\boldsymbol{\gamma}$ *(see Definition 3). Assume that* $N \geq 7^3$, $9n \leq q_e, q_p \leq N/2$, *and* $4q_e + 2q_p \leq N$. *Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,\boldsymbol{\gamma}]}(q_e, q_p) \leq \frac{10}{N} + \frac{4q_e^3 + 12q_e^2 q_p + 11q_e q_p^2 + 4q_p^2\sqrt{q_e q_p}}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{9q_p\sqrt{nq_e} + 6q_e\sqrt{nq_p}}{N} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}.$$

Letting $q = \max(q_e, q_p)$, and assuming $q \leq N^{\frac{2}{3}}$, the upper bound of Theorem 5 simplifies into

$$\frac{10}{N} + \frac{31q^3}{N^2} + \frac{2q^2}{N^{\frac{4}{3}}} + \frac{15\sqrt{n}q^{\frac{3}{2}}}{N} + \frac{33q}{N^{\frac{2}{3}}} \leq \frac{10}{N} + \frac{81\sqrt{n}q}{N^{\frac{2}{3}}} = \frac{10}{2^n} + \frac{81q}{2^{\frac{2n}{3} - \frac{1}{2}\log_2 n}}.$$

Hence, security is ensured up to $\mathcal{O}(2^{\frac{2n}{3} - \frac{1}{2}\log_2 n}) = \widetilde{\mathcal{O}}(2^{\frac{2n}{3}})$ queries of the adversary.

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 *Lecture Notes in Computer Science*, pages 531–550. Springer, 2013. Full version available at http://eprint.iacr.org/2013/061.

[AKKR08] Noga Alon, Tali Kaufman, Michael Krivelevich, and Dana Ron. Testing Triangle-Freeness in General Graphs. *SIAM J. Discrete Math.*, 22(2):786–819, 2008.

[Bab89] László Babai. The Fourier Transform and Equations over Finite Abelian Groups: An introduction to the method of trigonometric sums. Lecture notes, December 1989. Available at http://people.cs.uchicago.edu/~laci/reu02/fourier.pdf.

[BCD+13] Eli Biham, Yaniv Carmeli, Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. IACR Cryptology ePrint Archive, Report 2013/674, 2013. Available at http://eprint.iacr.org/2013/674.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J.B. Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[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 *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012.

[BW99] Alex Biryukov and David Wagner. Slide Attacks. In Lars R. Knudsen, editor, *Fast Software Encryption - FSE '99*, volume 1636 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 1999.

[BW00] Alex Biryukov and David Wagner. Advanced Slide Attacks. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 589–606. 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 *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.

[Dae91] Joan Daemen. Limitations of the Even-Mansour Construction. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 495–498. Springer, 1991.

[DDKS13] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES^2. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *Lecture Notes in Computer Science*, pages 337–356. Springer, 2013. Full version available at http://eprint.iacr.org/2013/391.

[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 *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[DR05] Joan Daemen and Vincent Rijmen. Probability Distributions of Correlations and Differentials in Block Ciphers. ePrint Archive, Report 2005/212, 2005. Available at http://eprint.iacr.org/2005/212.pdf.

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

[Gaz13] Peter Gazi. Plain versus Randomized Cascading-Based Key-Length Extension for Block Ciphers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *Lecture Notes in Computer Science*, pages 551–570. Springer, 2013.

[GGM99] Solomon W. Golomb, Guang Gong, and Lothrop Mittenthal. Constructions of Orthomorphisms of $\mathbb{Z}_n^2$. In Dieter Jungnickel and Harald Niederreiter, editors, *Proceedings of The Fifth International Conference on Finite Fields and Applications*, pages 178–195. Springer, 1999.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.

[GT12] Peter Gazi and Stefano Tessaro. Efficient and Optimally Secure Key-Length Extension for Block Ciphers via Randomized Cascading. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 63–80. Springer, 2012.

[Hay05] Thomas P. Hayes. A Large-Deviation Inequality for Vector-Valued Martingales. Manuscript, 2005. Available at http://www.cs.unm.edu/~hayes/papers/VectorAzuma.

[JV04] Pascal Junod and Serge Vaudenay. FOX : A New Family of Block Ciphers. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography - SAC 2004*, volume 3357 of *Lecture Notes in Computer Science*, pages 114–129. Springer, 2004.

[KPS13] Eike Kiltz, Krzysztof Pietrzak, and Mario Szegedy. Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 (Proceedings, Part I)*, volume 8042 of *Lecture Notes in Computer Science*, pages 571–588. Springer, 2013.

[KR01] Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001.

