Towards a Characterization of the Related-Key Attack Security of the Iterated Even-Mansour Cipher

Dana Dachman-Soled[*] Angela Park[†] Ben San Nicolas[‡]

July 15, 2016

Abstract

We prove the related-key security of the Iterated Even-Mansour cipher under broad classes of related key derivation (RKD) functions. Our result extends the classes of RKD functions considered by Farshim and Procter (FSE, 15). Moreover, we present a far simpler proof which uses techniques similar to those used by Cogliati and Seurin (EUROCRYPT, 15) in their proof that the four-round Even-Mansour cipher is secure against XOR related-key attacks—a special case of our result and the result of Farshim and Proctor. Finally, we give a concrete example of a class of RKD functions covered by our result which *does not* satisfy the requirements given by Farshim and Procter and prove that the three-round Even-Mansour cipher is secure against this class of RKD functions.

[*] Dept. of Electrical and Computer Engineering, University of Maryland. Email: danadach@ece.umd.edu. Work supported in part by NSF CAREER award #1453045. This work was performed under financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

[†] Cornell University. Email: adp88@cornell.edu. This work was done when the author was visiting the University of Maryland.

[‡] Dept. of Computer Science, University of Maryland. Email: bensannicolas@gmail.com.

1 Introduction

The security of modern block ciphers—i.e., families of pseudorandom permutations—such as the Advanced Encryption Standard (AES), is not based on highly structured mathematical assumptions such as factoring or discrete-log, but rather relies on heuristics and empirical evidence. Nevertheless, the design of modern block-ciphers is far from ad-hoc, and typically their high-level structure is derived from one of a few classical, well-studied paradigms.

One of the well-known paradigms for building practical block ciphers is known as the Iterated-Even-Mansour (or, equivalently, the key-alternating) cipher. In this paradigm, computation of the block cipher proceeds in $r+1$ rounds and it is assumed that the block-cipher has oracle access (in both the forward and backward direction) to r public, independent, random permutations $\mathrm{P} = (P_1, \ldots, P_r)$. The initial state st_1 is set to the input $x \in \{0,1\}^n$. In each round i, the current state st_i, is xor'd with the corresponding *round key* k_i and updated. Then the updated state st_i is queried to the permutation P_i and the state at the end of the round is set to the output of this query. In the final round, the state st_{r+1} is xor'd with the corresponding *round key* k_{r+1}, but no permutation is applied. In this work, we consider the case where all round keys are set to the same value (i.e. $k = k_1 = k_2 = \cdots = k_{r+1}$) and refer to this as the "trivial key schedule." Formally the computation of the cipher is defined as follows:

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

To invert the cipher, one can then compute:

$$\mathsf{EM}^{-1,\mathrm{P}}(k, y) := k \oplus P_1(k \oplus P_2(\cdots P_{r-1}^{-1}(k \oplus P_r^{-1}(k \oplus y)) \cdots)).$$

The Iterated Even-Mansour cipher models the high-level structure of modern block-ciphers such as the Advanced Encryption Standard (AES). In practice, of course, the public, random permutations applied in each round are replaced with concrete, efficient instantiations. Nevertheless, an important area of research is to understand the provable security guarantees offered by this classical paradigm. Specifically, studying the security of the Iterated Even-Mansour cipher in the idealized, random permutation model, reveals the strengths and weaknesses inherent to block ciphers that follow this high-level paradigm: When the security of concrete block ciphers such as AES differ from what the Iterated Even-Mansour cipher predicts, it points to a flaw in the low-level specification of the scheme, rather than the high-level structure.

In 1991, Even and Mansour [10] (and subsequently Dunkelman et al. [8] in 2012) proved that the two-round Even Mansour cipher is indistinguishable from a random permutation. In this work, we consider *increasing* the number of rounds in order to achieve a stronger notion of security, known as security against *related-key* attacks.

Related-Key Attacks and Prior Work. Security under related-key attacks (RKAs), first considered by Biham and Knudsen [6, 5, 13], captures non-traditional settings where an attacker may tamper with user keys, and thus cause the cryptosystem to be run on a sequence of related keys. Related-key attacks are also of concern in settings where, through faulty design, a higher-level protocol runs a lower-level protocol on related keys (instead of generating fresh keys for each instance), allowing an adversary to observe correlated outputs of the cryptosystem on related keys. Real-life examples of such incorrect key usage, are key derivation procedures in standardized protocols such as EMV [9] and the 3GPP integrity and confidentiality algorithms [12]. Due to these examples, related-key attacks have become a practical concern, and resilience against RKAs, particularly for blockciphers, is now a widely-accepted security goal. Bellare and Kohno [4] initiated the theoretical study of security under related-key attacks and introduced rigorous definitions capturing RKA-secure pseudorandom functions (PRFs) and pseudorandom permutations (PRPs). Subsequently, Albrecht et al. [1] extended these definitions to idealized models of computation (as we consider in our setting) to capture settings in which the key is derived in a way that depends on the ideal primitive. Both works prove that the ideal cipher is RKA secure against broad classes of related-key derivation (RKD) functions. Bellare and Cash [2] presented an RKA-secure pseudorandom function, against specific classes of related-key functions, from standard assumptions. Subsequently, Bellare, Cash, and Miller [3] investigated the possibility of RKA-preserving security reductions, showing e.g. a generic constructions of RKA and chosen ciphertext attack (CCA) secure public key encryption from any RKA-secure identity-based encryption (IBE).

In this work we are specifically interested in the RKA security of the $r+1$-round Even-Mansour cipher with the trivial key schedule. Formally, we consider a class of related-key derivation (RKD) functions Φ and a related-key adversary $\mathcal{A}$ who has access to $r+1$ oracles: r permutation oracles, and a related-key oracle RK—which is supposed to simulate the extra power afforded to the adversary by a related-key attack. In more detail, on input (ϕ, x), $x \in \{0,1\}^n$, the related-key oracle RK for a block cipher BC_k with key k (denoted $\mathsf{RK}[\mathsf{BC}_k]$) runs the block-cipher $\mathsf{BC}_{\phi(k)}(x)$ on input x and related-key $\phi(k)$ and returns the output to the adversary. In the security game, the adversary may make up to q_p queries to each $P_i \in \mathrm{P}$ and q_e queries to its RK oracle and must distinguish between the following two worlds:

- the "real" world, where it interacts with $(\mathsf{RK}[\mathsf{EM}_k^{\mathrm{P}}], \mathrm{P})$ where $\mathrm{P} = (P_1, \ldots, P_r)$ is a tuple of random permutations, EM^{P} is the $r+1$-round Even-Mansour cipher, and k is a randomly drawn key;

- the "ideal" world where it interacts with $(\mathsf{RK}[E_k], \mathrm{P})$ where $\mathrm{P} = (P_1, \ldots, P_r)$ is a tuple of random permutations, E is an ideal cipher independent from P, and k a randomly drawn key.

