Minimizing Even-Mansour Ciphers for Sequential Indifferentiability (Without Key Schedules)

Shanjie Xu[1,2], Qi Da[1,2], and Chun Guo[1,2,3](✉)

[1] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong 266237, China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China
{shanjie1997,daqi}@mail.sdu.edu.cn, chun.guo@sdu.edu.cn
[3] Shandong Research Institute of Industrial Technology, Jinan, Shandong, China

Abstract. Iterated Even-Mansour (IEM) schemes consist of a small number of fixed permutations separated by round key additions. They enjoy provable security, assuming the permutations are *public and random*. In particular, regarding chosen-key security in the sense of *sequential indifferentiability (seq-indifferentiability)*, Cogliati and Seurin (EUROCRYPT 2015) showed that without key schedule functions, the 4-round *Even-Mansour with Independent Permutations and no key schedule* $\mathrm{EMIP}_4(k,u) = k \oplus \mathbf{p}_4\big(k \oplus \mathbf{p}_3\big(k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_1(k \oplus u))\big)\big)$ is sequentially indifferentiable.
Minimizing IEM variants for classical strong (tweakable) pseudorandom security has stimulated an attractive line of research. In this paper, we seek for minimizing the EMIP_4 construction while retaining seq-indifferentiability. We first consider EMSP, a natural variant of EMIP using *a single round permutation*. Unfortunately, we exhibit a slide attack against EMSP with *any number of rounds*. In light of this, we show that the 4-round $\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}(k,u) = k \oplus \mathbf{p}_1\big(k \oplus \mathbf{p}_2\big(k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_1(k \oplus u))\big)\big)$ using 2 independent random permutations $\mathbf{p}_1, \mathbf{p}_2$ is seq-indifferentiable. This provides the *minimal seq-indifferentiable IEM without key schedule*.

Keywords: blockcipher · sequential indifferentiability · key-alternating cipher · iterated Even-Mansour cipher

1 Introduction

A fundamental cryptographic problem is to construct secure blockciphers from keyless permutations. A natural solution is the Iterated Even-Mansour (IEM) scheme (a.k.a. key-alternating cipher) initiated in [19] and extended and popularized in a series of works [24,4,17,1]. Given t permutations $\mathbf{p}_1, ..., \mathbf{p}_t : \{0,1\}^n \to \{0,1\}^n$ and a *key schedule* $\overrightarrow{\varphi} = (\varphi_0, ..., \varphi_t)$, $\varphi_i : \{0,1\}^\kappa \to \{0,1\}^n$, and for $(k,u) \in \{0,1\}^\kappa \times \{0,1\}^n$, the scheme is defined as

$$\mathrm{EM}[\overrightarrow{\varphi}]_t(k,u) := \varphi_t(k) \oplus \mathbf{p}_t\big(...\varphi_2(k) \oplus \mathbf{p}_2\big(\varphi_1(k) \oplus \mathbf{p}_1(\varphi_0(k) \oplus u)\big)...\big).$$

It abstracts *substitution-permutation network* that has been used by a number of standards [33,26,27]. Modeling $\mathbf{p}_1, ..., \mathbf{p}_t$ as public random permutations, variants of this scheme provably achieve various security notions, including indistinguishability [19,4,28,7,6,32,25,37,36], related-key security [20,8], known-key security [2,9], chosen-key security in the sense of correlation intractability [8,23], and indifferentiability [1,29,13]. Despite the theoretical uninstantiatability of the random oracle model [5], such arguments dismiss generic attacks and are typically viewed as evidences of the soundness of the design approaches.

Indifferentiability of IEM. The classical security definition for a blockcipher is *indistinguishability from a (secret) random permutation*. Though, reliable blockciphers are broadly used as *ideal ciphers*, i.e., randomly chosen blockciphers. Motivated by this, the notion of *indifferentiability [31] from ideal ciphers* was proposed [11,1,29] as the strongest security for blockcipher structures built upon (public) random functions and random permutations. Briefly speaking, for the IEM cipher $\mathrm{EM}^{\mathcal{P}}$ built upon random permutations $\mathcal{P}$, if there exists an efficient simulator $\mathcal{S}^E$ that queries an ideal cipher E to mimic its (non-existent) underlying permutations, such that $(E, \mathcal{S}^E)$ is indistinguishable from $(\mathrm{EM}^{\mathcal{P}}, \mathcal{P})$, then $\mathrm{EM}^{\mathcal{P}}$ is indifferentiable from E [31]. This property implies that the cipher $\mathrm{EM}^{\mathcal{P}}$ inherits all ideal cipher-properties defined by single-stage security games, including security against (various forms of) related-key and chosen-key attacks.

As results, Andreeva et al. [1] proposed the IEM variant $\mathrm{EMKD}_t(k, u) = \mathbf{h}(k) \oplus \mathbf{p}_t(...\mathbf{h}(k) \oplus \mathbf{p}_2(\mathbf{h}(k) \oplus \mathbf{p}_1(\mathbf{h}(k) \oplus u))...)$ using a random oracle $\mathbf{h} : \{0,1\}^\kappa \to \{0,1\}^n$ to derive the round key $\mathbf{h}(k)$, and proved indifferentiability at 5 rounds. Concurrently, Lampe and Seurin [29] proposed to consider the *"single-key" Even-Mansour* variant $\mathrm{EMIP}_t(k, u) = k \oplus \mathbf{p}_t(...k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_1(k \oplus u))...)$ without any non-trivial key schedule, and proved indifferentiability at 12 rounds. Both results are tightened in subsequent works [13,22], showing that 3-round EMKD and 5-round EMIP achieve indifferentiability.

Sequential Indifferentiability. Indifferentiable blockciphers [11,1,29,13,22] typically require unnecessarily complicated constructions [35], and their practical influences are not as notable as the analogues for hash function [10,15]. To remedy, weaker security definitions have been proposed [30,2,9,34]. In particular, to formalize *chosen-key security*, Mandal et al. [30] and subsequently Cogliati and Seurin [8] advocated the notion of *sequential-indifferentiability (seq-indifferentiability)*, which is a variant of indifferentiability concentrating on distinguishers that follow a strict restriction on the order of queries. The usefulness of seq-indifferentiability lies in its implication towards *correlation intractability* [5], meaning that no (chosen-key) adversary can find inputs/outputs of the blockcipher that satisfies evasive relations. For the aforementioned Even-Mansour variants, seq-indifferentiability (and CI) have been established for 3-round EMKD [23] and 4-round EMIP [8], both of which are tight. The fact that 4-round EMIP is seq-indifferentiable/CI but not "fully" indifferentiable also separated the two security notions [13].

Our Question. Besides initial positive results on the general $\text{EM}[\overrightarrow{\varphi}]_t$ model, another attractive line of work has been set to seek for *minimizing IEM cipher* for certain security properties. In detail, Dunkelman [17] was the first to minimize the 1-round Even-Mansour cipher by halving the key size without affecting its SPRP security. Following this and with significant technical novelty, Chen et al. [6] proposed minimal 2-round IEM variants with beyond-birthday SPRP security. Subsequently, Dutta [18] extended the discussion to tweakable Even-Mansour (TEM) ciphers and proposed minimal 2-round and 4-round IEM variants, depending on the assumptions on tweak schedule functions.

Regarding (seq-)indifferentiability, we stress that all the aforementioned results on IEM [1,29,8,23,13,22] requires *using t independent random permutations in the t rounds*. As will be elaborated, this independence is crucial for their (seq-)indifferentiability simulators. A natural next step is to investigate whether (weaker) indifferentiability is achievable using a single permutation. In particular, without key schedule, does the *single-permutation Even-Mansour* variant $\text{EMSP}_t(k, u) = k \oplus \mathbf{p}(...k \oplus \mathbf{p}(k \oplus \mathbf{p}(k \oplus u))...)$ suffice?

1.1 Our Contributions

We make the first step towards answering our question and analyze the IEM cipher with identical permutation w.r.t. the seq-indifferentiability.

New Attack Against Seq-Indifferentiability. Our first observation is that, even in the weaker model of seq-indifferentiability, the aforementioned *"single-key", single-permutation Even-Mansour* variant EMSP remains *insecure*, regardless of the number of rounds. Concretely, we exhibit a chosen-key attack that makes just 1 permutation query and 1 encryption query. Our attack utilized a sort of weakness that is related to slide attacks [3]. In detail, in the EMSP construction, a single input/output pair $\mathbf{p}(x) = y$ of the permutation already yields a full t-round EMSP_t evaluation $y \to \underbrace{(x, y) \to ... \to (x, y)}_{t \text{ times}} \to x$ with $k = x \oplus y$, by acting as the involved evaluations in all the t rounds.

Minimal and Secure Construction. Given our negative result on EMSP, to achieve security, one has to enhance 4-round EMSP by using at least 2 independent random permutations. This consideration yields a minimal IEM solution scheme $\text{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ uses two random permutations $\mathbf{p}_1, \mathbf{p}_2$ though no key schedule:

$$\text{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}(k, u) := k \oplus \mathbf{p}_1\big(k \oplus \mathbf{p}_2\big(k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_1(k \oplus u))\big)\big).$$

See Fig. 1 for an illustration. We established seq-indifferentiability for $\text{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}$ with $O(q^2)$ simulator complexity and $O(q^4/2^n)$ security which are comparable with EMIP_4 [8]. For ease of comparison, we summarize our results and the existing in Table 1.