[Lee13] Jooyoung Lee. Towards Key-Length Extension with Optimal Security: Cascade Encryption and Xor-cascade Encryption. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 405–425. Springer, 2013.

[LM90] Xuejia Lai and James L. Massey. A Proposal for a New Block Encryption Standard. In Ivan Damgård, editor, *Advances in Cryptology - EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer, 1990.

[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 *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012.

[LS13] 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 *Lecture Notes in Computer Science*, pages 444–463. Springer, 2013. Full version available at http://eprint.iacr.org/2013/255.

[Mit95] Lothrop Mittenthal. Block Substitutions Using Orthomorphic Mappings. *Advances in Applied Mathematics*, 16(1):59–71, 1995.

[NWW13] Ivica Nikolica, Lei Wang, and Shuang Wu. Cryptanalysis of Round-Reduced LED. In *Fast Software Encryption - FSE 2013*, 2013. To appear.

[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 *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

[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.

[Ste13] John Steinberger. Counting solutions to additive equations in random sets. arXiv Report 1309.5582, 2013. Available at http://arxiv.org/abs/1309.5582.

[Vau99] Serge Vaudenay. On the Lai-Massey Scheme. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology - ASIACRYPT '99*, volume 1716 of *Lecture Notes in Computer Science*, pages 8–19. Springer, 1999.

A Probability of Bad Transcripts for Three Independent Round Keys

In this section, we upper bound tho probability to get a bad transcript for the single-permutation two-round Even-Mansour cipher in the case where the round keys (k_0, k_1, k_2) are independent, or in other words, $\ell = 3n$, $K = (k_0, k_1, k_2)$, and γ_i selects the i-th n-bit string of K. The analysis is greatly simplified since we do not need to appeal to the sum-capture theorem of Section 3.

Lemma 13. *Assume that the round keys (k_0, k_1, k_2) in the single-permutation two-round Even-Mansour cipher are uniformly random and independent. Then*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{2q_e^2 q_p + 3q_e q_p^2}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}.$$

Proof. Let $(\mathcal{Q}_E, \mathcal{Q}_P)$ be any attainable permutation transcript. Since in the ideal world, $K = (k_0, k_1, k_2)$ is independent from $\mathcal{Q}_E$ and $\mathcal{Q}_P$, we have:

$$\Pr[K = (k_0, k_1, k_2) \leftarrow_{\$} \{0,1\}^{3n} : K \in \mathsf{BadK}] \leq \frac{|\mathsf{BadK}|}{N^3}.$$

Note that, for any permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$, one has:

$$\begin{aligned} |\mathsf{BadK}_1|, |\mathsf{BadK}_2|, |\mathsf{BadK}_3| &\leq N q_e q_p^2, \\ |\mathsf{BadK}_4|, |\mathsf{BadK}_5| &\leq N q_e^2 q_p, \\ |\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| &\leq \frac{3N^2 q_e q_p}{M}, \\ |\mathsf{BadK}_{10}| &\leq \frac{N^2 q_e^2}{M}. \end{aligned}$$

The result follows using $M = q_e/N^{1/3}$. □

Combining Lemmas 1, 10, and 13, we obtain the following theorem, which implies that the two-round Even-Mansour cipher with a single permutation and independent round keys ensures security up to $\mathcal{O}(2^{2n/3})$ queries of the adversary.

Theorem 6 (Single permutation and independent round keys). *Let $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, where $\gamma_i : (k_0, k_1, k_2) \mapsto k_i$. Consider the two-round Even-Mansour cipher with a single permutation and independent round keys $\mathsf{EMSP}[n, 2, \ell = 3n, \boldsymbol{\gamma}]$. Assume that $N \geq 7^3$ and $4q_e + 2q_p \leq N$. Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,3n,\boldsymbol{\gamma}]} \leq \frac{4q_e^3 + 10q_e^2 q_p + 7q_e q_p^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}.$$

B Probability of Bad Transcripts for Two Alternated Independent Round Keys

We consider in this section the case where the master key K is $2n$-bit long, namely $K = (k, k')$, and the round key sequence is (k, k', k). This case is interesting since it is the two-round analogue of the "alternating" key-schedule of LED-128 [GPPR11] (which has twelve rounds), where the master key $K = (k, k')$ is twice as long as the block length, and round keys k and k' are alternatively xored to the state. This setting is intermediate between the case of perfectly independent round keys and the case of an n-bit master key (in particular, the sum-capture theorem is only required to upper bound $|\mathsf{BadK}_1|$).