In both of the above worlds, the attacker interacts with its oracles to produce a transcript, τ, which represents everything the attacker has learned about the block cipher during its interactions. To prove security, we must show that the view of the adversary is indistinguishable in the above two worlds, which is equivalent to showing that the distributions over transcripts in the two worlds are statistically close. We denote by $\mathrm{Adv}^{\Phi}_{\mathrm{EM}[n,r]}(q_e, q_p)$ the distinguishing advantage of the adversary in the above game.

The related-key security of the Iterated Even-Mansour cipher in the model discussed above has been considered by the two prior works of Farshim and Proctor [11] and Cogliati and Seurin [7]. Briefly, Farshim and Proctor's result applies to general classes of RKD functions (in particular, their result encompasses RKD functions $\phi(k) = \phi^{\mathrm{P}}(k)$ that make oracle queries to P), while Cogliati and Seurin address the special case of XOR related-key attacks, where the key k may be xor'd with a known offset Δ. On the other hand, Cogliati and Seurin's proof, which uses the H-coefficient technique [14], is more rigorous and achieves somewhat improved concrete security bounds versus that of Farshim and Proctor.

1.1 Our Results

In this work, we prove the related-key security of the Iterated Even-Mansour Cipher against a strictly larger set of classes of RKD functions than the set of classes considered by Farshim and Proctor [11]. In particular, we note that our result (as well as the result of Farshim and Proctor) includes as a special case the class of XOR related-key attacks, defined above, which is of particular interest. We use proof techniques similar to the H-coefficient technique that was used by Cogliati and Seurin [7], thereby greatly simplifying our analysis.

The requirements on the classes of functions we consider can be framed in various ways: First, they can be framed with respect to events that occur during an execution of the Ideal experiment in the RKA security definition (see Section 2.1). We then show that the requirements on the classes of functions we consider can also be framed with respect to events that occur during an execution of the Real experiment in the RKA security definition, with only slight security loss (see Section 2.1 and Lemma 3.6). Finally, we show that these requirements can also be framed with respect to an adversary $\mathcal{A}^{\mathrm{P}}$ that has oracle access to P, but *no* oracle access to RK and thus no access at all to the secret key k (see Sections 2.2, 2.3). Framing our requirements in this way allows us to compare our requirements with the requirements of Farshim and Proctor, who adopted the latter approach.

We sketch below the three requirements we impose on the classes of RKD functions (see Section 2.1 for more details). Note that we allow our RKD functions $\phi(k) = \phi^{\mathrm{P}}(k)$ to make oracle queries to P.

First requirement: Output unpredictability says $\phi(k)$ is unpredictable and is a basic requirement already shown to be necessary for RKA security of the *ideal cipher* by Bellare and Kohno [4]. Our requirement is a strengthening of output unpredictability (similar to Farshim and Proctor) which essentially says that for known x, y, the quantities $P_1(\phi(k) \oplus x) \oplus \phi(k)$ and $P_3^{-1}(\phi(k) \oplus y) \oplus \phi(k)$ are unpredictable. Specifically, we define a bad event $\mathrm{EV}_{\mathrm{ou1}}$ which occurs if the same query to P_2 is made (1) directly to the P_2 oracle and (2) during computation of the encrypt/decrypt procedure within an RK query.

Second requirement: Claw-freeness (also called collision-resistance and required by Bellare and Kohno [4] to achieve RKA security of the *ideal cipher*) says that for it is hard to find distinct ϕ_1, ϕ_2 such that $\phi_1(k) = \phi_2(k)$. Our requirement is a strengthening of claw-freeness (again, similar to Farshim and Proctor) which essentially says that it is hard to find distinct ϕ_1, ϕ_2 and x_1, x_2 or y_1, y_2 such that $P_1(\phi_1(k) \oplus x_1) \oplus \phi_1(k) = P_1(\phi_2(k) \oplus x_2) \oplus \phi_2(k)$ or $P_3^{-1}(\phi_1(k) \oplus y_1) \oplus \phi_1(k) = P_3^{-1}(\phi_2(k) \oplus y_2) \oplus \phi_2(k)$. Note that our requirement implies claw-freeness by setting $x_1 = 0, x_2 = 0$. Specifically, we define a bad event $\mathrm{EV}_{\mathrm{cf1}}$ which occurs if the same query to P_2 is made during computation of the encrypt/decrypt procedure within two distinct RK queries.

Third requirement: Our third requirement is a technical requirement that seems necessary in order to complete the security proof. Our requirement is strictly weaker than the third requirement of Farshim and Proctor. Informally, in their result, Farshim and Proctor required that the same query to P_2 is never made both (1) during the computation of some RKD function $\phi_1(k)$ and (2) during the encryption/decryption procedure corresponding to some RK query with RKD function ϕ_2. In our work we relax this requirement and allow intersection queries as above, as long as the transcript can be re-ordered in such a way that the query during encryption/decryption occurs *first*. Specifically, the adversary $\mathcal{A}$ generates a transcript τ during the related-key attack experiment (making queries to its oracles in an arbitrary order). For each adversary $\mathcal{A}$, we consider all possible re-ordering functions $\mathcal{R}(\tau)$ that re-order the queries in the transcript τ. The event $\mathrm{EV}_{\mathrm{ord}}$ is the event that the same query to P_2 is made during (1) and (2) as above and, moreover, that (1) occurs before (2). For adversary $\mathcal{A}$ making (q_p, q_e) queries, we then consider the minimum probability that $\mathrm{EV}_{\mathrm{ord}}$ occurs over choice of re-ordering function $\mathcal{R}$. Let $\mathrm{EV}_{\mathrm{ord}}^{\mathcal{R}}$ denote the event that $\mathrm{EV}_{\mathrm{ord}}$ occurs when the best possible re-ordering function for $\mathcal{A}$, $\mathcal{R}$, is used. Note that the order of queries specified by $\mathcal{R}(\tau)$ may be entirely different from the order of queries made by the adversary, $\mathcal{A}$, during the security experiment.

