An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher

Rodolphe Lampe[1⋆], Jacques Patarin[1], and Yannick Seurin[2⋆⋆]

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

Abstract. We analyze the security of the iterated Even-Mansour cipher (*a.k.a.* key-alternating cipher), a very simple and natural construction of a blockcipher in the random permutation model. This construction, first considered by Even and Mansour (J. Cryptology, 1997) with a single permutation, was recently generalized to use t permutations in the work of Bogdanov *et al.* (EUROCRYPT 2012). They proved that the construction is secure up to $\mathcal{O}(N^{2/3})$ queries (where N is the domain size of the permutations), as soon as the number t of rounds is 2 or more. This is tight for $t = 2$, however in the general case the best known attack requires $\Omega(N^{t/(t+1)})$ queries. In this paper, we give asymptotically tight security proofs for two types of adversaries:

1. for non-adaptive chosen-plaintext adversaries, we prove that the construction achieves an optimal security bound of $\mathcal{O}(N^{t/(t+1)})$ queries;
2. for adaptive chosen-plaintext and ciphertext adversaries, we prove that the construction achieves security up to $\mathcal{O}(N^{t/(t+2)})$ queries (for t even). This improves previous results for $t \geq 6$.

Our proof crucially relies on the use of a *coupling* to upper-bound the statistical distance of the outputs of the iterated Even-Mansour cipher to the uniform distribution.

Keywords: blockcipher, Even-Mansour cipher, key-alternating cipher, random permutation model, coupling, provable security

1 Introduction

The Even-Mansour Cipher. Even and Mansour [9] proposed the following "minimal" construction of a blockcipher on message space $\{0,1\}^n$: given a public permutation P on $\{0,1\}^n$ (*e.g.* AES-128 with a fixed, publicly known key), encrypt x by computing $y = k_1 \oplus P(k_0 \oplus x)$, where k_0, k_1 are two n-bit keys. Their work was motivated by the DESX construction proposed by Rivest (1984, unpublished) and later formally analyzed by Kilian and Rogaway [13], in which

⋆ This author is partially supported by the French Department of Defense (DGA).
⋆⋆ This author is partially supported by the French National Agency of Research: ANR-11-INS-011.

Rivest suggested to strengthen DES against exhaustive key search by using two independent pre-whitening and post-whitening keys xored respectively to the input and the output of DES (thereby augmenting the key size of the resulting cipher from 56 to 184 bits). Even and Mansour analyzed their proposal in the random permutation model, where P is replaced by an oracle implementing a random (invertible) permutation, publicly accessible to all parties including the adversary. They showed that an adversary with black-box access to both P and the cipher with a random unknown key (as well as their inverse), has only a negligible probability to correctly inverse the cipher on an un-queried ciphertext of its choice (or to compute the ciphertext corresponding to some un-queried plaintext). In fact, the Even-Mansour cipher yields a (strong) pseudorandom permutation (in the random permutation model) in the sense that the system $(P, \mathtt{EM}_{P,(k_0,k_1)})$, where $\mathtt{EM}_{P,(k_0,k_1)}$ is the Even-Mansour cipher built from P with two uniformly random keys k_0 and k_1, is indistinguishable from an ideal system (P, Q), where Q is an independent random permutation. More precisely, any distinguisher has to make $\Omega(2^{n/2})$ queries to distinguish these two systems with non-negligible advantage.

The Iterated Even-Mansour Cipher. The Even-Mansour cipher was recently generalized in a very natural way by Bogdanov *et al.* [4] as follows: given t public permutations $P_1, \ldots, P_t$ on $\{0,1\}^n$, encrypt x by computing:

$$y = k_t \oplus P_t(k_{t-1} \oplus P_{t-1}(\cdots P_1(k_0 \oplus x)\cdots)) \ ,$$

where $k_0, \ldots, k_t$ are $t+1$ keys of n bits. They used the moniker (first coined in [7]) *key alternating cipher* for this construction, but we will prefer the name *iterated Even-Mansour cipher* in this paper to emphasize that we work in the random permutation model. We will refer to t as the number of *rounds* of the construction.

The main result of [4] is a proof (again, in the random permutation model for $P_1, \ldots P_t$) that the iterated Even-Mansour cipher with $t \geq 2$ rounds is secure (*i.e.*, indistinguishable from an independent random permutation) up to $\mathcal{O}(N^{2/3})$ queries (where $N = 2^n$). They also gave a distinguishing attack (in fact a key-recovery attack) requiring $\Omega(N^{t/(t+1)})$ queries. Hence, their analysis is tight for $t = 2$, but they left the security gap for $t > 2$ as an interesting open problem.

Our Contribution. In this work, we strengthen the security bounds of [4]. We obtain two distinct results depending on which type of adversaries we consider. For non-adaptive chosen-plaintext (NCPA for short) adversaries, we prove that the iterated Even-Mansour cipher with t rounds is secure up to $\mathcal{O}(N^{t/(t+1)})$ queries. Given that the attack described by [4] falls into this category of adversaries, this is tight up to constant factors. Tough this type of adversaries was not explicitly considered by [4], we note that this improves their general bound as soon as $t \geq 3$.

For adaptive chosen-plaintext and ciphertext (CCA for short) adversaries (*i.e.* the most powerful ones in terms of how queries may be issued to the system),

we prove that the iterated Even-Mansour cipher with t rounds is secure up to $\mathcal{O}(N^{t/(t+2)})$ queries when t is even. When t is odd, we get the same bound as for $t-1$ (since it is clear that adding a round to the construction cannot improve the advantage of a distinguisher). Our bound becomes better than $\mathcal{O}(N^{2/3})$, therefore improving [4]'s result, for $t \geq 6$. In particular, for $t = 6$, we obtain an improved security bound of $\mathcal{O}(N^{3/4})$ queries. Our findings are summarized in Table 1.

Our Techniques. Our proof strategy is very different and much simpler than the one of [4] (the counterpart of which is that for the interesting case of CCA adversaries, we improve their results only for t "large", where large means at least 6). One of the main ingredient of our proof is a well-known tool of the theory of Markov chains, namely the *coupling* technique. Indeed, a crucial step of our proof is to upper-bound, for any possible tuple of plaintext queries $(x^1, \ldots, x^{q_e})$ to the iterated Even-Mansour cipher, the statistical distance of the outputs of the cipher to the uniform distribution, conditioned on some partial information about the inner permutations $P_1, \ldots, P_t$ (namely equations of the form $P_i(a) = b$) that was gathered from the queries to these permutations. The outputs of permutations P_i, $i = 1, \ldots, t$, when computing the ciphertexts for inputs $(x^1, \ldots, x^{q_e})$, can be seen as the state of a Markov chain, so that we can reformulate the problem as studying how quick the distribution of this Markov chain converges to the uniform (as a function of the number of rounds). The coupling technique is one of the most efficient way to analyze this convergence rate (often named the *mixing time* of the Markov chain), and this is exactly the technique we adopt. Couplings were previously used in cryptography by Mironov [16] to analyze the RC4 stream cipher, and more recently by Morris *et al.* [17] to study maximally unbalanced Feistel networks and by Hoang and Rogaway [12] who generalized the results of [17] to many variants of the Feistel construction. In fact, our analysis was strongly inspired by the works of [17,12].