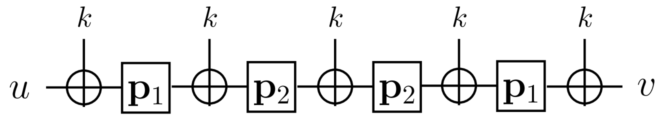

Fig. 1: The minimal construction $\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}$ using two independent random permutations $\mathbf{p}_1, \mathbf{p}_2 : \{0,1\}^n \to \{0,1\}^n$ and no key schedule.

Table 1: Comparison of ours with existing seq-indifferentiable/CI IEM results. The column **Key sch.** indicates the key schedule functions in the schemes. The column **Complex.** indicates the simulator complexities.

Scheme	**♯Rounds**	**♯Primitives**	**Key sch.**	**Complex.**	**Bounds**	**Ref.**
$\mathrm{EMIP}_4^{\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3,\mathbf{p}_4}$	4	4	no	q^2	$q^4/2^n$	[8]
$\mathrm{EMKD}_3^{\mathbf{h},\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3}$	3	4	random oracle $\mathbf{h}$	q^2	$q^4/2^n$	[23]
$\mathrm{EMSP}^{\mathbf{P}}$	t	1	no	insecure	insecure	Sect. 3
$\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}$	4	**2**	no	q^2	$q^4/2^n$	Sect. 4

Proof Approach. Our proof for the seq-indifferentiability of $\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}$ is an extension of [8], with subtle changes addressing new collision events due to permutation-reusing.

In general, to establish indifferentiability-type security, the first step is to construct a simulator that resists obvious attack. Then, it remains to argue:

- The simulator is efficient, i.e., its complexity can be bounded;
- The simulator gives rise to an ideal world $(E, \mathcal{S}^E)$ that is indistinguishable from the real world $(\mathrm{EM}^{\mathcal{P}}, \mathcal{P})$.

To design a simulator, we mostly follow the simulator strategy for EMIP_4 (which uses *independent* permutations) [8], taking queries to the middle (2nd and 3rd) rounds as "signals" for chain detection and the outer (1st and 4th) rounds for adaptations.

For example, a distinguisher D may arbitrarily pick $k, u \in \{0,1\}^n$ and evaluate $x_1 \leftarrow k \oplus u$, $\mathbf{p}_1(x_1) \to y_1$, $x_2 \leftarrow k \oplus y_1$, $\mathbf{p}_2(x_2) \to y_2$, $x_3 \leftarrow k \oplus y_2$, $\mathbf{p}_2(x_3) \to y_3$, $x_4 \leftarrow k \oplus y_4$, $\mathbf{p}_1(x_4) \to y_4$, $x_5 \leftarrow k \oplus y_4$. This creates a sequence of four *(query) records* $\big((1, x_1, y_1), (2, x_2, y_2), (2, x_3, y_3), (1, x_4, y_4)\big)$ that will be called a *computation chain* (the number 1 or 2 indicates the index of the permutation). When D is in the real world $(\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}, (\mathbf{p}_1, \mathbf{p}_2))$, it necessarily holds $\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}(k, u) = x_5$. To be consistent with this in the ideal world $(E, \mathcal{S}^E)$, $\mathcal{S}$ should "detect" such actions of D, "run ahead" of D and define some simulated (query) records to "complete" a similar computation chain.

The crucial observation on EM2P_4 is that permutations used in the middle (2nd and 3rd) rounds and the outer (1st and 4th) rounds remain independent. Consequently, upon D querying the permutation, the simulator can identify in clear if D is evaluating in the middle (when D queries P_2) or in the outer rounds (when D queries P_1). With these ideas, every time D queries P_2 or P_2^{-1}, our simulator completes all new pairs of records $\big((2, x, y), (2, x', y')\big)$ of P_2.[4]

Concretely, facing the aforementioned attack, $\mathcal{S}$ pinpoints the key $k = y_2 \oplus x_3$ and recognize the "partial chain" $\big((1, x_1, y_1), (2, x_2, y_2), (2, x_3, y_3)\big)$ upon the third permutation query $P_2(x_3) \to y_3$. $\mathcal{S}$ then queries the ideal cipher $E(k, k \oplus x_1) \to x_5$ and *adapts* the simulated P_1 by enforcing $P_1(k \oplus y_3) := k \oplus x_5$. As such, a simulated computation chain $\big((1, x_1, y_1), (2, x_2, y_2), (2, x_3, y_3), (1, k \oplus y_3, k \oplus x_5)\big)$ with $E(k, k \oplus x_1) = x_5$ is completed. Worth noting, queries to P_2 only function as "signals" for detection, while adaptations only create records on P_1 (such "adapted" records thus won't trigger new detection). This idea of assigning a unique role to every round/simulated primitive was initiated in [11], and it indeed significantly simplifies arguments.

Of course, D may pick $k', y_4' \in \{0,1\}^n$ and evaluate "conversely". In this case, our simulator detects the "partial chain" $\big((2, x_2', y_2'), (2, x_3', y_3'), (1, x_4', y_4')\big)$ after D's third query $P_2^{-1}(y_2') \to x_2'$, queries $E^{-1}(k', k' \oplus y_4') \to x_0'$ and pre-enforces $P_1(k' \oplus x_0') := k' \oplus x_5'$ to reach $\big((1, k' \oplus x_0', k' \oplus x_5'), (2, x_2', y_2'), (2, x_3', y_3'), (1, x_4', y_4')\big)$ with $E(k', k' \oplus x_1') = x_5'$. In the seq-indifferentiability setting, these have covered all adversarial possibilities. In particular, the distinguisher D cannot pick k', y_1' and evaluate $P_1^{-1}(y_1') \to x_1'$, $u' \leftarrow k' \oplus x_1'$, $E(k', u') \to v'$, and $P_1^{-1}(k' \oplus v') \to x_4'$, since this violates the query restriction. This greatly simplifies simulation [30,8,21,23] compared with the "full" indifferentiability setting.

Compared with [8], our novelty lies in handling new collision events that are harmless in the setting of EMIP_4. E.g., consider the previous example of enforcing $P_1(k \oplus y_3) := k \oplus x_5$ to complete $\big((1, x_1, y_1), (2, x_2, y_2), (2, x_3, y_3)\big)$. Since the 1st and 4th rounds are using the same permutation P_1, the collisions $k \oplus y_3 = x_1$ and $k \oplus x_5 = y_1$ also incur inconsistency in the simulated P_1 and prevent adaptation. But we do not need a paradigm-level shift: with all such events characterized, the proof follows that for EMIP_4. Clearly, the simulator detects and completes $O(q^2)$ chains, and indistinguishability of $(E, \mathcal{S}^E)$ and $(\text{EM2P}_4^{\mathbf{P}_1,\mathbf{P}_2}, \mathcal{P})$ follows a randomness mapping argument similar to [8].

1.2 Organization.

Sect. 2 serves notations and definitions. Then, in Sect. 3 and 4, we provide our attack on $\text{EMSP}_t^{\mathbf{P}}$ and sequential indifferentiability of 4-round $\text{EM2P}_4^{\mathbf{P}_1,\mathbf{P}_2}$ respectively. We finally conclude in Sect. 5.

[4] In comparison, Cogliati and Seurin's simulator for EMIP_4 completes all newly constituted pairs $\big((2, x_2, y_2), (3, x_3, y_3)\big)$ of records of P_2 *and* P_3.

2 Preliminaries

Notation. An n-bit random permutation $\mathbf{p} : \{0,1\}^n \to \{0,1\}^n$ is a permutation that is uniformly chosen from all $(2^n)!$ possible choices, and its inverse is denoted by $\mathbf{p}^{-1}$. Denote by $\mathcal{P}$ a tuple of independent random permutations $(\mathbf{p}_1, ..., \mathbf{p}_r)$, where the number t depends on the concrete context (and will be made concrete later). For integers κ and n, an ideal blockcipher $E[\kappa, n] : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is chosen randomly from the set of all blockciphers with key space $\{0,1\}^\kappa$ and message and ciphertext space $\{0,1\}^n$. For each key $k \in \{0,1\}^\kappa$, the map $E(k, \cdot)$ is a random permutation with inversion oracle $E^{-1}(k, \cdot)$. Since we focus on the case of $\kappa = n$, we will simply use E instead of $E[n, n]$.

Sequential Indifferentiability. The notion of sequential indifferentiability (seq-indifferentiability), introduced by Mandal et al. [30], is a weakened variant of (full) indifferentiability of Maurer et al. [31] tailored to *sequential distinguishers* [30], a class of restricted distinguishers. For concreteness, our formalism concentrates on blockciphers. Consider the blockcipher construction $\mathcal{C}^{\mathcal{P}}$ built upon several random permutations $\mathcal{P}$. A distinguisher $D^{\mathcal{C}^{\mathcal{P}},\mathcal{P}}$ with oracle access to both the cipher and the underlying permutations is trying to distinguish $\mathcal{C}^{\mathcal{P}}$ from the ideal cipher E. Then, D is *sequential*, if it proceeds in the following steps in a strict order: (1) queries the underlying permutations $\mathcal{P}$ in arbitrary; (2) queries the cipher $\mathcal{C}^{\mathcal{P}}$ in arbitrary; (3) outputs, and cannot query $\mathcal{P}$ again in this phase. This order of queries is illustrated by the numbers in Fig. 2.