We now present our main result:

Theorem 1.1 (Informal)**.** *Let q_e, q_p be positive integers, $N = 2^n$, and assume the trivial key-schedule. Let Φ_ρ^m be a class of RKD functions such that (1) every $\phi \in \Phi_\rho^m$ makes at most m queries to* P*; and (2) for all adversaries $\mathcal{A}$ making at most q_e queries to* RK *and q_p queries to each $P_i \in \mathrm{P}$, the probability that event $\mathrm{EV}_{\mathrm{ou1}}$ or $\mathrm{EV}_{\mathrm{cf1}}$ or $\mathrm{EV}_{\mathrm{ord}}^{\mathcal{R}}$ occurs is at most ρ.*

Then

$$\mathrm{Adv}_{\mathrm{EM}[n,r]}^{\Phi_\rho^{\mathrm{m}}}(q_e, q_p) \leq 2\rho + \frac{3m(q_e)^2}{N} + \frac{2(q_e)^2}{N} + \frac{q_e \cdot q_p}{N}.$$

Finally, we give a concrete example of a class Φ of RKD functions that satisfies our three requirements, but does not satisfy the requirements of Farshim and Proctor. Specifically, security of the four-round Even-Mansour cipher for this class Φ does *not* follow from the results of Farshim and Proctor, since it is possible to cause the same query to be made (1) during the computation of some RKD function $\phi_1(k)$ and (2) during the encryption/decryption procedure corresponding to some RK query with RKD function ϕ_2 *with probability* 1. Nevertheless, using our main theorem above, we are able to show that the three-round Even-Mansour cipher is secure against this RKD class Φ. More formally, we prove the following theorem:

Theorem 1.2. *Let $N = 2^n$, q_e, q_p be positive integers, I the identity function, and Φ the RKD class defined as:*

$$\Phi = \begin{cases} \phi_\Delta, & \Delta \in \{0,1\}^n \\ I \end{cases}$$

where $\phi_\Delta(k) := P_2(P_1(k \oplus \Delta) \oplus k) \oplus P_1(k \oplus \Delta)$. Then

$$\mathrm{Adv}_{\mathrm{EM}[n,2]}^{\Phi}(q_e, q_p) \leq \frac{13(q_e)^2}{N} + \frac{9q_e \cdot q_p}{N} + \frac{4(q_e)^2 \cdot q_p}{N} + \frac{8(q_e)^3}{N}.$$

Note that the P_2 query made by RKD function $\phi_\Delta(k)$ is the same as the P_2 query made during the encryption procedure when the RK oracle is queried with input (I, Δ).

We leave for future work the significant problem of fully characterizing the classes of RKD functions for which the $r + 1$-round Even-Mansour cipher achieves related-key security.

2 Methodology and Preliminaries

Notation. For positive integers x, y, $x \geq y$, we denote by $(x)_y := (x)(x-1)\cdots(x-y+1)$. For an event EV, we denote by $\overline{\mathrm{EV}}$ the complement of the event. The following is readily verified:

Fact 2.1. *For positive integers x, a, c such that $x > a \cdot c$, we have that*

$$\frac{(x-a)^c}{x^c} \geq 1 - \frac{ac}{x}.$$

The Iterated Even-Mansour Cipher. Fix integers $n, r \geq 1$. We consider the $r + 1$-round iterated Even-Mansour construction when the same key k is used in each round (we call this the "trivial key schedule"). In this paper, we consider only $r \geq 2$. It is defined in the following way: $\mathsf{EM}[n,r]$ specifies, from any r-tuple $\mathrm{P} = (P_1, \ldots, P_r)$ of permutations of $\{0,1\}^n$, a block cipher with n-bit keys and n-bit messages, simply denoted EM^{P} in all the following (parameters $[n,r]$ will always be clear from the context), which maps a plaintext $x \in \{0,1\}^n$ and a key $k \in \{0,1\}^n$ to the ciphertext defined by:

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

Related-Key Oracle. Let $E \in \mathsf{BC}(\kappa, n)$ be a block cipher, and fix a key $k \in \{0,1\}^\kappa$. We define the related-key oracle with respect to RKD class Φ, $\mathsf{RK}^\Phi[E_k]$, which takes as input a function $\phi \in \Phi$ and a plaintext $x \in \{0,1\}^n$, and returns $\mathsf{RK}^\Phi[E_k](\phi, x) := E_{\phi(k)}(x)$. The oracle can be queried backward, namely $\mathsf{RK}[E_k]^{\Phi,-1}(\phi, y) := E^{-1}_{\phi(k)}(y)$. Note that we allow functions $\phi \in \Phi$ to make *oracle queries* to P.

Security against related-key attacks. To formalize related-key attacks against the r-round Even-Mansour cipher, we extend in a straightforward way the classical Bellare-Kohno model [4] to the case where the adversary has access to additional oracles. Formally, we consider a class of RKD functions Φ and a related-key adversary $\mathcal{A}$ which has access to $r+1$ oracles—r permutation oracles and a related-key oracle—and must distinguish between the following two worlds:

- the "real" world, where it interacts with $(\mathsf{RK}[\mathsf{EM}^{\mathrm{P}}_k], \mathrm{P})$ where $\mathrm{P} = (P_1, \ldots, P_r)$ is a tuple of random permutations and k is a randomly drawn key;
- the "ideal" world where it interacts with $(\mathsf{RK}[E_k], \mathrm{P})$ where $\mathrm{P} = (P_1, ..., P_r)$ is a tuple of random permutations, E an ideal cipher independent from P, and k a randomly drawn key.