However, the coupling technique only enables to treat adversaries choosing their queries to the cipher non-adaptively. To leverage the result from NCPA-security to CCA-security, we use a composition strategy which is very similar to what is often referred to as the "two weak make one strong" technique [14,15]. For "classical" pseudorandom permutations (*i.e.* not build from ideal primitives as the Even-Mansour cipher), this strategy enables to prove the following: if $\{F_k\}$ and $\{G_{k'}\}$ are two permutation families secure against NCPA attacks (with upper-bounds resp. ε_F and ε_G on the advantage of any NCPA-distinguisher), then the composition $\{G_{k'}^{-1} \circ F_k\}$ is secure against CCA attacks (with advantage upper-bounded by $\varepsilon_F + \varepsilon_G$). This was proved by Maurer and Pietrzak [14] up to logarithmic factors and then refined by Maurer *et al.* [15], in the formalism of random systems. However, subtle complications appear when trying to use these results directly because of the additional inner permutation oracles $P_1, \ldots, P_t$, so that we prefer a more direct approach, very similar to the "H coefficients" technique of Patarin [18].

A caveat. We warn that the value of our results is similar to security proofs in the random oracle model [2], meaning that they offer no guarantee once the inner permutations are instantiated with real, standard permutations [5]. They show however that any attack beating our bounds cannot use the inner permutations as black-boxes.

t	NCPA	CCA	CCA ($n = 128$)
2	2/3	1/2	—
3	3/4	1/2	—
4	4/5	2/3	—
5	5/6	2/3	—
6	6/7	3/4	93
7	7/8	3/4	93
8	8/9	4/5	100

Table 1. Summary of our results. The NCPA (resp. CCA) column gives the constant c such that the iterated Even-Mansour cipher is secure up to N^c queries against NCPA-distinguishers (resp. CCA-distinguishers). Gray cells indicate when we improve the $N^{2/3}$ bound of [4]. The last column gives, for $n = 128$, the log in base 2 of the minimal number of queries a CCA-distinguisher has to make to have advantage at least 1/2 in distinguishing the cipher from random (we only give this number when our bound improves the one of [4]).

Related Work. We focus on security proofs in this work, but we stress that quite a few papers explored attacks (mainly key-recovery ones) against the Even-Mansour cipher. Daemen [6] gave a differential-style attack requiring q_p (direct) chosen queries to P and q_e chosen plaintext queries to the cipher, with $q_p q_e = \Omega(2^n)$ (hence the total query complexity is minimized for $q_p = q_e = \Omega(2^{n/2})$). Later, Biryukov and Wagner [3] gave an attack requiring $\Omega(2^{n/2})$ queries to both P and the cipher, but allowing to use known plaintexts rather than chosen ones. However, their method does not allow any trade-off between queries to P and the cipher as is possible in Daemen's attack. Recently, Dunkelman *et al.* [8] refined the work of [3] by giving a known-plaintext attack where such a trade-off is possible, thereby providing an optimal attack on the Even-Mansour cipher.

On the provable-security side, Gentry and Ramzan [10] showed that the Even-Mansour cipher remains secure when the random permutation oracle P is replaced by a Feistel construction with four rounds, where the round functions are public random function oracles.

Open Problems. Our work settles the case of non-adaptive chosen-plaintext adversaries; there remains however a gap for adaptive chosen-plaintext and ci-

phertext attacks between the proven bound of $\mathcal{O}(N^{t/(t+2)})$ queries and the best attack requiring $\Omega(N^{t/(t+1)})$ queries. The two practically appealing cases where all keys are identical (as was for example recently proposed in the blockcipher LED [11]), and where all inner permutations are identical, also remain interesting directions of research. It may even be possible that using both identical keys *and* a single inner permutation provides some level of security greater than $2^{n/2}$.[3]

Organization. In Section 2, we introduce the general notation, formally define the adversarial model, and give the necessary background on couplings. In Section 3, we prove our main result on the statistical distance of the outputs of the iterated Even-Mansour cipher to the uniform distribution using a coupling, which enables us to treat NCPA-adversaries. In Section 4, we deal with CCA-adversaries.

2 Preliminaries

2.1 General Notation

In all the following, we fix an integer $n \geq 1$. We denote $\mathcal{I}_n = \{0,1\}^n$ the set of binary strings of length n and $N = 2^n$. Given an integer $q \geq 1$, we denote $(\mathcal{I}_n)^{*q}$ the set of all sequences of pairwise distinct elements of $\mathcal{I}_n$ of length q. Given integers $q_1, \ldots, q_t$ we denote $(\mathcal{I}_n)^{*q_1,\ldots,q_t} = (\mathcal{I}_n)^{*q_1} \times \cdots \times (\mathcal{I}_n)^{*q_t}$. We denote $(N)_q = N(N-1)\cdots(N-q+1)$ the falling factorial. Note that $|(\mathcal{I}_n)^{*q}| = (N)_q$. We denote $[i;j]$ the set of integers k such that $i \leq k \leq j$.

The set of permutations on $\mathcal{I}_n$ will be denoted $\mathcal{P}_n$. Given $P \in \mathcal{P}_n$ and two sequences $x = (x^1, \ldots, x^q)$ and $y = (y^1, \ldots, y^q)$ of $(\mathcal{I}_n)^{*q}$, we will write $P(x) = y$ to mean that $P(x^i) = y^i$ for $i = 1, \ldots, q$. Given a tuple of permutations $\boldsymbol{P} = (P_1, \ldots, P_t) \in (\mathcal{P}_n)^t$ and two sequences $a = (a_1, \ldots, a_t)$ and $b = (b_1, \ldots, b_t)$ of $(\mathcal{I}_n)^{*q_1,\ldots,q_t}$, with $a_i = (a_i^1, \ldots, a_i^{q_i})$ and $b_i = (b_i^1, \ldots, b_i^{q_i})$, we will write $\boldsymbol{P}(a) = b$ to mean that $P_i(a_i) = b_i$ for $i = 1, \ldots, t$ (*i.e.* $P_i(a_i^j) = b_i^j$ for $j = 1, \ldots, q_i$).

Given a value $k \in \{0,1\}^n$, $\oplus_k$ denotes the mapping $x \mapsto x \oplus k$ from $\{0,1\}^n$ to itself. Fix an integer $t \geq 1$. Let $\boldsymbol{P} = (P_1, \ldots, P_t)$ be a tuple of permutations on $\{0,1\}^n$. Then the *iterated Even-Mansour cipher* associated with $\boldsymbol{P}$ is the cipher with message space $\{0,1\}^n$ and key space $(\{0,1\}^n)^{t+1}$ where the permutation associated with key $k = (k_0, \ldots, k_t)$ is defined as (see Fig. 1):

$$\mathtt{EM}_{\boldsymbol{P},k} = \oplus_{k_t} \circ P_t \circ \oplus_{k_{t-1}} \circ \cdots \circ \oplus_{k_1} \circ P_1 \circ \oplus_{k_0} \ .$$

We denote $\Omega_t = (\mathcal{P}_n)^t \times (\mathcal{I}_n)^{t+1}$. An element $(\boldsymbol{P}, k)$ of Ω_t names a tuple of permutations and a key for the resulting Even-Mansour cipher.

[3] Note however that, as observed by [4], using P and P^{-1} for the construction with $t = 2$ rounds causes the security to drop to $2^{n/2}$, even with three independent keys.

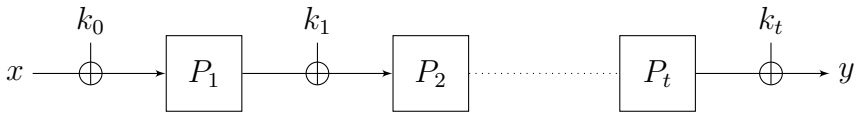

Fig. 1. The iterated Even-Mansour cipher.