In this setting, if there is a simulator $\mathcal{S}^E$ that has access to E and can mimic $\mathcal{P}$ such that in the view of any sequential distinguisher D, the system $(E, \mathcal{S}^E)$ is indistinguishable from the system $(\mathcal{C}^{\mathcal{P}}, \mathcal{P})$, then $\mathcal{C}^{\mathcal{P}}$ is *sequentially indifferentiable* (seq-indifferentiable) from E.

To characterize the adversarial power, we define a notion *total oracle query cost* of D, which refers to the total number of queries received by $\mathcal{P}$ (from D or $\mathcal{C}^{\mathcal{P}}$) when D interacts with $(\mathcal{C}^{\mathcal{P}}, \mathcal{P})$ [30]. Then, the definition of seq-indifferentiability due to Cogliati and Seurin [8] is as follows.

Definition 1 (Seq-indifferentiability). *A blockcipher construction $\mathcal{C}^{\mathcal{P}}$ with oracle access to a tuple of random permutations $\mathcal{P}$ is statistically and strongly $(q, \sigma, t, \varepsilon)$-seq-indifferentiable from an ideal cipher E, if there exists a simulator S^E such that for any sequential distinguisher D of total oracle query cost at most q, S^E issues at most σ queries to E and runs in time at most t, and it holds*

$$\left| \Pr_{\mathcal{P}}[D^{\mathcal{C}^{\mathcal{P}},\mathcal{P}} = 1] - \Pr_E[D^{E,\mathcal{S}^E} = 1] \right| \leq \varepsilon.$$

If D makes q queries, then its total oracle query cost is $\mathrm{poly}(q)$. As a concrete example, the t-round EM cipher $\mathrm{EM}_t^{\mathcal{P}}$ makes t queries to $\mathcal{P}$ to answer any query it receives, and if D makes q_e queries to $\mathrm{EM}_t^{\mathcal{P}}$ and q_p queries to $\mathcal{P}$, then the total oracle query cost of D is $q_p + tq_e = \mathrm{poly}(q_p + q_e) = \mathrm{poly}(q)$.

Albeit being weaker than "full" indifferentiability [31] (which can be viewed as seq-indifferentiability without restricting distinguishers to sequential), seq-indifferentiability already implies *correlation intractability* in the ideal model [30,8].

The notion of correlation intractability was introduced by Canetti et al. [5] and adapted to ideal models by Mandal et al. [30] to formalize the hardness of finding exploitable relation between the inputs and outputs of function ensembles. For simplicity, we only present asymptotic definitions. Consider a relation $\mathcal{R}$ over pairs of binary sequences.

– $\mathcal{R}$ is *evasive with respect to an ideal cipher* E, if no efficient oracle Turing machine $\mathcal{M}^E$ can output an m-tuple $(x_1, \ldots, x_m)$ such that $\big((x_1, \ldots, x_m), (E(x_1), \ldots, E(x_m))\big) \in \mathcal{R}$ with a significant success probability;
– An idealized blockcipher $\mathrm{EM}^{\mathcal{P}}$ is *correlation intractable with respect to* $\mathcal{R}$, if no efficient oracle Turing machine $\mathcal{M}^{\mathcal{P}}$ can output an m-tuple $(x_1, \ldots, x_m)$ such that $\big((x_1, \ldots, x_m), (\mathrm{EM}^{\mathcal{P}}(x_1), \ldots, \mathrm{EM}^{\mathcal{P}}(x_m))\big) \in \mathcal{R}$ with a significant success probability.

With these, the implication [30,8] states that if $\mathrm{EM}^{\mathcal{P}}$ is seq-indifferentiable from E, then for any m-ary relation $\mathcal{R}$ which is evasive with respect to E, $\mathrm{EM}^{\mathcal{P}}$ is correlation intractable with respect to $\mathcal{R}$.

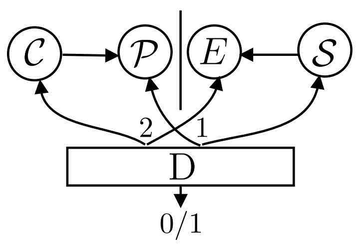

Fig. 2: Setting for seq-indifferentiability. The numbers 1 and 2 indicate the query order that D has to follow.

3 Slide Attack on the Single-key, Single-permutation EMSP

The t-round $\mathrm{EMSP}_t^{\mathbf{p}}$ uses the same permutation in every round, and is defined as

$$\mathrm{EMSP}_t^{\mathbf{p}}(k, u) := k \oplus \mathbf{p}\big(...k \oplus \mathbf{p}\big(k \oplus \mathbf{p}(k \oplus \mathbf{p}(k \oplus u))\big)...\big).$$

Our attack proceeds as follows.

1. Picks $x \in \{0,1\}^n$ in arbitrary and query $\mathbf{p}(x) \to y$.
2. Computes $k \leftarrow x \oplus y$. Outputs 1 if and only if $E(k, y) = x$.

Clearly, it always outputs 1 when interacting with $(\mathrm{EMSP}_t^{\mathbf{p}}, \mathbf{p})$ with *any rounds* t. In the ideal world, the simulator has to find a triple $(x \oplus y, y, x) \in (\{0,1\}^n)^3$ such that $E(x \oplus y, y) = x$ for the ideal cipher E. When the simulator makes q_S queries, it is easy to see: the probability that a forward ideal cipher query $E(x \oplus y, y)$ responds with x is at most $1/(2^n - q_S)$; the probability that a backward query $E^{-1}(x \oplus y, y)$ responds with x is at most $1/(2^n - q_S)$. Thus, the probability that the simulator pinpoints $E(x \oplus y, y) = x$ is at most $q_S/(2^n - q_S)$, and the attack advantage is at least $1 - q_S/(2^n - q_S)$.

It is also easy to see that, the above attack essentially leverages a relation that is evasive [8] w.r.t. an ideal cipher.

4 Seq-Indifferentiability of $\mathbf{EM2P_4}$

This section proves seq-indifferentiability for the 4-round $\mathrm{EM2P}_4^{\mathbf{p}_1,\mathbf{p}_2}$, the variant of single-key IEM using two permutations $\mathbf{p}_1, \mathbf{p}_2$, as shown in Fig. 1.

Theorem 1. *Assume that $\mathbf{p}_1$ and $\mathbf{p}_2$ are two independent random permutations. Then, the 4-round single-key Even-Mansour scheme $EM2P_4^{\mathbf{p}_1,\mathbf{p}_2}$ defined as*

$$EM2P_4^{\mathbf{p}_1,\mathbf{p}_2}(k,u) := k \oplus \mathbf{p}_1(k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_2(k \oplus \mathbf{p}_1(k \oplus u))))$$

is strongly and statistically $(q, \sigma, t, \varepsilon)$-seq-indifferentiable from an ideal cipher E, where $\sigma = q^2$, $t = O(q^2)$, and $\varepsilon \leq \frac{20q^3+29q^4}{2^n} = O(\frac{q^4}{2^n})$ (assuming $q+2q^2 \leq 2^n/2$).

To prove Theorem 1, we first describe our simulator in Sect. 4.1.

4.1 Simulator of $\mathbf{EM2P_4}$

Randomness and Interfaces. The simulator $\mathcal{S}$ offers four interfaces P_1, P_1^{-1}, P_2 and P_2^{-1} to the distinguisher for querying the internal permutations, and the input of the query is any element in the set $\{0,1\}^n$.

To handily describe lazying sampling during simulation, we follow previous works [1,29,21,16,12,14,11,13] and make the randomness used by $\mathcal{S}$ explicit through two random permutations p_1 and p_2. Namely, $\mathcal{S}$ queries $\mathbf{p}_1$ and $\mathbf{p}_2$ (see below for concreteness) to have a random value z rather than straightforwardly sampling $z \xleftarrow{\$} \{0,1\}^n$. Let $\mathcal{P} = (\mathbf{p}_1, \mathbf{p}_2)$. We denote by $\mathcal{S}^{E,\mathcal{P}}$ the simulator that emulates the primitives for E and queries $\mathbf{p}_1$ and $\mathbf{p}_2$ for necessary random values. As argued in [1], explicit randomness is merely an equivalent formalism of lazying sampling.

Maintaining Query Records. To keep track of previously answered permutation queries, $\mathcal{S}$ internally maintains two sets Π_1 and Π_2 that have entries in the form of $(i, x, y) \in \{1,2\} \times \{0,1\}^n \times \{0,1\}^n$. $\mathcal{S}$ will ensure that for any $x \in \{0,1\}^n$ and $i \in \{1,2\}$, there is at most one $y \in \{0,1\}^n$ such that $(i,x,y) \in \Pi_i$, and vice versa. As will be elaborated later, $\mathcal{S}$ aborts whenever it fails to ensure such consistency. By this, the sets Π_1 and Π_2 will define two partial permutations, and we denote by $domain(\Pi_i)$ ($range(\Pi_i)$, resp.) the (time-dependent) set of all n-bit values x (y, resp.) satisfying $\exists z \in \{0,1\}^n$ s.t. $(i,x,z) \in \Pi_i$ ($(i,z,y) \in \Pi_i$, resp.). We further denote by $\Pi_i(x)$ ($\Pi_i^{-1}(y)$, resp.) the corresponding value of z.