The adversary is adaptive, and can make two-sided queries to each oracle. As usual, we assume that it is computationally unbounded, deterministic, and never makes pointless queries. Note that in the ideal world, as long as $\phi_1(k) \neq \phi_2(k)$, the related-key oracle $\mathsf{RK}[E_k]$ simply implements an independent random permutation for each ϕ_1, ϕ_2. The distinguishing advantage of $\mathcal{A}$ is defined as

$$\mathrm{Adv}(\mathcal{A}) = \left| \Pr[\mathcal{A}^{\mathsf{RK}[\mathsf{EM}^{\mathrm{P}}_k], \mathrm{P}} = 1] - \Pr[\mathcal{A}^{\mathsf{RK}[E_k], \mathrm{P}} = 1] \right|,$$

where the first probability is taken over the random choice of k and P, and the second probability is taken over the random choice of E, k, and P. For q_e, q_p non-negative integers, we define the insecurity of the iterated Even-Mansour cipher against Φ-restricted related-key attacks as

$$\mathrm{Adv}^{\Phi}_{\mathrm{EM}[n,r]}(q_e, q_p) = \max_{\mathcal{A}} \mathrm{Adv}(\mathcal{A}),$$

where the maximum is taken over all adversaries making exactly q_e queries to the related-key oracle and exactly q_p queries to each inner permutation oracle, $P_i \in \mathrm{P}$. We assume without loss of generality, that for each RK query with RKD function ϕ made by $\mathcal{A}$, there is a corresponding RK query made by $\mathcal{A}$ with the same RKD function ϕ and the input (x or y) set to 0.

Transcript. The transcript τ consists of two parts: A key k and a set $\mathcal{S}_\tau$ of tuples (representing adversarial queries) of the following form: $(\mathcal{O}, \phi, x, y)$ where $\mathcal{O}$ denotes whether the oracle the query was made to was $P_i, i \in [r]$ or RK, ϕ denotes the associated RKD function if $\mathcal{O} = \mathsf{RK}$, and is set to $\perp$ otherwise, and x, y denote the input/output received by the adversary, respectively. We do not make a distinction between queries made in the forward or inverse direction to RK or P_i. Let $\mathcal{T}$ denote the set of all possible transcripts. The transcript τ is meant to capture the view of the adversary $\mathcal{A}$ in the security experiment. We denote by T_{re}, resp. T_{id}, the probability distribution of the transcript τ induced by the real world, resp. the ideal world (note that these two probability distributions depend on the adversary). By extension, we use the same notation to denote a random variable distributed according to each distribution. The advantage of adversary $\mathcal{A}$ can be upper-bounded by the statistical distance between T_{re} and T_{id}. We denote by $\mathcal{T}_{\mathrm{re}}$ and $\mathcal{T}_{\mathrm{id}}$ the support of T_{re} and T_{id}, respectively.

Extended Transcript. The extended transcript τ_{ext} represents all the randomness needed to implement the oracles in the real experiment and consists of two parts: A key k and a set $\mathcal{S}_{\tau_{ext}}$ of tuples (representing all queries made to P_i during the experiment—even "hidden" ones) of the following forms: $(P_i, \perp, x, y)$ denotes a direct query made to oracle P_i. $(\mathsf{RK}, \phi, x, y, b, P_i, x', y')$ denotes a hidden query to P_i made during an adversarial query to RK with RKD function ϕ and input/output x, y. More specifically, $(\mathsf{RK}, \phi, x, y)$ denotes the original adversarial query, b is a bit set to 1 if the hidden query was made during evaluation of the RKD function $\phi(k)$ and 0 otherwise, P_i represents the oracle the hidden query was made to, and x', y' denote the input/output of the query to P_i. Note that, for fixed $\mathcal{A}$, given an extended transcript τ_{ext}, the original transcript τ can be recovered. We write $\tau_{ext} \vdash \tau$ to indicate that τ_{ext} is an extended transcript consistent with τ. Note that $\mathcal{A}$'s view does not include everything in τ_{ext}. We denote by $\mathrm{T}_{\mathrm{re}}^{\mathrm{ext}}$, the probability distribution of the extended transcript τ_{ext} induced by the real world (note that this probability distribution depends on the adversary). By extension, we use the same notation to denote a random variable distributed according to the distribution.

Ordered Transcript. For a given τ, an ordering of τ, τ^{ord} consists of two parts A key k and a set $\mathcal{S}_{\tau}^{ord}$ of tuples (representing adversarial queries) of the following form: $(\mathcal{O}, \phi, x, y, j)$ where $(\mathcal{O}, \phi, x, y) \in \mathcal{S}_{\tau}$, and the index $j \in |\mathcal{S}_{\tau}|$ indicates an ordering of the queries in $\mathcal{S}_{\tau}$. For a fixed τ, let $Ord(\tau)$ denote the set of all possible orderings of τ. For transcripts containing at most s queries, we consider the set of all possible re-ordering functions $\mathcal{R}$ that take as input τ with s queries and output an ordered transcript $\tau^{ord} \in Ord(\tau)$.

2.1 Our Requirements on RKD Classes

We next present our requirements on RKD classes. In Sections 2.2 and 2.3 we show that our requirements are strictly weaker than those of Farshim and Proctor. At a very high-level, our requirements state that the following events occur with small probability. Details follow.

The event $\mathrm{EV}_{\mathrm{ou1}}$**.** Given a (partial) extended transcript τ_{ext}, $\mathrm{EV}_{\mathrm{ou1}}$ occurs if:

$$\exists (\mathsf{RK}, \phi, x', y', 0, P_2, x, y), (P_2, \perp, 0, P_2, x, y) \in \tau_{ext},$$

i.e. the same query is made to P_2 within an RK query and directly to the P_2 oracle.

The events $\mathrm{EV}_{\mathrm{cf}}$ **and** $\mathrm{EV}_{\mathrm{cf1}}$**.** If (in the Real or Ideal game) $\mathcal{A}$ makes two RK queries such that $\phi_1 \neq \phi_2$, but $\phi_1(k) = \phi_2(k)$, then $(\phi_1, \phi_2, \mathrm{COL})$ is recorded in the transcript, τ, and $\mathrm{EV}_{\mathrm{cf}}$ is said to occur. Note that this event occurs *internally* during a draw $\tau \sim \mathrm{T}_{\mathrm{id}}$ (resp. $\tau \sim \mathrm{T}_{\mathrm{re}}$).