2.2 Distinguishers

We consider distinguishers interacting with systems constituted of $t+1$ permutations. A query to such a system is a triplet (i, b, z) where $i \in [1; t+1]$ names which permutation is being queried, b is a bit indicating whether the query is forward or backward, and $z \in \{0,1\}^n$ is the actual query to the permutation. The goal of the distinguisher is to tell whether it is interacting with a tuple of $t+1$ uniformly random and independent (URI for short) permutations $(P_1, \ldots, P_t, Q)$, or with $(P_1, \ldots, P_t, \mathtt{EM}_{\boldsymbol{P},k})$ where $(P_1, \ldots, P_t)$ are URI and $\mathtt{EM}_{\boldsymbol{P},k}$ is the Even-Mansour cipher associated with $\boldsymbol{P} = (P_1, \ldots, P_t)$ with a uniformly random key $k = (k_0, \ldots, k_t)$. In the following we will refer to the first t permutations of the system as the *inner permutations*, by opposition to the last permutation of the system (which may be an independent random permutation Q or the Even-Mansour cipher $\mathtt{EM}_{\boldsymbol{P},k}$) to which we will refer to as the *outer permutation*. A $(q_1, \ldots, q_t, q_e)$-distinguisher is a distinguisher that makes at most q_i queries to inner permutation P_i for $i = 1, \ldots, t$ and q_e queries to the outer permutation. We will consider only computationally unbounded distinguishers. As usual we restrict ourself *wlog* to deterministic distinguishers that never make redundant queries and always make the maximal number of allowed queries to each permutation of the system.

The way we define chosen-plaintext/-ciphertext and adaptive/non-adaptive distinguishers is very specific to the context of our work. The qualifier chosen-plaintext/-ciphertext will only refer to the queries the distinguisher is allowed to make to the *outer permutation* of the system (it will always be allowed to make both forward and backward queries to the inner permutations). As well, adaptivity will only refer to how the distinguisher is allowed to choose its queries to the outer permutation (it will always be allowed to choose its queries to the inner permutations adaptively), and also to whether the distinguisher is allowed to query the inner permutations as a function of the answers received from the outer permutation. We now give a precise definition of the two types of distinguishers we consider: non-adaptive chosen-plaintext (NCPA) distinguishers and adaptive chosen-plaintext and ciphertext (CCA) distinguishers.

Definition 1. *A $(q_1, \ldots, q_t, q_e)$-NCPA-distinguisher runs in two phases:*

1. *in a first phase, it can only query the inner permutations $(P_1, \ldots, P_t)$. These queries can be adaptive, and both forward and backward queries are allowed. During this phase it makes exactly q_i queries to P_i for $i = 1, \ldots, t$;*

2. *in a second phase, it chooses a tuple of q_e non-adaptive*[4] *forward queries $x = (x^1, \ldots, x^{q_e})$ to the outer permutation of the system, and receives the corresponding answers.*

A $(q_1, \ldots, q_t, q_e)$-CCA-distinguisher is the most general one: it is allowed to make both forward and backward queries to all permutations of the system, in any order it wishes (in particular it may interleave queries to the outer permutation and to the inner permutations).

In all the following, the probability of an event E when $\mathcal{D}$ interacts with $t+1$ URI permutations $(P_1, \ldots, P_t, Q)$ will simply be denoted $\Pr^*[E]$, whereas the probability of an event E when $\mathcal{D}$ interacts with $(P_1, \ldots, P_t, \mathtt{EM}_{\boldsymbol{P},k})$, where $\boldsymbol{P} = (P_1, \ldots, P_t)$ are URI permutations and the key k is uniformly random, will simply be denoted $\Pr[E]$. With these notations, the advantage of a distinguisher $\mathcal{D}$ is defined as $|\Pr[\mathcal{D}(1^n) = 1] - \Pr^*[\mathcal{D}(1^n) = 1]|$ (we omit the oracles in this notation since they can be deduced from the notation $\Pr[\cdot]$ or $\Pr^*[\cdot]$). The maximum advantage of a $(q_1, \ldots, q_t, q_e)$-ATK-distinguisher against the iterated Even-Mansour cipher with t rounds (where ATK is NCPA or CCA) will be denoted $\mathbf{Adv}^{\mathrm{atk}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e)$. When considering distinguishers making at most q queries in total, we simply denote $\mathbf{Adv}^{\mathrm{atk}}_{\mathcal{EM}[t]}(q)$.

Remark 1. We warn that our NCPA-security notion should not be considered as interesting in itself, but rather as a preliminary step towards proving CCA-security. The reason why it is rather artificial is that once the distinguisher has received the answers to its queries to the outer permutation, it is not allowed to query the inner permutations any more. This is not satisfying since these permutations are public primitives, and hence adversaries should be allowed to query them in their entire discretion.

2.3 Total Variation Distance and Coupling

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

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

The following definitions can easily be seen equivalent:

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

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that for all $x \in \Omega$, $\sum_{y \in \Omega} \lambda(x, y) = \mu(x)$ and for all $y \in \Omega$, $\sum_{x \in \Omega} \lambda(x, y) = \nu(y)$. In other

[4] By non-adaptive we mean that all queries have to be chosen before receiving any corresponding answer from the outer permutation. However the choice of x may depend on the answers received from the inner permutations during the first phase.

words, λ is a joint distribution whose marginal distributions are resp. μ and ν. The fundamental result of the coupling technique is the following one. For completeness, we provide the proof in Appendix A.

Lemma 1 (Coupling Lemma). *Let μ and ν be probability distributions on a finite event space Ω, let λ be a coupling of μ and ν, and let $(X, Y) \sim \lambda$ (*i.e. *(X, Y) is a random variable sampled according to distribution λ). Then $\|\mu - \nu\| \leq \Pr[X \neq Y]$.*

For the analysis of CCA attacks, we will rely on the following observation.

Lemma 2. *Let Ω be some finite event space and ν be the uniform probability distribution on Ω. Let μ be a probability distribution on Ω such that $\|\mu - \nu\| \leq \varepsilon$. Then there is a set $S \subset \Omega$ such that:*

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

Proof. Define $S = \{x \in \Omega : \mu(x) \geq (1 - \sqrt{\varepsilon})\nu(x)\}$. We will show that $|S| \geq (1 - \sqrt{\varepsilon})|\Omega|$. Assume for contradiction that $|S| < (1 - \sqrt{\varepsilon})|\Omega|$, or equivalently $|\bar{S}| > \sqrt{\varepsilon}|\Omega|$, *i.e.* $\nu(\bar{S}) > \sqrt{\varepsilon}$. By definition, for any $x \in \bar{S}$, $\nu(x) - \mu(x) > \sqrt{\varepsilon}\nu(x)$. Consequently,

$$\nu(\bar{S}) - \mu(\bar{S}) > \sqrt{\varepsilon}\nu(\bar{S}) > (\sqrt{\varepsilon})^2 = \varepsilon \ ,$$

a contradiction with $\|\mu - \nu\| \leq \varepsilon$. □

3 Security Against Non-Adaptive Distinguishers

In this section, we start with dealing with NCPA-distinguishers. The crucial point will be to upper bound the statistical distance between the outputs of the iterated Even-Mansour cipher *conditioned on partial information on the inner permutations* (namely $\boldsymbol{P}(a) = b$ for some tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$) and the uniform distribution on $(\mathcal{I}_n)^{*q_e}$. We introduce the following important definitions and notations.