Simulation Strategy. Upon the distinguisher D querying $P_i(x)$ ($P_i^{-1}(y)$, resp.), $\mathcal{S}$ checks if $x \in \Pi_1$ ($y \in \Pi_1^{-1}$, resp.), and answers with $\Pi_1(x)$ ($\Pi_1^{-1}(y)$, resp.) when it is the case. Otherwise, the query is new, and $\mathcal{S}$ queries $\mathbf{p}_i$ for $y \leftarrow \mathbf{p}_i(x)$ ($x \leftarrow \mathbf{p}_i^{-1}(y)$, resp.). If $y \notin range(\Pi_i)$, $\mathcal{S}$ adds the record (i, x, y) to the set Π_i; otherwise, $\mathcal{S}$ aborts to avoid inconsistency in Π_i (as mentioned). Then, when $i = 1$, $\mathcal{S}$ simply answers with x (y, resp.); when $i = 2$, $\mathcal{S}$ completes the partial chains formed by this new record $(2, x, y)$ and previously created records in Π_2 (as mentioned in the Introduction).

In detail, when the new adversarial query is to $P_2(x)$ and $\mathcal{S}$ adds a new record $(2, x, y)$ to Π_2, $\mathcal{S}$ considers all pairs of triples $\big((2, x, y), (2, x', y')\big) \in (\Pi_2)^2$ (including the pair $\big((2, x, y), (2, x, y)\big)$) *and* all $\big((2, x', y'), (2, x, y)\big) \in (\Pi_2)^2$ (with $x' \neq x$ for distinction). Then,

- For every pair $\big((2, x, y), (2, x', y')\big) \in (\Pi_2)^2$, $\mathcal{S}$ computes $k \leftarrow y \oplus x'$ and $x_4 \leftarrow y' \oplus k$. $\mathcal{S}$ then internally invokes P_1 to have $y_4 \leftarrow P_1(x_4)$ and $v \leftarrow y_4 \oplus k$. $\mathcal{S}$ then queries the ideal cipher to have $u \leftarrow E^{-1}(k, v)$, and further computes $x_1 \leftarrow u \oplus k$ and $y_1 \leftarrow x \oplus k$. Finally, if $x_1 \notin domain(\Pi_1)$ and $y_1 \notin range(\Pi_1)$, $\mathcal{S}$ adds the record (i, x, y) to the set Π_i, to complete the 4-chain $\big((1, x_1, y_1), (2, x, y), (2, x', y'), (1, x_4, y_4)\big)$; otherwise, $\mathcal{S}$ aborts to avoid inconsistency. The record $(1, x_1, y_1)$ is called *adapted*, since it is created to "link" the simulated computation. In our pseudocode, this process is implemented as a procedure $Complete^-$;
- For every pair $\big((2, x', y'), (2, x, y)\big) \in (\Pi_2)^2$, $\mathcal{S}$ computes $k \leftarrow y' \oplus x$, $y_1 \leftarrow x' \oplus k$, $x_1 \leftarrow P_1^{-1}(y_1)$, $u \leftarrow x_1 \oplus k$; $v \leftarrow E(k, u)$, $y_4 \leftarrow v \oplus k$ and $x_4 \leftarrow y \oplus k$. $\mathcal{S}$ finally adds the adapted record $(1, x_4, y_4)$ to Π_1 when $x_4 \notin domain(\Pi_1)$ and $y_4 \notin range(\Pi_1)$, to complete $\big((1, x_1, y_1), (2, x', y'), (2, x, y), (1, x_4, y_4)\big)$, or aborts otherwise. In our pseudocode, this process is implemented as a procedure $Complete^+$.

Upon D querying $P_2^{-1}(y)$, the simulator actions are similar to $P_2(x)$ by symmetry. Our strategy is formally described via pseudocode in the next paragraph.

Simulator in Pseudocode.

Simulator $\mathcal{S}^{E,\mathcal{P}}$
Variables: Sets Π_1, Π_2, X_{Dom}, and X_{Rng}, all initially empty

public procedure $P_1(x)$
  if $x \notin domain(\Pi_1)$ **then**
    $y \leftarrow \mathbf{p}_1(x)$
    if $\Pi_1^{-1}(y) \neq \perp$ **then abort**
    if $y \in X_{Rng}$ **then abort**
    $\Pi_1 \leftarrow \Pi_1 \cup \{(1, x, y)\}$
  return $\Pi_1(x)$

public procedure $P_1^{-1}(y)$
  if $y \notin range(\Pi_1)$ **then**
    $x \leftarrow \mathbf{p}_1^{-1}(y)$
    if $\Pi_1(x) \neq \perp$ **then abort**
    if $x \in X_{Dom}$ **then abort**
    $\Pi_1 \leftarrow \Pi_1 \cup \{(1, x, y)\}$
  return $\Pi_1^{-1}(y)$

```
public procedure P_2(x)
  if x ∉ domain(Π_2) then
    y ← p_2(x)
    Π_2 ← Π_2 ∪ {(2, x, y)}
    forall (2, x', y') ∈ Π_2 do
      // 3^+ chain
      k ← y' ⊕ x
      if y ⊕ k ∈ domain(Π_1)
        then abort
      X_Dom ← X_Dom ∪ {y ⊕ k}
      X_Rng ← X_Rng ∪ {x' ⊕ k}
      // 2^+ chain
      k ← y ⊕ x'
      if x ⊕ k ∈ range(Π_1)
        then abort
      if ∃(2, x'', y'') ∈ Π_2 :
         x' ⊕ y' ⊕ x = x ⊕ y ⊕ x''
        then abort
      X_Dom ← X_Dom ∪ {y' ⊕ k}
      X_Rng ← X_Rng ∪ {x ⊕ k}
    forall (2, x', y') ∈ Π_2
      s.t. x' ≠ x do
      k ← x ⊕ y'
      Complete^+(x', k)
    forall (2, x', y') ∈ Π_2 do
      k ← y ⊕ x'
      Complete^-(y', k)
  // Clear the pending sets
  X_Dom ← ∅, X_Rng ← ∅
  return Π_2(x)
```

```
public procedure P_2^{-1}(y)
  if y ∉ range(Π_2) then
    x ← p_2^{-1}(y)
    Π_2 ← Π_2 ∪ {(2, x, y)}
    forall (2, x', y') ∈ Π_2 do
      // 2^- chain
      k ← y ⊕ x'
      if x ⊕ k ∈ range(Π_1)
        then abort
      X_Dom ← X_Dom ∪ {y' ⊕ k}
      X_Rng ← X_Rng ∪ {x ⊕ k}
      // 3^- chain
      k ← y' ⊕ x
      if y ⊕ k ∈ domain(Π_1)
        then abort
      if ∃(2, x'', y'') ∈ Π_2 :
         y' ⊕ x' ⊕ y = y'' ⊕ x ⊕ y
        then abort
      X_Dom ← X_Dom ∪ {y ⊕ k}
      X_Rng ← X_Rng ∪ {x' ⊕ k}
    forall (2, x', y') ∈ Π_2
      s.t. x' ≠ x do
      k ← y ⊕ x'
      Complete^-(y', k)
    forall (2, x', y') ∈ Π_2 do
      k ← x ⊕ y'
      Complete^+(x', k)
  // Clear the pending sets
  X_Dom ← ∅, X_Rng ← ∅
  return Π_2^{-1}(y)
```

```
private procedure Complete^+(x_2, k)
  y_1 ← x_2 ⊕ k, x_1 ← P_1^{-1}(y_1)
  u ← x_1 ⊕ k, v ← E(k, u)
  y_4 ← v ⊕ k
  y_2 ← P_2(x)
  x_3 ← y_2 ⊕ k, y_3 ← P_2(x_3)
  x_4 ← y_3 ⊕ k
  if x_4 ∈ domain(Π_1) then abort
  if y_4 ∈ range(Π_1) then abort
  if y_4 ∈ X_Rng then abort
  Π_1 ← Π_1 ∪ {(1, x_4, y_4)}
```

```
private procedure Complete^-(y_3, k)
  x_4 ← y_3 ⊕ k, y_4 ← P_1(x_4)
  v ← y_4 ⊕ k, u ← E^{-1}(k, v)
  x_1 ← u ⊕ k
  x_3 ← P_2^{-1}(y_3)
  y_2 ← x_3 ⊕ k, x_2 ← P_2^{-1}(y_2)
  y_1 ← x_2 ⊕ k
  if x_1 ∈ domain(Π_1) then abort
  if y_1 ∈ range(Π_1) then abort
  if x_1 ∈ X_Dom then abort
  Π_1 ← Π_1 ∪ {(1, x_1, y_1)}
```

We identify a number of bad events during the simulation and coded them in $\mathcal{S}$. The occurrence of such events indicates potential abortions due to adaptations in future. In detail, before calling $Complete^+$ and $Complete^-$, $\mathcal{S}$ creates two sets X_{Rng} and X_{Dom} for the values that will be used in subsequent adaptations: for every $x \in X_{Dom}$, $\mathcal{S}$ will create an adapted record of the form $(1, x, \star)$; for every

$y \in X_{Rng}$, $\mathcal{S}$ will create an adapted record of the form $(1, \star, y)$. Therefore, collisions among values in X_{Dom} and $domain(\Pi_1)$ (resp., X_{Rng} and $range(\Pi_1)$) already indicate the failure of some future adaptations. Thus, once such events occur, $\mathcal{S}$ also aborts to terminate the doomed execution.

4.2 The Indistinguishability Proof

It remains to establish two claims for any distinguisher D: (a) the simulator $\mathcal{S}^{E,\mathcal{P}}$ has bounded complexity; (b) the real and ideal worlds are indistinguishable. To this end, we introduce a helper intermediate system in the next paragraph. Then, subsequent paragraphs establish claims (a) and (b) in turn.