Given a (partial) extended transcript τ_{ext}, $\mathrm{EV}_{\mathrm{cf1}}$ occurs if:

$$\exists (\mathsf{RK}, \phi_1, x_1, y_1, 0, P_2, x', y'), (\mathsf{RK}, \phi_2, x_2, y_2, 0, P_2, x', y') \in \tau_{ext} \text{ s.t. } (\phi_1, x_1, y_1) \neq (\phi_2, x_2, y_2),$$

i.e. there exist two distinct queries to RK, in which the same query is made to P_2 and these queries were not made during evaluation of the RKD function.

The event $\mathrm{EV}_{\mathrm{ord}}$**.** Given a (partial) extended transcript τ_{ext} and a re-ordering function $\mathcal{R}$, $\mathrm{EV}_{\mathrm{ord}}$ occurs if:

$$\begin{aligned} &\exists (\mathsf{RK}, \phi_1, x_1, y_1, 1, P_2, x', y'), (\mathsf{RK}, \phi_2, x_2, y_2, 0, P_2, x', y') \in \tau_{ext} \text{ s.t.} \\ &\quad (1)\ (\mathsf{RK}, \phi_1, x_1, y_1, j_1), (\mathsf{RK}, \phi_2, x_2, y_2, j_2) \in \mathcal{R}(\tau) \text{ for some } j_1, j_2 \\ &\quad (2)\ j_1 \leq j_2, \end{aligned}$$

i.e. while querying RK, the same query is made to P_2 both during evaluation of an RKD function and not during the evaluation of an RKD function. Moreover, in the ordering $\mathcal{R}(\tau)$ of the transcript τ, the query made during the evaluation of the RKD function occurs first.

The event $\mathrm{EV}_{\mathrm{bp}}$**.** This event occurs with low probability for *every* class Φ and is only included since it will be useful for the proof. Given a (partial) extended transcript τ_{ext}, $\mathrm{EV}_{\mathrm{bp}}$ occurs if:

$$\begin{aligned}&\exists(\mathsf{RK}, \phi_1, x_1, y_1, 1, P_2, x_3, y_3), (\mathsf{RK}, \phi_2, x_2, y_2, 0, P_2, x_4, y_4) \in \tau_{ext} \text{ s.t.}\\ &\qquad (x_3 = x_4 \wedge y_3 \neq y_4) \vee (x_3 \neq x_4 \wedge y_3 = y_4),\end{aligned}$$

i.e. inconsistent answers are given to queries made to P_2 during calls to RK—once during the evaluation of the RKD function and once not during the evaluation of the RKD function.

We next define a distribution over extended transcripts in the Ideal setting, which will help us formally define the classes of RKD sets for which we can prove security.

Distribution $\mathrm{T}^{\mathrm{ext}}_{\mathrm{id}}$

- Sample $\tau \sim \mathrm{T}_{\mathrm{id}}$ and compute $\mathcal{R}(\tau)$.
- Sample P conditioned *the direct queries to* P *contained in* τ *only.*
- Answer hidden queries to produce τ_{ext} as specified in Procedure Hidden and output τ_{ext}.

Procedure Hidden**:**

1. For each RK query inside the re-ordering of τ, $\mathcal{R}(\tau)$, make the next hidden query to $P_1, \ldots, P_r$, with the P_2 query during the encrypt/decrypt procedure (not during computation of $\phi(k)$) always made *last.*
2. Hidden queries are answered in the following way: If the query already appears in τ, or has already been answered, answer as before. If the query is a query to P_2 during the encrypt/decrypt procedure, its answer must already be determined by previous queries and the transcript τ. For all other queries, use access to P in order to answer the query.
3. Once $m \cdot q_e$ queries have been answered via access to P_2 during the experiment, then for all subsequent queries to P_2 made during evaluation of an RKD function, ignore P and output the lexicographically first response that has not been used yet.

For an event EV, we denote by $\Pr_{\mathrm{Ideal}}[\mathrm{EV}]$ (resp. $\Pr_{\mathrm{Real}}[\mathrm{EV}]$) the probability of EV occurring in extended transcript τ_{ext}, where $\tau_{ext} \sim \mathrm{T}^{\mathrm{ext}}_{\mathrm{re}}$ (resp. $\tau_{ext} \sim \mathrm{T}^{\mathrm{ext}}_{\mathrm{id}}$).

Given the above, we present the following definitions: Let the advantage of an adversary $\mathcal{A}$ against the first-order output unpredictability of an RKD set Φ be defined as:

$$\mathrm{Adv}^{\mathrm{ou1}}_{\Phi,\mathrm{Ideal}}(\mathcal{A}) := \Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{ou1}}]; \quad \mathrm{Adv}^{\mathrm{ou1}}_{\Phi,\mathrm{Real}}(\mathcal{A}) := \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{ou1}}].$$

(Note that the above quantities will be the same, regardless of choice of $\mathcal{R}$.)

Similarly, let advantage of an adversary $\mathcal{A}$ against the (first order) claw-freeness of an RKD set Φ be defined as:

$$\begin{aligned}\mathrm{Adv}^{\mathrm{cf}}_{\Phi,\mathrm{Ideal}}(\mathcal{A}) &:= \Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{cf}}]; &\quad \mathrm{Adv}^{\mathrm{cf}}_{\Phi,\mathrm{Real}}(\mathcal{A}) &:= \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{cf}}].\\ \mathrm{Adv}^{\mathrm{cf1}}_{\Phi,\mathrm{Ideal}}(\mathcal{A}) &:= \Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{cf1}}]; &\quad \mathrm{Adv}^{\mathrm{cf1}}_{\Phi,\mathrm{Real}}(\mathcal{A}) &:= \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{cf1}}]\end{aligned}$$

(Note that the above quantities will be the same, regardless of choice of $\mathcal{R}$.)