Definition 2. *Let $q_1, \ldots, q_t, q_e$ be positive integers. Fix tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x \in (\mathcal{I}_n)^{*q_e}$. We denote $\mu_x(\cdot|\boldsymbol{P}(a) = b)$ the distribution of $\mathtt{EM}_{\boldsymbol{P},k}(x)$ conditioned on the event $\boldsymbol{P}(a) = b$ (*i.e. *when the key $k = (k_0, \ldots, k_t)$ is uniformly random and the permutations $\boldsymbol{P} = (P_1, \ldots, P_t)$ are uniformly random among permutations satisfying $\boldsymbol{P}(a) = b$). We also denote $\mu^*_{q_e} = 1/(N)_{q_e}$ the uniform distribution on $(\mathcal{I}_n)^{*q_e}$.*

We have the following expression for $\mu_x(\cdot|\boldsymbol{P}(a) = b)$.

Lemma 3. *Let $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x \in (\mathcal{I}_n)^{*q_e}$. Then for any $y \in (\mathcal{I}_n)^{*q_e}$ one has:*

$$\mu_x(y|\boldsymbol{P}(a) = b) = \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y\}}{|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}} \ .$$

Proof. This follows easily from the observation that the number of $(\boldsymbol{P}, k) \in \Omega_t$ such that $\boldsymbol{P}(a) = b$ is $|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}$. □

The following lemma states that the advantage of a NCPA-distinguisher is upper-bounded by the total variation distance between $\mu_x(\cdot|\boldsymbol{P}(a) = b)$ and $\mu^*_{q_e}$. This is a classical result regarding the advantage of the best NCPA-distinguisher for a pseudorandom permutation, however we need to adapt it here to fit the random permutation model.

Lemma 4. *Let $q_1, \ldots, q_t, q_e$ be positive integers. Assume that there exists α such that for any tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x \in (\mathcal{I}_n)^{*q_e}$, one has*

$$\|\mu_x(\cdot|\boldsymbol{P}(a) = b) - \mu^*_{q_e}\| \leq \alpha \ .$$

Then $\mathbf{Adv}^{\mathrm{ncpa}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq \alpha$.

Proof. Fix a $(q_1, \ldots, q_t, q_e)$-NCPA-distinguisher $\mathcal{D}$. Such a distinguisher first queries the inner permutations $(P_1, \ldots, P_t)$. Let τ be the resulting transcript, *i.e.* the ordered sequence of $q_1 + \ldots + q_t$ queries with the corresponding answer (i, b, z, z'), where $i \in [1; t]$ names which permutation is being queried, b is a bit indicating whether the query is forward or backward, $z \in \{0,1\}^n$ is the actual query and z' the answer. Let also Φ be the function that maps a tuple of permutations $\boldsymbol{P} = (P_1, \ldots, P_t)$ to the transcript of the first phase of the attack when $\mathcal{D}$ interacts with $(P_1, \ldots, P_t, *)$, where $*$ is either an independent random permutation Q or $\mathtt{EM}_{\boldsymbol{P},k}$ (this is clearly irrelevant since $\mathcal{D}$ does not query the outer permutation during the first phase of the attack). We say that a transcript τ is *consistent* if there exists a tuple of permutations $\boldsymbol{P}$ such that $\Phi(\boldsymbol{P}) = \tau$, and we denote Γ the set of consistent transcripts. Finally, from a consistent transcript τ, we build the sequences $a(\tau), b(\tau) \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ as follows: let (i, b, z, z') be the j-th query and corresponding answer to P_i in the transcript. If this is a forward query ($b = 0$), then we define $a_i^j = z$ and $b_i^j = z'$; else, when this is a backward query ($b = 1$), we define $a_i^j = z'$ and $b_i^j = z$. Note that for a consistent transcript τ, $\Phi(\boldsymbol{P}) = \tau$ iff $\boldsymbol{P}(a(\tau)) = b(\tau)$. The number of consistent transcripts can be exactly determined:

$$|\Gamma| = \prod_{i=1}^{t} (N)_{q_i} \ . \tag{1}$$

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

The tuple of non-adaptive plaintext queries $x = (x^1, \ldots, x^{q_e}) \in (\mathcal{I}_n)^{*q_e}$ of $\mathcal{D}$ to the outer permutation is a deterministic function of the transcript τ of the first phase of the attack. Let Ψ denote the function which maps a consistent transcript τ to the corresponding tuple of queries. The output of $\mathcal{D}$ is then a

deterministic function of τ and the answers $y = (y^1, \ldots, y^{q_e})$ received from the outer permutation to the tuple of queries $\Psi(\tau)$. For any consistent transcript τ, we denote Σ_τ the set of tuples y such that $\mathcal{D}$ outputs 1 when receiving answers y to the queries $\Psi(\tau)$. Then, by definition we have:

$$\begin{aligned}\Pr^*[\mathcal{D}(1^n) = 1] &= \sum_{\tau \in \Gamma} \sum_{y \in \Sigma_\tau} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \Phi(\boldsymbol{P}) = \tau \wedge Q(\Psi(\tau)) = y\}}{|\mathcal{P}_n|^{t+1}} \\ &= \sum_{\tau \in \Gamma} \sum_{y \in \Sigma_\tau} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \boldsymbol{P}(a(\tau)) = b(\tau) \wedge Q(\Psi(\tau)) = y\}}{|\mathcal{P}_n|^{t+1}} \\ &= \sum_{\tau \in \Gamma} \sum_{y \in \Sigma_\tau} \frac{1}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \quad . \end{aligned} \tag{2}$$

Also, we have:

$$\Pr[\mathcal{D}(1^n) = 1] = \sum_{\tau \in \Gamma} \sum_{y \in \Sigma_\tau} \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \Phi(\boldsymbol{P}) = \tau \wedge \mathtt{EM}_{\boldsymbol{P},k}(\Psi(\tau)) = y\}}{|\Omega_t|} \quad . \tag{3}$$

We now use the assumption that, for all tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x \in (\mathcal{I}_n)^{*q_e}$, one has $\|\mu_x(\cdot|\boldsymbol{P}(a) = b) - \mu^*_{q_e}\| \leq \alpha$. By Lemma 3, this exactly means that for all tuples a, b, x and any subset $S \subset (\mathcal{I}_n)^{*q_e}$, one has:

$$\left| \sum_{y \in S} \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y\}}{|\Omega_t| / \prod_{i=1}^{t} (N)_{q_i}} - \sum_{y \in S} \frac{1}{(N)_{q_e}} \right| \leq \alpha \quad .$$

For any $\tau \in \Gamma$ we can apply the above inequality with $(a, b) = (a(\tau), b(\tau))$, $x = \Psi(\tau)$, and $S = \Sigma_\tau$ to get:

$$\left| \sum_{y \in \Sigma_\tau} \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \boldsymbol{P}(a(\tau)) = b(\tau) \wedge \mathtt{EM}_{\boldsymbol{P},k}(\Psi(\tau)) = y\}}{|\Omega_t|} - \sum_{y \in \Sigma_\tau} \frac{1}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \right| \leq \frac{\alpha}{\prod_{i=1}^{t} (N)_{q_i}} \quad . \tag{4}$$

Combining Eqs. (2-3-4), and using that for a consistent transcript τ, $\Phi(\boldsymbol{P}) = \tau$ iff $\boldsymbol{P}(a(\tau)) = b(\tau)$, we obtain:

$$|\Pr[\mathcal{D}(1^n) = 1] - \Pr^*[\mathcal{D}(1^n) = 1]| \leq \sum_{\tau \in \Gamma} \frac{\alpha}{\prod_{i=1}^{t} (N)_{q_i}} \quad .$$

Finally, we deduce using Eq. (1) that the advantage of $\mathcal{D}$ is less than α, which concludes the proof. □

The rest of this section is devoted to establishing an appropriate upper bound α for $\|\mu_x(\cdot|\boldsymbol{P}(a)=b)-\mu^*_{q_e}\|$ as required to apply Lemma 4. The following lemma can be regarded as the main contribution of this work.