Intermediate System. As shown in Fig. 3, we use three systems for the proof. In detail, let $\Sigma_1(E, \mathcal{S}^{E,\mathcal{P}})$ be the system capturing the ideal world, where E is an ideal cipher and $\mathbf{p}_1$, $\mathbf{p}_2$ are independent random permutations; and let $\Sigma_3(\text{EM2P}_4^{\mathcal{P}}, \mathcal{P})$ be the real world.

We follow [30,8] and introduce $\Sigma_2(\text{EM2P}_4^{\mathcal{S}^{E,\mathcal{P}}}, \mathcal{S}^{E,\mathcal{P}})$ as an intermediate system, which is modified from Σ_1 by replacing E with an EM2P_4 instance that queries the simulator to evaluate.

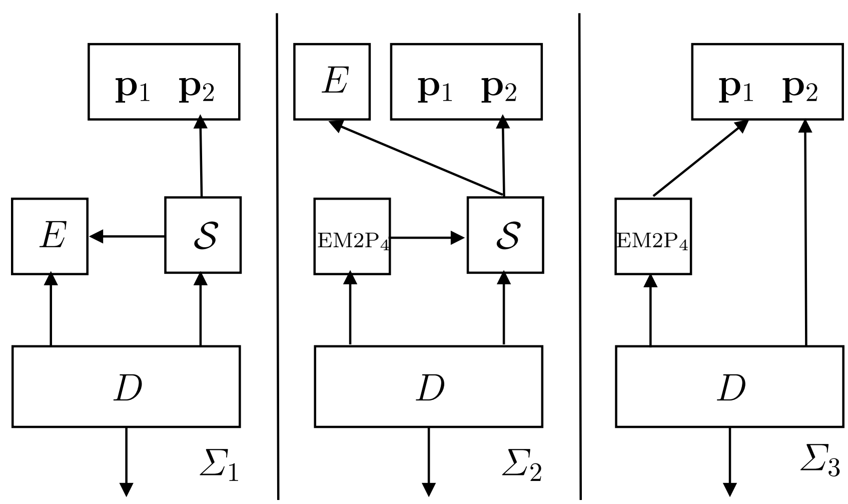

Fig. 3: Systems used in the proof.

Then, consider a fixed sequential distinguisher D of total oracle query cost at most q. The remaining key points are as follows.

Complexity of $\mathcal{S}^{E,\mathcal{P}}$. As the key observation, $\mathcal{S}^{E,\mathcal{P}}$ never adds records to Π_2 internally. Thus, $|\Pi_2|$ increases by 1 after each adversarial query, and thus

$|\Pi_2| \le q$. By this, the number of detected chains $\big((2, x_2, y_2), (2, x_2', y_2')\big) \in (\Pi_2)^2$ is at most q^2. This also means $\mathcal{S}^{E,\mathcal{P}}$ makes at most q^2 queries to E, since such a query only appears during completing a detected chain. For each detected chain, $\mathcal{S}^{E,\mathcal{P}}$ adds at most 2 records to Π_1. Moreover, $|\Pi_1|$ may also increase by q due to D straightforwardly querying P_1 or P_1^{-1}. It thus holds $|\Pi_1| \le q + 2q^2$. Finally, the running time is dominated by completing chains, and is thus $O(q^2)$.

Indistinguishability of $\boldsymbol{\Sigma_1}$, $\boldsymbol{\Sigma_2}$ and $\boldsymbol{\Sigma_3}$. First, we need to show that the two simulated permutations are consistent, which is of course necessary for indistinguishability. Note that the occurrence of such inconsistency would particularly render $\mathcal{S}^{E,\mathcal{P}}$ abort. Therefore, via a fine-grained analysis of the various involved values, we establish an upper bound on the probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts.

4.3 Abort Probability of $\mathcal{S}^{E,\mathcal{P}}$

As discussed in Sect. 4.2, when the total oracle query cost of D does not exceed q, it holds $|\Pi_2| \le q$, and the total number of detected chains $\big((2, x_2, y_2), (2, x_2', y_2')\big) \in (\Pi_2)^2$ is at most q^2. The latter means:

(i) the number of adapted records in Π_1 is at most q;
(ii) the number of calls to P_1 and P_1^{-1} is at most $q + q^2$ in total (which is the number of detected chains plus the number of adversarial queries to P_1 and P_1^{-1});
(iii) $|X_{Dom}| \le q^2$, $|X_{Rng}| \le q^2$.

With the above bounds, we analyze the abort conditions in turn.

Lemma 1. *The probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts at lines 6, 7, 13 and 14 is at most $(2q^3 + 2q^4)/2^n$.*

Proof. Consider lines 6 and 7 in P_1 first. The value $y \leftarrow \mathbf{p}_1(x)$ newly "downloaded" from $\mathbf{p}_1$ is uniformly distributed in $2^n - |\Pi_1| \ge 2^n - q - 2q^2$ possibilities. This value y is independent of the values in Π_1 and X_{Rng}. Thus, the conditions for lines 6 and 7 are fulfilled with probability at most $|range(\Pi_1) \cup X_{Rng}|$. However, it is easy to see that, the size of the union set $range(\Pi_1) \cup X_{Rng}$ cannot exceed the upper bound on the number of adapted records in Π_1 at the end of the execution, since every value y' in X_{Rng} eventually becomes a corresponding adapted record $(1, x', y')$ in Π_1 as long as $\mathcal{S}^{E,\mathcal{P}}$ does not abort. Therefore, $|range(\Pi_1) \cup X_{Rng}| \le q^2$, and thus each call to P_1 aborts with probability at most $q^2/(2^n - q - 2q^2)$. Similarly by symmetry, each call to P_1^{-1} aborts with probability at most $q^2/(2^n - q - 2q^2)$. Since the number of calls to P_1 and P_1^{-1} is at most $q + q^2$ in total, the probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts at lines 6, 7, 13 and 14 is at most

$$(q + q^2) \cdot \frac{q^2}{2^n - (q + 2q^2)} \le \frac{2q^3 + 2q^4}{2^n},$$

assuming $q + 2q^2 \le 2^n/2$. □

Next, we analyze the probability of the "early abort" conditions in P_2 and P_2^{-1}.

Lemma 2. *The probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts at lines 25, 31 and 32 in the procedure P_2 (resp., lines 52, 58 and 59 in the procedure P_2^{-1}) is at most* $(6q^3 + 8q^4)/2^n$.

Proof. Consider the conditions in P_2 first. The value $y \leftarrow \mathbf{p}_1(x)$ newly "downloaded" from $\mathbf{p}_1$ is uniformly distributed in $2^n - |\Pi_1| \geq 2^n - q - 2q^2$ possibilities. Moreover, this value y is independent of the values in Π_1, Π_2 and X_{Rng}.

With the above in mind, we analyze the conditions in turn. First, consider line 25. For every detected partial chain $\big((2, x', y'), (2, x, y)\big)$, the condition $y \oplus k \in domain(\Pi_1)$ translates into $y \oplus y' \oplus x \in domain(\Pi_1)$, which holds with probability at most $|domain(\Pi_1)|/(2^n - q - 2q^2) \leq (q + 2q^2)/(2^n - q - 2q^2)$ (since $|\Pi_1| \leq q + 2q^2$).

The arguments for the remaining conditions are similar: since y is uniform,

- for every detected partial chain $\big((2, x, y), (2, x', y')\big)$, the condition $x \oplus k \in range(\Pi_1) \Leftrightarrow x \oplus y \oplus x' \in range(\Pi_1)$ is fulfilled with probability at most $(q + 2q^2)/(2^n - q)$ (again using $|\Pi_1| \leq q + 2q^2$);
- for every detected partial chain $\big((2, x', y'), (2, x, y)\big)$, the probability to have $x' \oplus y' \oplus x = x \oplus y \oplus x''$ for some $(2, x'', y'') \in \Pi_2$ is at most $q/(2^n - q - 2q^2)$(since $|\Pi_2| \leq q$).

Since the number of detected partial chains $\big((2, x', y'), (2, x, y)\big)$ is at most $|\Pi_2| \leq q$, the probability that a single query or call to $P_2(x)$ aborts at lines 25, 31 and 32 is at most

$$q \times \Big(\frac{q + 2q^2}{2^n - q - 2q^2} + \frac{q + 2q^2}{2^n - q - 2q^2} + \frac{q}{2^n - q - 2q^2}\Big) \leq \frac{3q^2 + 4q^3}{2^n - q - 2q^2} \leq \frac{6q^2 + 8q^3}{2^n},$$

assuming $q + 2q^2 \leq 2^n/2$.

The above complete the analysis for P_2. The analysis for lines 52, 58 and 59 in P_2^{-1} is similar by symmetry, yielding the same bound. Summing over the at most q queries or calls to P_2 and P_2^{-1}, we reach the claimed bound $q(6q^2 + 8q^3)/2^n \leq 6q^3 + 8q^4/2^n$. ◻

For the subsequent argument, we introduce a bad event BadE_ℓ regarding the ideal cipher queries made during $\mathcal{S}$ processing the ℓ-th adversarial query to $P_2(x^{(\ell)})$ or $P_2^{-1}(y^{(\ell)})$. Formally, BadE_ℓ occurs if:

- In this period, during a call to $Complete^{+}(x_2, k)$ in this period, a query to $v \leftarrow E(k, u)$ is made, and the response satisfies $v \oplus k \in range(\Pi_1)$ or $v \oplus k \in X_{Rng}$; or
- In this period, during a call to $Complete^{-}(y_3, k)$ in this period, a query to $u \leftarrow E^{-1}(k, v)$ is made, and the response satisfies $u \oplus k \in domain(\Pi_1)$ or $u \oplus k \in X_{Dom}$.