We define the advantage of an adversary against the ordering of an RKD set Φ with reordering function $\mathcal{R}$ as:

$$\mathrm{Adv}^{\mathrm{ord}}_{\Phi,\mathrm{Ideal}}(\mathcal{A},\mathcal{R}) := \Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{ord}}]; \quad \mathrm{Adv}^{\mathrm{ord}}_{\Phi,\mathrm{Real}}(\mathcal{A},\mathcal{R}) := \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{ord}}].$$

Finally, note that regardless of the adversary $\mathcal{A}$ or the class Φ, we have that

$$\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{bp}}] \leq \frac{2m(q_e)^2}{N}; \quad \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{bp}}] = 0.$$

2.2 The Requirements on Φ of Farshim and Proctor

We introduce the following notation: $\sigma \in \{+,-\}$ and P_i^{σ} indicates a query to P_i in either the forward or backward direction. Farshim and Proctor presented the following requirements on RKD sets Φ and showed that the 4-round Even-Mansour construction is RKA-secure against RKD sets Φ that satisfy them.

First-Order Output Unpredictability. The advantage of an adversary $\mathcal{A}$ against the first-order output unpredictability of an RKD set Φ with access to t ideal permutations is defined via:

$$\mathrm{Adv}^{\mathrm{fp,ou1}}_{\Phi}(\mathcal{A}) := \Pr[\exists (i,\sigma,\phi,x,c) \in \mathsf{List} \text{ s.t. } P_i^{\sigma}(\phi(k)\oplus x)\oplus\phi(k) = c : \mathsf{List} \leftarrow \mathcal{A}^{\mathrm{P}}].$$

First-Order Claw-Freeness. The advantage of an adversary $\mathcal{A}$ against the (first-order) claw-freeness of an RKD set Φ with access to t ideal permutations is defined via:

$$\begin{aligned}\mathrm{Adv}^{\mathrm{fp,cf}}_{\Phi}(\mathcal{A}) &:= \Pr[\exists (i,\sigma,\phi_1,x_1,\phi_2,x_2) \in \mathsf{List} \text{ s.t. } \phi_1(k) = \phi_2(k) \wedge \phi_1 \neq \phi_2 : \mathsf{List} \leftarrow \mathcal{A}^{\mathrm{P}}].\\ \mathrm{Adv}^{\mathrm{fp,cf1}}_{\Phi}(\mathcal{A}) &:= \Pr[\exists (i,\sigma,\phi_1,x_1,\phi_2,x_2) \in \mathsf{List} \text{ s.t. } P_i^{\sigma}(\phi_1(k)\oplus x_1)\oplus\phi_1(k) = \\ &\qquad P_i^{\sigma}(\phi_2(k)\oplus x_2)\oplus\phi_2(k) \wedge \phi_1 \neq \phi_2 : \mathsf{List} \leftarrow \mathcal{A}^{\mathrm{P}}].\end{aligned}$$

First-Order Query Independence. The advantage of an adversary $\mathcal{A}$ against the first-order query independence of an RKD set Φ with access to t ideal permutations is defined via:

$$\mathrm{Adv}^{\mathrm{fp,qi1}}_{\Phi}(\mathcal{A}) := \Pr[\exists (i,\sigma,\phi_1,x_1,\phi_2) \in \mathsf{List} \text{ s.t. } (2, P_i^{\sigma}(\phi_1(k)\oplus x_1)\oplus\phi_1(k), \pm) \in \overline{\mathsf{Qry}}[\phi(k)] : \mathsf{List} \leftarrow \mathcal{A}^{\mathrm{P}}],$$

where

$$\begin{aligned}\mathsf{Qry}[\phi(k)] &:= \{(i,x,\sigma) : (i,x,\sigma) \text{ queried to P by } \phi(k)\},\\ \overline{\mathsf{Qry}}[\phi(k)] &:= \mathsf{Qry}[\phi(k)] \cup \{(i, P_i^{\sigma}(x), -\sigma) : (i,x,\sigma) \in \mathsf{Qry}[\phi(k)]\}.\end{aligned}$$

2.3 Comparison of our requirements on Φ with those of Farshim and Proctor

We claim that for the case of the 3-round Even-Mansour cipher with trivial key schedule, $\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{ou1}} \vee \mathrm{EV}_{\mathrm{cf}} \vee \mathrm{EV}_{\mathrm{cf1}} \vee \mathrm{EV}_{\mathrm{ord}}] \leq \mathrm{Adv}^{\mathrm{fp,ou1}}_{\Phi}(\mathcal{A}') + \mathrm{Adv}^{\mathrm{fp,cf}}_{\Phi}(\mathcal{A}') + \mathrm{Adv}^{\mathrm{fp,cf1}}_{\Phi}(\mathcal{A}') + \mathrm{Adv}^{\mathrm{fp,qi1}}_{\Phi}(\mathcal{A}')$. Where $\mathcal{A}, \mathcal{A}'$ make the same number of queries to P. As a first step in reconciling the two definitions, we present a transformation F which converts a transcript $\tau \sim \mathrm{T}_{\mathrm{id}}$ into a list List as in the definition of Farshim and Proctor. $F(\tau)$ does the following:

- For each $(\mathsf{RK}, \phi, x, y) \in \tau$, and each $(P_2, \perp, x', y') \in \tau$, we add tuples $(1, +, \phi, x, x')$, $(3, -, \phi, y, y')$ to List.
- For each pair $(\mathsf{RK}, \phi_1, x_1, y_1), (\mathsf{RK}, \phi_2, x_2, y_2) \in \tau$, $\phi_1 \neq \phi_2$, we add tuples $(1, +, \phi_1, x_1, \phi_2, x_2)$, $(3, -, \phi_1, y_1, \phi_2, y_2)$ to List.
- For each pair $(\mathsf{RK}, \phi_1, x_1, y_1, i), (\mathsf{RK}, \phi_2, x_2, y_2, j) \in \mathcal{R}(\tau)$, where $i \leq j$, we add tuples $(1, +, \phi_2, x_2, \phi_1), (3, -, \phi_2, y_2, \phi_1)$ to List.