Lemma 5. *Let $q_1,\ldots,q_t,q_e$ be positive integers. Fix tuples $a,b\in(\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x\in(\mathcal{I}_n)^{*q_e}$. Then:*

$$\|\mu_x(\cdot|\boldsymbol{P}(a)=b)-\mu^*_{q_e}\|\leq 2^t\frac{q_e\prod_{i=1}^t q_i}{N^t}\ .$$

Proof. Fix tuples $a,b\in(\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x\in(\mathcal{I}_n)^{*q_e}$, with $x=(x^1,\ldots,x^{q_e})$. For each $\ell\in[0;q_e]$, let $(z^1,\ldots,z^{q_e})$ be a tuple of queries such that $z^i=x^i$ for $i\leq\ell$, and z^i is uniformly random in $\{0,1\}^n\setminus\{z^1,\ldots,z^{i-1}\}$ for $i>\ell$. Denote ν_ℓ the distribution of the tuple of q_e outputs when $\mathtt{EM}_{\boldsymbol{P},k}$ receives inputs $(z^1,\ldots,z^{q_e})$, conditioned on $\boldsymbol{P}(a)=b$. Note that $\nu_0=\mu^*_{q_e}$ since for $\ell=0$ the tuple of inputs is uniformly random in $(\mathcal{I}_n)^{*q_e}$, and $\nu_{q_e}=\mu_x(\cdot|\boldsymbol{P}(a)=b)$. Hence we have:

$$\|\mu_x(\cdot|\boldsymbol{P}(a)=b)-\mu^*_{q_e}\|=\|\nu_{q_e}-\nu_0\|\leq\sum_{l=0}^{q_e-1}\|\nu_{\ell+1}-\nu_\ell\|\ . \tag{5}$$

It remains to upper bound the total variation distance between $\nu_{\ell+1}$ and ν_ℓ, for each $\ell\in[0;q_e-1]$. For this, we will construct a suitable coupling of the two distributions. Note that we only have to consider the first $\ell+1$ elements of the two tuples of outputs since for both distributions, the i-th inputs for $i>\ell+1$ are sampled at random. In other words, $\|\nu_{\ell+1}-\nu_\ell\|=\|\nu'_{\ell+1}-\nu'_\ell\|$, where $\nu'_{\ell+1}$ and ν'_ℓ are the respective distributions of the $\ell+1$ first outputs of the cipher. To define the coupling of $\nu'_{\ell+1}$ and ν'_ℓ, we consider the iterated Even-Mansour cipher $\mathtt{EM}_{\boldsymbol{P},k}$, where $\boldsymbol{P}$ satisfies $\boldsymbol{P}(a)=b$, that receives inputs $x'=(x^1,\ldots,x^{\ell+1})$, so that $\mathtt{EM}_{\boldsymbol{P},k}(x')$ is distributed according to $\nu'_{\ell+1}$. We will construct a second Even-Mansour cipher $\mathtt{EM}_{\boldsymbol{P}',k'}$, with inputs $u=(u^1,\ldots,u^{\ell+1})$, satisfying the following properties:

1) $u^i=x^i$ for $i=1,\ldots,\ell$, and $u^{\ell+1}$ is uniformly random in $\{0,1\}^n\setminus\{u^1,\ldots,u^\ell\}$;
2) for $i=1,\ldots,\ell+1$, if the outputs of the j-th inner permutation in the computations of $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$ and $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$ are equal, then this also holds for any subsequent inner permutation;
3) $\boldsymbol{P}'$ is uniformly random among permutation tuples satisfying $\boldsymbol{P}'(a)=b$ and k' is uniformly random in $(\mathcal{I}_n)^{t+1}$.

Note that properties 1) and 3) will ensure that $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$ is distributed according to ν'_ℓ. We warn that $(\boldsymbol{P}',k')$ will not be *independent* from $(\boldsymbol{P},k)$, however this is not required for the Coupling Lemma to apply. The only requirement is that both $(\boldsymbol{P},k)$ and $(\boldsymbol{P}',k')$ have the correct marginal distribution.

We now describe how the second iterated Even-Mansour cipher is constructed. First, it uses exactly the same keys as the original one, namely $k'=(k_0,\ldots,k_t)$. In order to construct permutations $\boldsymbol{P}'$ (on points encountered when computing $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$), we compare the computations of $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$ and $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$ for

$i = 1, \ldots, \ell+1$. For $j = 1, \ldots, t$, we define x_j^i as the output of P_j when computing $\mathtt{EM}_{\boldsymbol{P},k}(x^i)$, and similarly u_j^i as the output of P'_j when computing $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i)$, *i.e.*

$$x_j^i = P_j(k_{j-1} \oplus P_{j-1}(\cdots P_1(x^i \oplus k_0)\cdots))$$
$$\text{and } u_j^i = P'_j(k_{j-1} \oplus P'_{j-1}(\cdots P'_1(u^i \oplus k_0)\cdots)) \ .$$

We also let $x_0^i = x^i$ and $u_0^i = u^i$. For $j = 0, \ldots, t-1$ we use the following rules:

i) if $u_j^i \oplus k_j \in a_{j+1}$, then $u_{j+1}^i = P'_{j+1}(u_j^i \oplus k_j)$ is determined by the constraint $\boldsymbol{P}'(a) = b$;
ii) if $u_j^i \oplus k_j \notin a_{j+1}$ and $x_j^i \oplus k_j \in a_{j+1}$, then we choose $u_{j+1}^i = P'_{j+1}(u_j^i \oplus k_j)$ uniformly at random in $\{0,1\}^n \setminus (b_{j+1} \cup \{u_{j+1}^1, \ldots, u_{j+1}^{i-1}\})$;
iii) if $u_j^i \oplus k_j \notin a_{j+1}$ and $x_j^i \oplus k_j \notin a_{j+1}$, then we define $u_{j+1}^i = x_{j+1}^i$, that is $P'_{j+1}(u_j^i \oplus k_j) = P_{j+1}(x_j^i \oplus k_j)$.