Lemma 14. *Consider the single-permutation two-round Even-Mansour cipher with master key $K = (k, k')$ and round keys (k, k', k), k and k' being random and independent. Assume that $9n \leq q_e, q_p \leq N/2$. Then*

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \leq \frac{2}{N} + \frac{4q_e^2 q_p + 3q_e q_p^2}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}.$$

Proof. In the ideal world, sets BadK_i only depend on the random permutations E and P, and not on the key $K = (k, k')$, which is drawn uniformly at random at the end of the interaction of the distinguisher with (E, P). Moreover, the size of BadK_i for $i = 2$ to 10 can be upper bounded independently of E, P, namely for any permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$, one has:

$$|\mathsf{BadK}_2|, |\mathsf{BadK}_3| \leq q_e q_p^2,$$

$$|\mathsf{BadK}_4|, |\mathsf{BadK}_5| \le q_e^2 q_p,$$
$$|\mathsf{BadK}_6|, |\mathsf{BadK}_7|, |\mathsf{BadK}_8|, |\mathsf{BadK}_9| \le \frac{3Nq_eq_p}{M},$$
$$|\mathsf{BadK}_{10}| \le \frac{Nq_e^2}{M},$$

so that

$$\Pr\left[(k,k') \leftarrow_{\$} \{0,1\}^{2n} : (k,k') \in \bigcup_{i=2}^{10} \mathsf{BadK}_i\right] \le \frac{2q_eq_p^2 + 2q_e^2q_p}{N^2} + \frac{12q_eq_p}{NM} + \frac{q_e^2}{NM}$$
$$\le \frac{2q_eq_p^2 + 2q_e^2q_p}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}.$$

It remains to upper bound $|\mathsf{BadK}_1|$. For this, we need to appeal to the sum-capture theorem of Section 3. For a permutation transcript $(\mathcal{Q}_E, \mathcal{Q}_P)$, let

$$X = \{x \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\}, \qquad Y = \{y \in \{0,1\}^n : (x,y) \in \mathcal{Q}_E\},$$
$$U = \{u \in \{0,1\}^n : (u,v) \in \mathcal{Q}_P\}, \qquad V = \{v \in \{0,1\}^n : (u,v) \in \mathcal{Q}_P\}$$

denote the domains and the ranges of $\mathcal{Q}_E$ and $\mathcal{Q}_P$, respectively. Then one has

$$|\mathsf{BadK}_1| \le \mu(\mathcal{Q}_E, U, V) \stackrel{\text{def}}{=} |\{((x,y),u,v) \in \mathcal{Q}_E \times U \times V : x \oplus u = y \oplus v\}|.$$

Thus, if we set

$$C_1 = \frac{q_eq_p^2}{N} + \frac{2q_e^2q_p}{N} + 3q_p\sqrt{nq_e},$$

one has, by Theorem 1, $\Pr[E, P \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_1| \ge C_1] \le 2/N$. Hence, we obtain

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_2] \le \Pr[E, P \leftarrow_{\$} \mathcal{P}_n : |\mathsf{BadK}_1| \ge C_1] + \frac{C_1}{N}$$
$$+ \Pr\left[(k,k') \leftarrow_{\$} \{0,1\}^{2n} : (k,k') \in \bigcup_{i=2}^{10} \mathsf{BadK}_i\right]$$
$$\le \frac{2}{N} + \frac{q_eq_p^2}{N^2} + \frac{2q_e^2q_p}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{2q_eq_p^2 + 2q_e^2q_p}{N^2} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}$$
$$= \frac{2}{N} + \frac{4q_e^2q_p + 3q_eq_p^2}{N^2} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{q_e + 12q_p}{N^{\frac{2}{3}}}. \qquad \square$$

Combining Lemmas 1, 10, and 14, we obtain the following theorem, which implies that the two-round Even-Mansour cipher with a single permutation and two alternated independent round keys ensures security up to $\widetilde{\mathcal{O}}(2^{2n/3})$ queries of the adversary.

Theorem 7 (Single permutation and two alternated independent round keys). *Let $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$, where $\gamma_i : (k_0, k_1) \mapsto k_{i \bmod 2}$. Consider the two-round Even-Mansour cipher with a single permutation and two alternated independent round keys $\mathsf{EMSP}[n, 2, \ell = 2n, \boldsymbol{\gamma}]$. Assume that $N \ge 7^3$, $9n \le q_e, q_p \le N/2$, and $4q_e + 2q_p \le N$. Then*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathsf{EMSP}[n,2,2n,\boldsymbol{\gamma}]} \le \frac{2}{N} + \frac{4q_e^3 + 12q_e^2q_p + 7q_eq_p^2}{N^2} + \frac{2q_e^2}{N^{\frac{4}{3}}} + \frac{3q_p\sqrt{nq_e}}{N} + \frac{21q_e + 12q_p}{N^{\frac{2}{3}}}.$$