Now, consider an adversary $\mathcal{A}$ and the distribution over transcripts τ_{ext} generated, conditioned on $\mathrm{EV_{cf}}$ not occurring. Assume the event $\mathrm{EV_{ou1}} \vee \mathrm{EV_{cf1}} \vee \mathrm{EV_{ord}}$ occurs with probability ρ_1, conditioned on $\mathrm{EV_{cf}}$ not occurring. We construct an adversary $\mathcal{A}'$ who gets access only to P such that $\mathrm{Adv}_{\Phi}^{\mathrm{fp,ou1}}(\mathcal{A}') + \mathrm{Adv}_{\Phi}^{\mathrm{fp,cf1}}(\mathcal{A}') + \mathrm{Adv}_{\Phi}^{\mathrm{fp,qi1}}(\mathcal{A}') \geq \rho_1$. $\mathcal{A}'$ runs $\mathcal{A}$ internally and receives queries from $\mathcal{A}$. $\mathcal{A}'$ forwards all of $\mathcal{A}$'s queries to P to its own oracle. When $\mathcal{A}$ queries RK with input $\phi \in \Phi$ and x or y, $\mathcal{A}'$ responds as follows: $\mathcal{A}'$ keeps a separate table for each distinct RKD function ϕ. Each table has a column for inputs x and outputs y and is filled in on the fly. At each moment $\mathcal{A}$ maintains the invariant that each table is consistent with some permutation (i.e. no two inputs map to the same output). When $\mathcal{A}$ queries RK with RKD function ϕ, $\mathcal{A}'$ completes the corresponding row of the corresponding table at random, conditioned on maintaining the invariant, and returns the response to $\mathcal{A}$. When $\mathcal{A}$ is done querying, $\mathcal{A}'$ receives a random key k and begins making the hidden queries with respect to P as specified by $\mathrm{T_{id}^{ext}}$. Note that the distribution induced by $\mathcal{A}'$ is identical to the distribution induced by $\tau_{ext} \sim \mathrm{T_{id}^{ext}}$, conditioned on $\mathrm{EV_{cf}}$ not occurring. So $\Pr_{\mathrm{Ideal}}[\mathrm{EV_{ou1}} \vee \mathrm{EV_{cf1}} \vee \mathrm{EV_{ord}}]$ is the same as the probability that one of these events occur in the simulation of $\mathcal{A}'$. Moreover, if $\mathrm{EV_{ou1}}$ (resp. $\mathrm{EV_{cf1}}, \mathrm{EV_{ord}}$) occurs during the simulation of $\mathcal{A}'$, then $F(\tau)$ contains a tuple (i, σ, ϕ, x, c) (resp. $(i, \sigma, \phi_1, x_1, \phi_2, x_2)$, $(i, \sigma, \phi_1, x_1, \phi_2)$) as in the definition of $\mathrm{Adv}_{\Phi}^{\mathrm{fp,ou1}}(\mathcal{A}')$ (resp. $\mathrm{Adv}_{\Phi}^{\mathrm{fp,cf1}}(\mathcal{A}')$, $\mathrm{Adv}_{\Phi}^{\mathrm{fp,qi1}}(\mathcal{A}')$).

Showing that $\Pr_{\mathrm{Ideal}}[\mathrm{EV_{cf}}] \leq \mathrm{Adv}_{\Phi}^{\mathrm{fp,cf}}(\mathcal{A}')$ follows similarly to the above: $\mathcal{A}'$ responds to queries of $\mathcal{A}$ as above. When $\mathcal{A}$ is done querying, $\mathcal{A}'$ receives a random key k and begins making *only* the hidden RKD queries with respect to P. The induced distribution over τ and hidden RKD queries differs from the correct distribution only in the case that $\mathcal{A}$ queried distinct ϕ_1, ϕ_2 such that $\phi_1(k) = \phi_2(k)$ (which causes the response forwarded to $\mathcal{A}$ to possibly be inconsistent with key k). But in this case, $\mathrm{EV_{cf}}$ has already occurred.

Note that it is possible that $\mathrm{Adv}_{\Phi}^{\mathrm{fp,qi1}}(\mathcal{A})$ is high for some adversary $\mathcal{A}$ making t queries, while for some $\mathcal{R}$, our event $\mathrm{EV_{ord}}$ still occurs with low probability for all adversaries $\mathcal{A}$ making the same number of queries. Indeed, in Section 4, we present a concrete class of RKD functions Φ for which Farshim and Proctor's notion of first-order query independence does not hold, but for which our techniques allow us to prove RKA-security of the three-round Even Mansour construction with respect to this class Φ. Specifically, for our concrete class Φ, we have that $\mathrm{Adv}_{\Phi}^{\mathrm{fp,qi1}} = 1$, and so the results of Farshim and Proctor do not even allow proving that the 4-round Even-Mansour cipher is secure against this RKD class. On the other hand, in our setting we show that for class Φ, there is a re-ordering function $\mathcal{R}$ such that $\Pr_{\mathrm{Ideal}}[\mathrm{EV_{ou1}} \vee \mathrm{EV_{cf}} \vee \mathrm{EV_{cf1}} \vee \mathrm{EV_{ord}}]$ is small even for the 3-round Even-Mansour cipher, which allows us to prove security of the 3-round Even-Mansour cipher against this class of RKD functions.

3 Main Results

Let $\mathcal{A}$ be an adversary making q_e, q_p queries to RK and each $P_i \in \mathrm{P}$, respectively, and let $\mathcal{R}$ be the re-ordering function used in the experiment. We define $\mathrm{EV_{good}} := \overline{\mathrm{EV_{ou1}}} \wedge \overline{\mathrm{EV_{cf}}} \wedge$

$\overline{\mathrm{EV}_{\mathrm{cf1}}} \wedge \overline{\mathrm{EV}_{\mathrm{ord}}}$ and $\mathrm{EV}^+_{\mathrm{good}} := \overline{\mathrm{EV}_{\mathrm{ou1}}} \wedge \overline{\mathrm{EV}_{\mathrm{cf}}} \wedge \overline{\mathrm{EV}_{\mathrm{cf1}}} \wedge \overline{\mathrm{EV}_{\mathrm{ord}}} \wedge \overline{\mathrm{EV}_{\mathrm{bp}}}$. Define $\mathrm{Adv}^{\mathrm{EV}}_{\Phi,\mathrm{Ideal}}(\mathcal{A},\mathcal{R}) := 1 - \Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}}]$ and $\mathrm{Adv}^{\mathrm{EV}}_{\Phi,\mathrm{Real}}(\mathcal{A},\mathcal{R}) := 1 - \Pr_{\mathrm{Real}}[\mathrm{EV}_{\mathrm{good}}] = 1 - \Pr_{\mathrm{Real}}[\mathrm{EV}^+_{\mathrm{good}}]$.