Property 2) can easily be seen to follow from these rules and the fact that the keys are the same in both ciphers. Since $\boldsymbol{P}$ is uniformly random among permutation tuples satisfying $\boldsymbol{P}(a) = b$, so is $\boldsymbol{P}'$. This follows from the fact that when using rule iii), $x_j^i \oplus k_j \notin a_{j+1}$ implies that x_{j+1}^i is uniformly random in $\{0,1\}^n \setminus (b_{j+1} \cup \{x_{j+1}^1, \ldots, x_{j+1}^{i-1}\})$, and hence u_{j+1}^i is uniformly random in $\{0,1\}^n \setminus (b_{j+1} \cup \{u_{j+1}^1, \ldots, u_{j+1}^{i-1}\})$ as well. This justifies Property 3). Hence, the joint distribution probability we created for the random variable $(\mathtt{EM}_{\boldsymbol{P},k}(x'), \mathtt{EM}_{\boldsymbol{P}',k'}(u))$ is such that the marginal distributions of $\mathtt{EM}_{\boldsymbol{P},k}(x')$ and $\mathtt{EM}_{\boldsymbol{P}',k'}(u)$ are respectively $\nu'_{\ell+1}$ and ν'_ℓ. We can now apply Lemma 1 to obtain:

$$\|\nu_{\ell+1} - \nu_\ell\| = \|\nu'_{\ell+1} - \nu'_\ell\| \leq \Pr\left[(x_t^1, \ldots, x_t^{\ell+1}) \neq (u_t^1, \ldots, u_t^{\ell+1})\right]$$

where we used $\mathtt{EM}_{\boldsymbol{P},k}(x^i) = x_t^i \oplus k_{t+1}$ and $\mathtt{EM}_{\boldsymbol{P}',k'}(u^i) = u_t^i \oplus k_{t+1}$. Clearly, the rules (combined with the fact that $u^i = x^i$ for $i = 1, \ldots, \ell$) imply that $u_j^i = x_j^i$ for $i = 1, \ldots, \ell$ and $j = 0, \ldots, t$, so that the above expression simplifies to $\|\nu_{\ell+1} - \nu_\ell\| \leq \Pr[x_t^{\ell+1} \neq u_t^{\ell+1}]$. Hence, we are left with the task of upper-bounding the probability not to equate $x_j^{\ell+1}$ and $u_j^{\ell+1}$ in any of the t rounds.

Consider the first round. Unless we have $u_0^{\ell+1} \oplus k_0 \in a_1$ or $x_0^{\ell+1} \oplus k_0 \in a_1$, we will use rule iii) so that we will have $u_1^{\ell+1} = x_1^{\ell+1}$. Since the size of a_1 is q_1, and k_0 is uniformly random, we see that $\Pr[x_1^{\ell+1} \neq u_1^{\ell+1}] \leq 2q_1/N$. Assume now that $x_j^{\ell+1} \neq u_j^{\ell+1}$ for some $j \in [1; t-1]$. As in the preceding case, unless $u_j^{\ell+1} \oplus k_j \in a_{j+1}$ or $x_j^{\ell+1} \oplus k_j \in a_{j+1}$, we will have $u_{j+1}^{\ell+1} = x_{j+1}^{\ell+1}$, so that $\Pr[x_{j+1}^{\ell+1} \neq u_{j+1}^{\ell+1} | x_j^{\ell+1} \neq u_j^{\ell+1}] \leq 2q_{j+1}/N$. Using a chain of conditional probabilities, we get:

$$\|\nu_{\ell+1} - \nu_\ell\| \leq \Pr[x_t^{\ell+1} \neq u_t^{\ell+1}] \leq \frac{2q_1}{N} \cdot \frac{2q_2}{N} \cdots \frac{2q_t}{N} = 2^t \frac{\prod_{i=1}^t q_i}{N^t} \ .$$

Finally, using Eq. (5), we see that

$$\|\mu_x(\cdot | \boldsymbol{P}(a) = b) - \mu^*_{q_e}\| = \|\nu_{q_e} - \nu_0\| \leq 2^t \frac{q_e \prod_{i=1}^t q_i}{N^t} \ ,$$

as claimed. □

Remark 2. It can easily be checked that the final key k_t does not play any role in the proof of Lemma 5. Hence it also holds for iterated Even-Mansour cipher without the last key.

Remark 3. The proof of Lemma 5 can be straightforwardly extended to handle distinguishers that are allowed to make both forward *and* backward queries to the outer permutation, in a non-adaptive way (such adversaries could be named NCCA). However, notations become quite cumbersome, so that we omit the details.

Combining Lemmata 4 and 5, we obtain the following theorem.

Theorem 1. *Let $q_1, \ldots, q_t, q_e$ be positive integers. Then:*

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq 2^t \frac{q_e \prod_{i=1}^{t} q_i}{N^t} \quad .$$

In particular, for any positive integer q:

$$\mathbf{Adv}^{\mathrm{ncpa}}_{\mathcal{EM}[t]}(q) \leq 2^t \frac{q^{t+1}}{N^t} \quad .$$

This remains true for the iterated Even-Mansour cipher where the last key k_t is omitted.

More concretely, the iterated Even-Mansour cipher with t rounds achieves NCPA-security up to $N^{\frac{t}{t+1}}$ queries. This is optimal (neglecting constant factors) considering the attack described in [4].

4 From Non-Adaptive to Adaptive Distinguishers

In this section, we turn to the case of CCA-distinguishers. For this, we will need the following refinement to Lemma 4, which relies on a stronger assumption on the distribution of the outputs of the iterated Even-Mansour cipher.

Lemma 6. *Let $q_1, \ldots, q_t, q_e$ be positive integers. Assume that there exists β such that for any tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x, y \in (\mathcal{I}_n)^{*q_e}$, one has*

$$\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y] \geq \frac{1-\beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \quad .$$

Then $\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q_1, \ldots, q_t, q_e) \leq \beta$.

Proof. The proof is very similar to the one of Lemma 4. Fix a $(q_1, \ldots, q_t, q_e)$-CCA-distinguisher $\mathcal{D}$. Let τ be the transcript of the interaction of $\mathcal{D}$ with the system of $t+1$ permutations, *i.e.* the ordered sequence of $q_1 + \ldots + q_t + q_e$ queries with the corresponding answer (i, b, z, z'), where $i \in [1; t+1]$ names which permutation is being queried, b is a bit indicating whether the query is forward or backward, $z \in \{0,1\}^n$ is the actual query and z' the answer. Let

also Φ be the function that maps a tuple of permutations $(\boldsymbol{P}, P_{t+1}) \in (\mathcal{P}_n)^{t+1}$ to the transcript of the attack when $\mathcal{D}$ interacts with $(\boldsymbol{P}, P_{t+1})$. We say that a transcript is *consistent* if there exists a tuple of permutations $(\boldsymbol{P}, P_{t+1})$ such that $\Phi(\boldsymbol{P}, P_{t+1}) = \tau$, and we denote Γ the set of consistent transcripts. Finally, from a consistent transcript τ, we build the sequences $a(\tau), b(\tau) \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x(\tau), y(\tau) \in (\mathcal{I}_n)^{*q_e}$ as follows. For $i = 1, \ldots, t$, let (i, b, z, z') be the j-th query and corresponding answer to P_i in the transcript. If this is a forward query ($b = 0$), then we define $a_i^j = z$ and $b_i^j = z'$; else, when this is a backward query ($b = 1$), we define $a_i^j = z'$ and $b_i^j = z$. Similarly, let $(t+1, b, z, z')$ be the j-th query and corresponding answer to the outer permutation P_{t+1} in the transcript. If this is a forward query ($b = 0$), then we define $x^j = z$ and $y^j = z'$; else, when this is a backward query ($b = 1$), we define $x^j = z'$ and $y^j = z$. Note that for a consistent transcript τ, $\Phi(\boldsymbol{P}, P_{t+1}) = \tau$ iff $\boldsymbol{P}(a(\tau)) = b(\tau)$ and $P_{t+1}(x(\tau)) = y(\tau)$.