To analyze BadE_ℓ, we need a helper lemma as follows.

Lemma 3. *Inside every call to Complete$^+$, resp. Complete$^-$, the ideal cipher query $E(k,u)$, resp. $E^{-1}(k,v)$, is fresh. Namely, the simulator $\mathcal{S}^{E,\mathcal{P}}$ never made this query $E(k,u)$, resp. $E^{-1}(k,v)$, before.*

Proof. Assume that this does not hold. Then this means that such a query previously occurred when completing another chain. By the construction of $\mathrm{EM2P}_4$ and our simulator, this means right after the call to *Complete*$^+$ or *Complete*$^-$ that queried $E(k,u)$, all the four corresponding round inputs/outputs $(1,x_1,y_1)$, $(2,x_2,y_2)$, $(2,x_3,y_3)$ and $(1,x_4,y_4)$ with $k = u \oplus x_1 = y_1 \oplus x_2 = ... = y_4 \oplus E(k,u)$ have been in Π_1 and Π_2. This in particular includes the query to P_2/P_2^{-1} that was purported to incur the current call to *Complete*$^+$/*Complete*$^-$. But since the query to P_2/P_2^{-1} is not new, this contradicts the construction of our simulator. Therefore, the ideal cipher query must be fresh. □

The probability of BadE_ℓ is then bounded as follows.

Lemma 4. *In each call to Complete$^+$ or Complete$^-$, the probability that BadE_ℓ occurs is at most $2(q+2q^2)/2^n$.*

Proof. We first analyze the abort probabilities of calls to *Complete*$^+$ and *Complete*$^-$. Consider a call to *Complete*$^+(x_2,k)$ first. By Lemma 3, the ideal cipher query $E(k,u) \to v$ made inside this call is new. Since $\mathcal{S}^{E,\mathcal{P}}$ makes at most q^2 queries to E, the value v is uniform in at least $2^n - q^2$ possibilities. Furthermore, v is independent of the values in X_{Rng} and $range(\Pi_1)$. Therefore,

$$\Pr[v \oplus k \in (X_{Rng} \cup range(\Pi_1))] \le \frac{|X_{Rng} \cup range(\Pi_1)|}{2^n - q^2}.$$

It is easy to see that $|X_{Rng} \cup range(\Pi_1)|$ cannot exceed the upper bound $q+2q^2$ on $|\Pi_1|$ at the end of the execution. Therefore, the probability to have BadE_ℓ in a call to *Complete*$^+(x_2,k)$ is at most $(q+2q^2)/(2^n-q^2)$.

The analysis of *Complete*$^-(y_3,k)$ is similar by symmetry, yielding the same bound $(q+2q^2)/(2^n-q^2)$. Assuming $q^2 \le 2^n/2$, we obtain the claim. □

Then, we address the abort probability due to adaptations in *Complete*$^+$ and *Complete*$^-$ call.

Lemma 5. *The probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts at lines 78, 79, and 80; 89, 90, and 91 is at most $(2q^3+4q^4)/2^n$.*

Proof. Noting that *Complete*$^+$ and *Complete*$^-$ are only called during processing adversarial queries to $P_2(x)/P_2^{-1}(y)$, we quickly sketch the process of the latter. Wlog we focus on processing a query $P_2(x)$, as the case of $P_2^{-1}(y)$ is similar by symmetry.

Upon D making the ℓ-th query to $P_2(x^{(\ell)})$, $\mathcal{S}^{E,\mathcal{P}}$ first "downloads" the response $y^{(\ell)} \leftarrow \mathbf{p}_2(x)$ from $\mathbf{p}_2$ and then detects a number of partial chains as follows:

$$\begin{aligned}
2^{+}\text{chains}: &\big((2,x^{(1)},y^{(1)}),(2,x^{(\ell)},y^{(\ell)})\big),...,\big((2,x^{(\ell-1)},y^{(\ell-1)}),(2,x^{(\ell)},y^{(\ell)})\big),\\
3^{+}\text{chains}: &\big((2,x^{(\ell)},y^{(\ell)}),(2,x^{(1)},y^{(1)})\big),...,\big((2,x^{(\ell)},y^{(\ell)}),(2,x^{(\ell-1)},y^{(\ell-1)})\big),\\
&\big((2,x^{(\ell)},y^{(\ell)}),(2,x^{(\ell)},y^{(\ell)})\big),
\end{aligned}$$

where $(2,x^{(1)},y^{(1)}),...,(2,x^{(\ell-1)},y^{(\ell-1)})\in\Pi_2$ are the triples created due to the earlier $\ell-1$ adversarial queries to P_2 or P_2^{-1}. For conceptual convenience we refer to the former type of chains as 2^{+}*chains* and the latter as 3^{+}*chains*. $\mathcal{S}$ then proceeds in two steps:

- First, completes the 3^{+}chains in turn, making a number of calls to *Complete*$^{+}$;
- Second, completes the 2^{+}chains in turn, making a number of calls to *Complete*$^{-}$.

We proceed to argue that, during processing the ℓ-th query to $P_2(x^{(\ell)})$, the above calls to *Complete*$^{+}$/*Complete*$^{-}$ abort with probability at most $\big(2(2\ell-1)(q+2q^2)\big)/2^n$ in total.

To this end, consider the j-th 3^{+}chain $\big((2,x^{(j)},y^{(j)}),(2,x^{(\ell)},y^{(\ell)})\big)$. Let $k^{(j)}=y^{(j)}\oplus x^{(\ell)}$ and $x_4^{(j)}=k^{(j)}\oplus y^{(\ell)}$. Since $\mathcal{S}$ did not abort at line 25, it holds $x_4^{(j)}\notin \mathit{domain}(\Pi_1)$ right after $\mathcal{S}$ "downloads" $y^{(\ell)}\leftarrow \mathbf{p}_2(x)$. We then show that $x_4^{(j)}\notin \mathit{domain}(\Pi_1)$ is kept till the call to *Complete*$^{+}(x^{(j)},k^{(j)})$ adapts by adding $(1,x_4^{(j)},y_4^{(j)})$ to Π_1, so that lines 78, 79 and 80 won't cause abort.

- First, for any 3^{+}chain $\big((2,x^{(j')},y^{(j')}),(2,x^{(\ell)},y^{(\ell)})\big)$ completed before the chain $\big((2,x^{(j)},y^{(j)}),(2,x^{(\ell)},y^{(\ell)})\big)$, its adaptation cannot add $(1,x_4^{(j)},\star)$ to Π_1, since its adapted pair is of the form $x_4^{(j')}=y^{(j')}\oplus x^{(\ell)}\oplus y^{(\ell)}\neq x_4^{(j)}$;
- Second, internal queries to $P_1^{-1}(y_1)\to x_1$ (with $x_1\leftarrow \mathbf{p}_1^{-1}(y_1)$) during this period cannot add $(1,x_4^{(j)},\star)$ to Π_1, since $x_4^{(j)}$ was added to X_{Dom} and since $x_1\notin X_{Dom}$ (otherwise $\mathcal{S}$ has aborted at line 7).

Thus, line 78 won't cause abort at all. On the other hand, with $\neg\mathsf{BadE}_\ell$ as the condition, $y_4^{(j)}\notin(\mathit{range}(\Pi_1)\cup X_{Rng})$ necessarily holds. Therefore, in the call to *Complete*$^{+}(x^{(j)},k^{(j)})$ adapts, lines 79 and 80 will not cause abort. The above completes the argument for *Complete*$^{+}$ calls due to 3^{+}chains.

We then address 2^{+}chains by considering the j-th $\big((2,x^{(\ell)},y^{(\ell)}),(2,x^{(j)},y^{(j)})\big)$. Let $k^{(j)}=y^{(j)}\oplus x^{(\ell)}$ and $x_4^{(j)}=k^{(j)}\oplus y^{(\ell)}$. Since $\mathcal{S}$ did not abort at line 25, it holds $x_4^{(j)}\notin \mathit{domain}(\Pi_1)$ right after $\mathcal{S}$ downloads $y^{(\ell)}\leftarrow \mathbf{p}_2(x)$. We then show that $x_4^{(j)}\notin \mathit{domain}(\Pi_1)$ is kept till the call to *Complete*$^{+}(x^{(j)},k^{(j)})$ adapts by adding $(1,x_4^{(j)},y_4^{(j)})$ to Π_1, so that lines 78, 79 and 80 won't cause abort.

Therefore, during processing the ℓ-th query to $P_2(x^{(\ell)})$ or $P_2^{-1}(y^{(\ell)})$, the probability that $\mathcal{S}$ aborts in each call to *Complete*$^{+}$ or *Complete*$^{-}$ is equal to $\Pr[\mathsf{BadE}_\ell]$, which does not exceed $2(q+2q^2)/2^n$ by Lemma 4.

To summarize, recall that the total number of detected partial chains/calls to *Complete*$^+$ or *Complete*$^-$ is bounded by $|\Pi_2|^2 \leq q^2$. Therefore, the probability that $\mathcal{S}^{E,\mathcal{P}}$ aborts at lines 78, 79, and 80; 89, 90, and 91 is bounded by

$$q^2 \times \Big(\frac{2(q+2q^2)}{2^n}\Big) \leq \frac{2q^3+4q^4}{2^n},$$

as claimed. □

Lemma 6. *The probability that* $\mathcal{S}^{E,\mathcal{P}}$ *aborts in* D^{Σ_2} *is at most* $(10q^3+14q^4)/2^n$.

Proof. Gathering Lemmas 1, 2 and 5 yields the bound.

4.4 Indistinguishability of Σ_1 and Σ_3

A random tuple $(E,\mathcal{P})$ is *good*, if $\mathcal{S}^{E,\mathcal{P}}$ does not abort in $D^{\Sigma_2(E,\mathcal{P})}$. It can be proved that, for any good tuple $(E,\mathcal{P})$, the transcript of the interaction of D with $\Sigma_1(E,\mathcal{P})$ and $\Sigma_2(E,\mathcal{P})$ is exactly the same. This means the gap between Σ_1 and Σ_2 is the abort probability.

Σ_1 to Σ_2.

Lemma 7. *For any distinguisher* D *of total oracle query cost at most* q*, it holds*

$$\Big|\Pr[D^{\Sigma_1(E,\mathcal{S}^{E,\mathcal{P}})}=1]-\Pr[D^{\Sigma_2(EM2P_4^{\mathcal{S}^{E,\mathcal{P}}},\mathcal{S}^{E,\mathcal{P}})}=1]\Big| \leq \frac{10q^3+14q^4}{2^n}.$$

Proof. Note that in Σ_1 and Σ_2, the sequential distinguisher D necessarily first queries $\mathcal{S}$ and then E (in Σ_1) or $\mathrm{EM2P}_4$ (in Σ_2) only. Thus, the transcript of the first phase of the interaction (i.e., for the queries of D to $\mathcal{S}^{E,\mathcal{P}}$) are clearly the same, since in both cases they are answered by $\mathcal{S}$ using the same randomness $(E,\mathcal{P})$. For the second phase of the interaction (i.e., queries of D to its left oracle), it directly follows from the adaptation mechanism. Hence, the transcripts of the interaction of D with $\Sigma_1(E,\mathcal{P})$ and $\Sigma_2(E,\mathcal{P})$ are the same for any good tuple $(E,\mathcal{P})$. Further using Lemma 6 yields

$$\begin{aligned}&\Big|\Pr[D^{\Sigma_1(E,\mathcal{S}^{E,\mathcal{P}})}=1]-\Pr[D^{\Sigma_2(\mathrm{EM2P}_4^{\mathcal{S}^{E,\mathcal{P}}},\mathcal{S}^{E,\mathcal{P}})}=1]\Big|\\ \leq\ &\Pr[(E,\mathcal{P})\ \textit{is bad}] \leq \frac{10q^3+14q^4}{2^n},\end{aligned}$$

as claimed. □

Σ_2 to Σ_3: Randomness Mapping. We now bound the gap between Σ_2 and Σ_3. Following [11,8], the technique is the randomness mapping argument.

We define a map Λ mapping pairs $(E,\mathcal{P})$ either to the special symbol $\perp$ when $(E,\mathcal{P})$ is bad, or to a pair of *partial permutations* $\mathcal{P}'=(\mathbf{p}'_1,\mathbf{p}'_2)$ when $(E,\mathcal{P})$ is good. A partial permutation is functions $\mathbf{p}'_i\colon \{0,1\}^n \to \{0,1\}^n \cup \{*\}$

and $\mathbf{p}_i'^{-1}\colon \{0,1\}^n \to \{0,1\}^n \cup \{*\}$, such that for all $x, y \in \{0,1\}^n$, $\mathbf{p}_i'(x) = y \neq * \Leftrightarrow \mathbf{p}_i'^{-1}(y) = x \neq *$.

Then map Λ is defined for good pairs $(E, \mathcal{P})$ as follows: run $D^{\Sigma_2(E,\mathcal{P})}$, and consider the tables Π_i of the simulator at the end of the execution: then fill all undefined entries of the Π_i's with the special symbol $*$. The result is exactly $\Lambda(E,\mathcal{P})$. Since for a good pair $(E,\mathcal{P})$, the simulator never overwrite an entry in its tables, it follows that $\Lambda(E,\mathcal{P})$ is a pair of partial permutations as just defined above. We say that a pair of partial permutations $\mathcal{P}' = (\mathbf{p}_1', \mathbf{p}_2')$ is good if it has a good preimage by Λ. Then, we say that a pair of permutations $\mathcal{P}$ extends a pair of partial permutations $\mathcal{P}' = (\mathbf{p}_1', \mathbf{p}_2')$, denoted $\mathcal{P} \vdash \mathcal{P}'$, if for each $i = 1, 2$, $\mathbf{p}_i$ and $\mathbf{p}_i'$ agree on all entries such that $\mathbf{p}_i'(x) \neq *$ and $\mathbf{p}_i'^{-1}(y) \neq *$.

By definition of the randomness mapping, for any good tuple of partial permutations $\mathcal{P}'$, the outputs of $D^{\Sigma_2(E,\mathcal{P})}$ and $D^{\Sigma_3(\mathcal{P})}$ are equal for any pair $(E,\mathcal{P})$ such that $\Lambda(E,\mathcal{P}) = \mathcal{P}'$ and any tuple of permutations $\mathcal{P}$ such that $\mathcal{P} \vdash \mathcal{P}'$. Let Ω_1 be the set of partial permutations $\mathcal{P}'$ such that $D^{\Sigma_2(E,\mathcal{P})}$ output 1 for any pair $(E,\mathcal{P})$ such that $\Lambda(E,\mathcal{P}) = \mathcal{P}'$. Then, we have the following ratio.

Lemma 8. *Consider a fixed distinguisher D with total oracle query cost at most q. Then, for any $\mathcal{P}' = (\mathbf{p}_1', \mathbf{p}_2') \in \Omega_1$, it holds*

$$\frac{\Pr\big[\mathcal{P} \vdash \mathcal{P}'\big]}{\Pr\big[\Lambda(E,\mathcal{P}) = \mathcal{P}'\big]} \geq 1 - \frac{q^4}{2^n}.$$

Proof. Since the number of "non-empty" entries $\mathbf{p}_1'(x) \neq *$ and $\mathbf{p}_2'(x) \neq *$ are $|\Pi_1|$ and $|\Pi_2|$ respectively, we have

$$\Pr\big[\mathcal{P} \vdash \mathcal{P}'\big] = \bigg(\prod_{j=0}^{|\Pi_1|-1} \frac{1}{2^n - j}\bigg)\bigg(\prod_{j=0}^{|\Pi_2|-1} \frac{1}{2^n - j}\bigg).$$

Fix any good preimage $(\widetilde{E}, \widetilde{\mathcal{P}})$ of $\mathcal{P}'$. One can check that for any tuple $(E,\mathcal{P})$, $\Lambda(E,\mathcal{P}) = \mathcal{P}'$ *iff* the transcript of the interaction of $\mathcal{S}$ with $(E,\mathcal{P})$ in $D^{\Sigma_2(E,\mathcal{P})}$ is the same as the transcript of the interaction of $\mathcal{S}$ with $(\widetilde{E}, \widetilde{\mathcal{P}})$ in $D^{\Sigma_2(\widetilde{E}, \widetilde{\mathcal{P}})}$.

Assume that during the Σ_2 execution $D^{\Sigma_2(\mathrm{EM2P}_4^{\mathcal{S}^{E,\mathcal{P}}}, \mathcal{S}^{E,\mathcal{P}})}$, $\mathcal{S}$ makes q_e, q_1 and q_2 queries to E, $\mathbf{p}_1$ and $\mathbf{p}_2$ respectively. Then,

$$\Pr\big[\Lambda(E,\mathcal{P}) = \mathcal{P}'\big] \leq \bigg(\prod_{j=0}^{q_e-1} \frac{1}{2^n - j}\bigg)\bigg(\prod_{j=0}^{q_1-1} \frac{1}{2^n - j}\bigg)\bigg(\prod_{j=0}^{q_2-1} \frac{1}{2^n - j}\bigg).$$

It is easy to see that, $q_e + q_1 + q_2 = |\Pi_1| + |\Pi_2|$: because $q_1 + q_2$ equal the number of lazily sampled records in Π_1 and Π_2, while q_e equal the number of adapted records in Π_1.