The output of $\mathcal{D}$ is a deterministic function of the transcript. We let Σ denote the set of consistent transcripts τ such that $\mathcal{D}$ outputs 1 when the transcript is τ. Then, by definition we have:

$$\begin{aligned}
\Pr^*[\mathcal{D}(1^n) = 1] &= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \Phi(\boldsymbol{P}, Q) = \tau\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, Q) \in (\mathcal{P}_n)^{t+1} : \boldsymbol{P}(a(\tau)) = b(\tau) \wedge Q(x(\tau)) = y(\tau)\}}{|\mathcal{P}_n|^{t+1}} \\
&= \sum_{\tau \in \Sigma} \frac{1}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \quad . \qquad (6)
\end{aligned}$$

Also, we have:

$$\begin{aligned}
\Pr[\mathcal{D}(1^n) = 1] &= \sum_{\tau \in \Sigma} \frac{\#\{(\boldsymbol{P}, k) \in \Omega_t : \Phi(\boldsymbol{P}, \mathtt{EM}_{\boldsymbol{P},k}) = \tau\}}{|\Omega_t|} \\
&= \sum_{\tau \in \Sigma} \Pr\left[\boldsymbol{P}(a(\tau) = b(\tau) \wedge \mathtt{EM}_{\boldsymbol{P},k}(x(\tau)) = y(\tau)\right] \quad . \qquad (7)
\end{aligned}$$

Using the assumption and Eq. (6), we see that:

$$\Pr[\mathcal{D}(1^n) = 1] \geq \sum_{\tau \in \Sigma} \frac{1 - \beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} = (1 - \beta) \Pr^*[\mathcal{D}(1^n) = 1] \quad ,$$

so that $\Pr^*[\mathcal{D}(1^n) = 1] - \Pr[\mathcal{D}(1^n) = 1] \leq \beta$. Applying the same reasoning to the distinguisher $\mathcal{D}'$ which outputs the negation of $\mathcal{D}$'s output, we obtain

$$(1 - \Pr^*[\mathcal{D}(1^n) = 1]) - (1 - \Pr[\mathcal{D}(1^n) = 1]) \leq \beta \quad ,$$

which implies that the advantage of $\mathcal{D}$ is at most β. This concludes the proof. □

We will now derive an appropriate bound β refining Lemma 5 by doubling the number of rounds of the construction and using Lemma 2.

Lemma 7. *Let t be an even integer and $t' = t/2$. Let $q_1, \ldots, q_t, q_e$ be positive integers. We denote:*

$$\alpha_1 = 2^{t'} \frac{q_e \prod_{i=1}^{t'} q_i}{N^{t'}} \quad \text{and} \quad \alpha_2 = 2^{t'} \frac{q_e \prod_{i=t'+1}^{t} q_i}{N^{t'}} \ .$$

Then for any tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x, y \in (\mathcal{I}_n)^{*q_e}$, one has

$$\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y] \geq \frac{1-\beta}{(N)_{q_e} \prod_{i=1}^{t} (N)_{q_i}} \ ,$$

where $\beta = 2(\sqrt{\alpha_1} + \sqrt{\alpha_2})$.

Proof. First, we slightly modify how the Even-Mansour cipher with $2t'$ rounds is defined in order to write it as the composition of two Even-Mansour ciphers with t' rounds. For this, we write the middle key $k_{t'}$ between permutations $P_{t'}$ and $P_{t'+1}$ as the xor of two independent keys $k^1_{t'}$ and $k^2_{t'}$, and we redefine $\mathtt{EM}_{\boldsymbol{P},k}$ where $\boldsymbol{P} = (P_1, \ldots, P_{2t'}) \in (\mathcal{P}_n)^{2t'}$ and $k = (k_0, \ldots, k_{t'-1}, k^1_{t'}, k^2_{t'}, k_{t'+1}, \ldots, k_{2t'}) \in (\mathcal{I}_n)^{2t'+2}$, as:

$$\mathtt{EM}_{\boldsymbol{P},k} = \underbrace{\oplus_{k_{2t'}} \circ P_{2t'} \circ \oplus_{k_{2t'-1}} \circ \cdots \circ P_{t'+1} \circ \oplus_{k^2_{t'}}}_{\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}} \circ \underbrace{\oplus_{k^1_{t'}} \circ P_{t'} \circ \cdots \circ \oplus_{k_1} \circ P_1 \circ \oplus_{k_0}}_{\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}} \ .$$

Clearly, this does not change the quantity $\Pr[\boldsymbol{P}(a) = b \wedge \mathtt{EM}_{\boldsymbol{P},k}(x) = y]$ since $k^1_{t'} \oplus k^2_{t'}$ is uniformly distributed when $k^1_{t'}$ and $k^2_{t'}$ are. This enables to write $\mathtt{EM}_{\boldsymbol{P},k} = \mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2} \circ \mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}$, where $\boldsymbol{P}_1 = (P_1, \ldots, P_{t'})$, $\boldsymbol{P}_2 = (P_{t'+1}, \ldots, P_{2t'})$, $\tilde{k}_1 = (k_0, \ldots, k_{t'-1}, k^1_{t'})$, $\tilde{k}_2 = (k^2_{t'}, k_{t'+1}, \ldots, k_{2t'})$. In the following we denote $\widetilde{\Omega}_{2t'} = (\mathcal{P}_n)^{2t'} \times (\mathcal{I}_n)^{2t'+2}$. Note that $|\widetilde{\Omega}_{2t'}| = |\Omega_{t'}|^2$.

Fix tuples $a, b \in (\mathcal{I}_n)^{*q_1,\ldots,q_t}$ and $x, y \in (\mathcal{I}_n)^{*q_e}$. We denote $\tilde{a}_1 = (a_1, \ldots, a_{t'})$, $\tilde{a}_2 = (a_{t'+1}, \ldots, a_{2t'})$, $\tilde{b}_1 = (b_1, \ldots, b_{t'})$, and $\tilde{b}_2 = (b_{t'+1}, \ldots, b_{2t'})$. We will apply Lemma 2 independently to each half of the cipher $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}$ and $\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}$. Consider the first half $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}$. By Lemma 5, we have $\|\mu^1_x(\cdot|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1) - \mu^*_{q_e}\| \leq \alpha_1$, where $\mu^1_x(\cdot|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1)$ is the distribution of $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x)$ conditioned on $\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1$. Hence Lemma 2 ensures that there is a subset $S_x \subset (\mathcal{I}_n)^{*q_e}$ of size at least $(1 - \sqrt{\alpha_1})(N)_{q_e}$ such that for all $z \in S_x$:

$$\begin{aligned} \mu^1_x(z|\boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1) &= \frac{\#\{(\boldsymbol{P}_1, \tilde{k}_1) \in \Omega_{t'} : \boldsymbol{P}_1(\tilde{a}_1) = \tilde{b}_1 \wedge \mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x) = z\}}{|\Omega_{t'}| / \prod_{i=1}^{t'} (N)_{q_i}} \\ &\geq (1 - \sqrt{\alpha_1}) \frac{1}{(N)_{q_e}} \ . \end{aligned}$$