Furthermore, $q_e \le q^2$ by Sect. 4.2. It thus holds

$$\begin{aligned}\frac{\Pr\left[\mathcal{P} \vdash \mathcal{P}'\right]}{\Pr\left[\Lambda(E,\mathcal{P}) = \mathcal{P}'\right]} &\geq \frac{\left(\prod_{j=0}^{|\Pi_1|-1} \frac{1}{2^n-j}\right)\left(\prod_{j=0}^{|\Pi_2|-1} \frac{1}{2^n-j}\right)}{\left(\prod_{j=0}^{q_e-1} \frac{1}{2^n-j}\right)\left(\prod_{j=0}^{q_1-1} \frac{1}{2^n-j}\right)\left(\prod_{j=0}^{q_2-1} \frac{1}{2^n-j}\right)} \\ &\geq \prod_{j=0}^{q^2-1} \left(1 - \frac{j}{2^n}\right) \\ &\geq 1 - \frac{(q^2)^2}{2^n} \geq 1 - \frac{q^4}{2^n},\end{aligned}$$

as claimed. □

Lemma 9. *For any distinguisher D with total oracle query cost at most q, it holds*

$$\left|\Pr\left[D^{\Sigma_2(EM2P_4^{\mathcal{S}^{E,\mathcal{P}}},\mathcal{S}^{E,\mathcal{P}})} = 1\right] - \Pr\left[D^{\Sigma_3(EM2P_4^{\mathcal{P}},\mathcal{P})} = 1\right]\right| \leq \frac{10q^3 + 15q^4}{2^n}.$$

Proof. Gathering Lemmas 6 and 8 yields

$$\begin{aligned}&\left|\Pr\left[D^{\Sigma_2(\mathrm{EM2P}_4^{\mathcal{S}^{E,\mathcal{P}}},\mathcal{S}^{E,\mathcal{P}})} = 1\right] - \Pr\left[D^{\Sigma_3(\mathrm{EM2P}_4^{\mathcal{P}},\mathcal{P})} = 1\right]\right| \\ \leq &\Pr\left[(E,\mathcal{P}) \textit{ is bad}\right] + \sum_{\mathcal{P}' \in \Omega_1} \Pr\left[\Lambda(E,\mathcal{P}) = \mathcal{P}'\right] - \sum_{\mathcal{P}' \in \Omega_1} \Pr\left[\mathcal{P} \vdash \mathcal{P}'\right] \\ \leq &\Pr\left[(E,\mathcal{P}) \textit{ is bad}\right] + \sum_{\mathcal{P}' \in \Omega_1} \Pr\left[\Lambda(E,\mathcal{P}) = \mathcal{P}'\right]\left(1 - \frac{\Pr\left[\mathcal{P} \vdash \mathcal{P}'\right]}{\Pr\left[\Lambda(E,\mathcal{P}) = \mathcal{P}'\right]}\right) \\ \leq &\frac{10q^3 + 14q^4}{2^n} + \frac{q^4}{2^n} \sum_{\mathcal{P}' \in \Omega_1} \Pr\left[\Lambda(E,\mathcal{P}) = \mathcal{P}'\right] \\ \leq &\frac{10q^3 + 15q^4}{2^n},\end{aligned}$$

as claimed. □

Gathering Lemmas 7 and 9 yields the bound in Theorem 1.

5 Conclusion

We make a step towards minimizing the 4-round iterated Even-Mansour ciphers while retaining sequential indifferentiability. On the negative side, we exhibit an attack against single-key, single-permutation Even-Mansour with any rounds; on the positive side, we prove sequential indifferentiability for 4-round single-key Even-Mansour using 2 permutations. These provide the minimal Even-Mansour variant that achieve sequential indifferentiability without key schedule functions.

Acknowledgements

We sincerely thank the anonymous reviewers for their helpful comments. Chun Guo was partly supported by the National Natural Science Foundation of China (Grant No. 62002202).

References

1. Andreeva, E., Bogdanov, A., Dodis, Y., Mennink, B., Steinberger, J.P.: On the indifferentiability of key-alternating ciphers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 531–550. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40041-4_29
2. Andreeva, E., Bogdanov, A., Mennink, B.: Towards understanding the known-key security of block ciphers. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 348–366. Springer, Heidelberg (Mar 2014). https://doi.org/10.1007/978-3-662-43933-3_18
3. Biryukov, A., Wagner, D.: Slide attacks. In: Knudsen, L.R. (ed.) FSE'99. LNCS, vol. 1636, pp. 245–259. Springer, Heidelberg (Mar 1999). https://doi.org/10.1007/3-540-48519-8_18
4. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.X., Steinberger, J.P., Tischhauser, E.: Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (Apr 2012). https://doi.org/10.1007/978-3-642-29011-4_5
5. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM **51**(4), 557–594 (2004). https://doi.org/10.1145/1008731.1008734
6. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: Minimizing the two-round Even-Mansour cipher. Journal of Cryptology **31**(4), 1064–1119 (Oct 2018). https://doi.org/10.1007/s00145-018-9295-y
7. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (May 2014). https://doi.org/10.1007/978-3-642-55220-5_19
8. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46800-5_23
9. Cogliati, B., Seurin, Y.: Strengthening the known-key security notion for block ciphers. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 494–513. Springer, Heidelberg (Mar 2016). https://doi.org/10.1007/978-3-662-52993-5_25
10. Coron, J.S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-Damgård revisited: How to construct a hash function. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 430–448. Springer, Heidelberg (Aug 2005). https://doi.org/10.1007/11535218_26
11. Coron, J.S., Holenstein, T., Künzler, R., Patarin, J., Seurin, Y., Tessaro, S.: How to build an ideal cipher: The indifferentiability of the Feistel construction. Journal of Cryptology **29**(1), 61–114 (Jan 2016). https://doi.org/10.1007/s00145-014-9189-6

12. Dachman-Soled, D., Katz, J., Thiruvengadam, A.: 10-round Feistel is indifferentiable from an ideal cipher. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 649–678. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_23
13. Dai, Y., Seurin, Y., Steinberger, J.P., Thiruvengadam, A.: Indifferentiability of iterated Even-Mansour ciphers with non-idealized key-schedules: Five rounds are necessary and sufficient. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 524–555. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63697-9_18
14. Dai, Y., Steinberger, J.P.: Indifferentiability of 8-round Feistel networks. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 95–120. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_4
15. Dodis, Y., Ristenpart, T., Steinberger, J.P., Tessaro, S.: To hash or not to hash again? (In)differentiability results for H^2 and HMAC. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 348–366. Springer, Heidelberg (Aug 2012). https://doi.org/10.1007/978-3-642-32009-5_21
16. Dodis, Y., Stam, M., Steinberger, J.P., Liu, T.: Indifferentiability of confusion-diffusion networks. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 679–704. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_24
17. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: The Even-Mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer, Heidelberg (Apr 2012). https://doi.org/10.1007/978-3-642-29011-4_21
18. Dutta, A.: Minimizing the two-round tweakable Even-Mansour cipher. In: ASIACRYPT 2020, Part I. pp. 601–629. LNCS, Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_20
19. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology **10**(3), 151–162 (Jun 1997). https://doi.org/10.1007/s001459900025
20. Farshim, P., Procter, G.: The related-key security of iterated Even-Mansour ciphers. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 342–363. Springer, Heidelberg (Mar 2015). https://doi.org/10.1007/978-3-662-48116-5_17
21. Guo, C., Lin, D.: A synthetic indifferentiability analysis of interleaved double-key Even-Mansour ciphers. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 389–410. Springer, Heidelberg (Nov / Dec 2015). https://doi.org/10.1007/978-3-662-48800-3_16
22. Guo, C., Lin, D.: Indifferentiability of 3-round even-mansour with random oracle key derivation. IACR Cryptol. ePrint Arch. p. 894 (2016), http://eprint.iacr.org/2016/894
23. Guo, C., Lin, D.: Separating invertible key derivations from non-invertible ones: sequential indifferentiability of 3-round even–mansour. Designs, Codes and Cryptography **81**(1), 109–129 (2016). https://doi.org/10.1007/s10623-015-0132-0
24. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (Sep / Oct 2011). https://doi.org/10.1007/978-3-642-23951-9_22
25. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 3–32. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_1

26. ISO/IEC: Information technology — security techniques – lightweight cryptography – part 2: Block ciphers. ISO/IEC 29192-2:2012 (2012), https://www.iso.org/standard/56552.html
27. ISO/IEC: Information security – encryption algorithms – part 7: Tweakable block ciphers. ISO/IEC FDIS 18033-7 (2021), https://www.iso.org/standard/80505.html
28. Lampe, R., Patarin, J., Seurin, Y.: An asymptotically tight security analysis of the iterated Even-Mansour cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 278–295. Springer, Heidelberg (Dec 2012). https://doi.org/10.1007/978-3-642-34961-4_18
29. Lampe, R., Seurin, Y.: How to construct an ideal cipher from a small set of public permutations. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 444–463. Springer, Heidelberg (Dec 2013). https://doi.org/10.1007/978-3-642-42033-7_23
30. Mandal, A., Patarin, J., Seurin, Y.: On the public indifferentiability and correlation intractability of the 6-round Feistel construction. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 285–302. Springer, Heidelberg (Mar 2012). https://doi.org/10.1007/978-3-642-28914-9_16
31. Maurer, U.M., Renner, R., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (Feb 2004). https://doi.org/10.1007/978-3-540-24638-1_2
32. Mouha, N., Luykx, A.: Multi-key security: The Even-Mansour construction revisited. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 209–223. Springer, Heidelberg (Aug 2015). https://doi.org/10.1007/978-3-662-47989-6_10
33. Pub, N.F.: 197: Advanced encryption standard (aes). Federal information processing standards publication **197**(441), 0311 (2001)
34. Soni, P., Tessaro, S.: Public-seed pseudorandom permutations. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part II. LNCS, vol. 10211, pp. 412–441. Springer, Heidelberg (Apr / May 2017). https://doi.org/10.1007/978-3-319-56614-6_14
35. Soni, P., Tessaro, S.: Naor-Reingold goes public: The complexity of known-key security. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 653–684. Springer, Heidelberg (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_21
36. Tessaro, S., Zhang, X.: Tight security for key-alternating ciphers with correlated sub-keys. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021, Part III. Lecture Notes in Computer Science, vol. 13092, pp. 435–464. Springer (2021). https://doi.org/10.1007/978-3-030-92078-4
37. Wu, Y., Yu, L., Cao, Z., Dong, X.: Tight security analysis of 3-round key-alternating cipher with a single permutation. In: ASIACRYPT 2020, Part I. pp. 662–693. LNCS, Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_22