Applying a similar reasoning to the distribution $\mu^2_y(\cdot|\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2)$ of $\mathtt{EM}^{-1}_{\boldsymbol{P}_2,\tilde{k}_2}(y)$ conditioned on $\boldsymbol{P}_2(\tilde{a}_2) = \tilde{b}_2$, we see that there exits a subset $S_y \subset (\mathcal{I}_n)^{*q_e}$ of size

at least $(1-\sqrt{\alpha_2})(N)_{q_e}$ such that for all $z \in S_y$:

$$\mu_y^2(z|\boldsymbol{P}_2(\tilde{a}_2)=\tilde{b}_2) = \frac{\#\{(\boldsymbol{P}_2,\tilde{k}_2)\in\Omega_{t'} : \boldsymbol{P}_2(\tilde{a}_2)=\tilde{b}_2 \wedge \mathtt{EM}^{-1}_{\boldsymbol{P}_2,\tilde{k}_2}(y)=z\}}{|\Omega_{t'}|/\prod_{i=t'+1}^{t}(N)_{q_i}} \\ \geq (1-\sqrt{\alpha_2})\frac{1}{(N)_{q_e}} \ .$$

We can now lower-bound the number of $(\boldsymbol{P},k)\in\widetilde{\Omega}_{2t'}$ satisfying $\boldsymbol{P}(a)=b$ and $\mathtt{EM}_{\boldsymbol{P},k}(x)=y$ by summing, over all intermediate values $z\in S_x\cap S_y$, the product of the number of $(\boldsymbol{P}_1,\tilde{k}_1)\in\Omega_{t'}$ satisfying $\boldsymbol{P}_1(\tilde{a}_1)=\tilde{b}_1$ and $\mathtt{EM}_{\boldsymbol{P}_1,\tilde{k}_1}(x)=z$ times the number of $(\boldsymbol{P}_2,\tilde{k}_2)\in\Omega_{t'}$ satisfying $\boldsymbol{P}_2(\tilde{a}_2)=\tilde{b}_2$ and $\mathtt{EM}_{\boldsymbol{P}_2,\tilde{k}_2}(z)=y$. Combining the two above equations yields:

$$\#\{(\boldsymbol{P},k)\in\widetilde{\Omega}_{2t'} : \boldsymbol{P}(a)=b\wedge\mathtt{EM}_{\boldsymbol{P},k}(x)=y\} \geq \\ \frac{|S_x\cap S_y|(1-\sqrt{\alpha_1})(1-\sqrt{\alpha_2})|\Omega_{t'}|^2}{((N)_{q_e})^2\prod_{i=1}^{t}(N)_{q_i}} \ .$$

Finally, noting that $|S_x\cap S_y|\geq(1-\sqrt{\alpha_1}-\sqrt{\alpha_2})(N)_{q_e}$, dividing both terms by $|\Omega_{t'}|^2=|\widetilde{\Omega}_{2t'}|$, and using

$$(1-\sqrt{\alpha_1}-\sqrt{\alpha_2})(1-\sqrt{\alpha_1})(1-\sqrt{\alpha_2}) \geq 1-2(\sqrt{\alpha_1}+\sqrt{\alpha_2}) \ ,$$

we obtain:

$$\Pr[\boldsymbol{P}(a)=b\wedge\mathtt{EM}_{\boldsymbol{P},k}(x)=y] \geq \frac{1-\beta}{(N)_{q_e}\prod_{i=1}^{t}(N)_{q_i}} \ ,$$

with $\beta=2(\sqrt{\alpha_1}+\sqrt{\alpha_2})$, which concludes the proof. □

Combining Lemmata 6 and 7, we finally obtain our main theorem.

Theorem 2. *Let t be an even integer and $t'=t/2$. Let $q_1,\ldots,q_t,q_e$ be positive integers. Then:*

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q_1,\ldots,q_t,q_e) \leq \left(\frac{2^{t'+2}q_e\prod_{i=1}^{t'}q_i}{N^{t'}}\right)^{1/2} + \left(\frac{2^{t'+2}q_e\prod_{i=t'+1}^{t}q_i}{N^{t'}}\right)^{1/2} \ .$$

In particular, for any positive integer q:

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}(q) \leq 2^{t/4+3}\frac{q^{(t+2)/4}}{N^{t/4}} \ .$$

For odd t, we have $\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t]}\leq\mathbf{Adv}^{\mathrm{cca}}_{\mathcal{EM}[t-1]}$, so that we can use the above bounds with $t-1$.

More concretely, the iterated Even-Mansour cipher with t rounds achieves CCA-security up to $N^{\frac{t}{t+2}}$ queries.

References

1. D. J. Aldous. Random walks on finite groups and rapidly mixing Markov chains. In *Séminaire de Probabilités XVII*, volume 986 of *Lecture Notes in Mathematics*, pages 243–297. Springer, 1983.
2. M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
3. A. Biryukov and D. Wagner. Advanced Slide Attacks. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 589–606. Springer, 2000.
4. A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. P. Steinberger, and E. Tischhauser. Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations - (Extended Abstract). In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2012.
5. R. Canetti, O. Goldreich, and S. Halevi. The Random Oracle Methodology, Revisited (Preliminary Version). In *Symposium on Theory of Computing - STOC '98*, pages 209–218. ACM, 1998. Full version available at `http://arxiv.org/abs/cs.CR/0010019`.
6. J. Daemen. Limitations of the Even-Mansour Construction. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 495–498. Springer, 1991.
7. J. Daemen and V. 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`.
8. O. Dunkelman, N. Keller, and A. Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012.
9. S. Even and Y. Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *Journal of Cryptology*, 10(3):151–162, 1997.
10. C. Gentry and Z. Ramzan. Eliminating Random Permutation Oracles in the Even-Mansour Cipher. In P. J. Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2004.
11. J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED Block Cipher. In B. Preneel and T. Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.
12. V. T. Hoang and P. Rogaway. On Generalized Feistel Networks. In T. Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer, 2010.
13. J. Kilian and P. Rogaway. How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). *Journal of Cryptology*, 14(1):17–35, 2001.
14. U. M. Maurer and K. Pietrzak. Composition of Random Systems: When Two Weak Make One Strong. In M. Naor, editor, *Theory of Cryptography Conference - TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 410–427. Springer, 2004.
15. U. M. Maurer, K. Pietrzak, and R. Renner. Indistinguishability Amplification. In A. Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2007.

16. I. Mironov. (Not So) Random Shuffles of RC4. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer, 2002.
17. B. Morris, P. Rogaway, and T. Stegers. How to Encipher Messages on a Small Domain. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 286–302. Springer, 2009.
18. J. Patarin. New Results on Pseudorandom Permutation Generators Based on the DES Scheme. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 301–312. Springer, 1991.

A Proof of the Coupling Lemma

The original statement and proof of the Coupling Lemma is due to Aldous [1]. Here we follow closely a proof by Vigoda.[5]

Let λ be a coupling of μ and ν, and $(X, Y) \sim \lambda$. By definition, we have that for any $z \in \omega$, $\lambda(z, z) \leq \min\{\mu(z), \nu(z)\}$. Moreover, $\Pr[X = Y] = \sum_{z \in \Omega} \lambda(z, z)$. Hence we have:

$$\Pr[X = Y] \leq \sum_{z \in \Omega} \min\{\mu(z), \nu(z)\} \ .$$

Therefore:

$$\begin{aligned}
\Pr[X \neq Y] &\geq 1 - \sum_{z \in \Omega} \min\{\mu(z), \nu(z)\} \\
&= \sum_{z \in \Omega} (\mu(z) - \min\{\mu(z), \nu(z)\}) \\
&= \sum_{\substack{z \in \Omega \\ \mu(z) \geq \nu(z)}} (\mu(z) - \nu(z)) \\
&= \max_{S \subset \Omega} \{\mu(S) - \nu(S)\} \\
&= \|\mu - \nu\| \ .
\end{aligned}$$

[5] Available from `www.cc.gatech.edu/~vigoda/MCMC_Course/MC-basics.pdf`.