In this section, we prove our main Theorem:

Theorem 3.1. *Let q_e, q_p be positive integers, $N = 2^n$, and assume the trivial key-schedule. Let Φ^m_ρ be a class of RKD functions such that (1) every $\phi \in \Phi^m_\rho$ makes at most m queries to* P*; and (2) for all adversaries $\mathcal{A}$ making at most q_e queries to* RK *and q_p queries to each $P_i \in$* P*, $\min_{\mathcal{R}}[\mathrm{Adv}^{\mathrm{EV}}_{\Phi^m_\rho,\mathrm{Ideal}}(\mathcal{A},\mathcal{R})] \le \rho$. Then*

$$\mathrm{Adv}^{\Phi^{\mathrm{m}}_\rho}_{\mathrm{EM}[n,r]}(q_e,q_p) \le 2\rho + \frac{3m(q_e)^2}{N} + \frac{2(q_e)^2}{N} + \frac{q_e \cdot q_p}{N}.$$

To aid in the proof of Theorem 3.1, we introduce several claims, lemmas and corollaries.

The following claim can be verified by inspection of the distributions $\mathrm{T}^{\mathrm{ext}}_{\mathrm{id}}, \mathrm{T}^{\mathrm{ext}}_{\mathrm{re}}$.

Claim 3.2. *For every $\tau \in \mathcal{T}_{\mathrm{re}} \cup \mathcal{T}_{\mathrm{id}}$ (where $\mathcal{T}_{\mathrm{re}}$ and $\mathcal{T}_{\mathrm{id}}$, denote the supports of* T_{re} *and* T_{id}*, respectively),* $\Pr_{\mathrm{Real}}[\mathrm{EV}^+_{\mathrm{good}} \wedge \mathrm{T}_{\mathrm{re}} = \tau] > 0$ *if and only if* $\Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}} \wedge \mathrm{T}_{\mathrm{id}} = \tau] > 0$.

The following lemma follows from the fact that if $\mathrm{EV}_{\mathrm{cf}}$ occurs for a transcript $\tau \sim \mathrm{T}_{\mathrm{id}}$ then $\Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{id}} = \tau] = 0$, whereas if the event does not occur (with probability at least $1-\rho$), then the transcript contains q_e "fresh" calls to the ideal cipher.

Lemma 3.3. *For every τ such that* $\Pr[\mathrm{T}_{\mathrm{id}} = \tau \wedge \mathrm{EV}^+_{\mathrm{good}}] > 0$*,*

$$(1-\rho)\frac{\Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{id}} = \tau]}{N((N)_{q_p})^r N^{q_e}} \le \Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}} = \tau \wedge \mathrm{EV}^+_{\mathrm{good}}] \le \frac{\Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{id}} = \tau]}{N((N)_{q_p})^r (N)_{q_e}},$$

The following lemma is the main technical lemma in this section:

Lemma 3.4. *Let $M := q_e(m+1)$. For every $\tau \in \mathcal{T}_{\mathrm{re}}$,*

$$\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}} = \tau \wedge \mathrm{EV}^+_{\mathrm{good}}] = \Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{id}} = \tau] \cdot \frac{1}{N((N)_{q_p})^r (N - q_p - M + q_e)_{q_e}}.$$

Proof. We observe that

$$\Pr[T_{\mathrm{re}} = \tau \wedge \mathrm{EV}^+_{\mathrm{good}}] = \sum_{\tau_{ext} \vdash \tau \wedge \mathrm{EV}^+_{\mathrm{good}}} \Pr[T^{\mathrm{ext}}_{\mathrm{re}} = \tau_{\mathrm{ext}}].$$

To compute the above sum, we first calculate the exact probability of obtaining a particular extended transcript τ_{ext} and then multiply by the number of valid extensions $\tau_{ext} \vdash \tau$, in which $\mathrm{EV}^+_{\mathrm{good}}$ occurs.

In more detail: The probability that ${\mathrm{T}_{\mathrm{re}}}^{ext} = \tau_{ext}$ for a particular τ_{ext} is simply the probability of selecting the correct key k and, selecting each explicit query in τ to $P_1, \ldots, P_r$ and then selecting each "hidden" query to $P_1, \ldots, P_r$ during computation of RK queries (note this includes queries made to ϕ during the computation of the RKD function). Assume WLOG that τ_{ext} contains *exactly* $M = q_e(m+1)$ new queries to each of $P_1 \ldots, P_r$ that are not explicitly contained in τ. Thus, for any particular τ_{ext}, we have that

$$\Pr_{\mathrm{Real}}[{\mathrm{T}_{\mathrm{re}}}^{ext} = \tau_{ext}] = \frac{1}{N \cdot \big((N)_{q_p+M}\big)^r}. \tag{1}$$

Now, for a particular τ, we must compute the number of extended transcripts τ_{ext} such that (1) $\mathrm{EV}^{+}_{\mathrm{good}}$ holds and (2) τ_{ext} is consistent with τ. To do this, we present a mapping ψ_τ from a set $\mathcal{D}_\tau$ to the set of extended transcripts τ_{ext} such that (1) and (2) hold and show that this mapping is a *bijection*. Then, the size of $\mathcal{D}_\tau$ is exactly equal to the desired quantity.

We first define a set $\mathcal{D}'_\tau$, such that $\mathcal{D}_\tau \subseteq \mathcal{D}'_\tau$. $\mathcal{D}'_\tau$ consists of tuples of the form $(Q_{P_1}, \ldots, Q_{P_r})$. Each Q_{P_i} for $i \in [r], i \neq 2$, is a tuple of M values $(y^i_1, \ldots, y^i_M)$, where each $y^i_j \in [N - q_p - j + 1]$. Similarly, Q_{P_2} is a tuple of $M - q_e$ values $(y^2_1, \ldots, y^2_{M-q_e})$, where each $y^2_j \in [N - q_p - j + 1]$. Clearly,

$$|\mathcal{D}'| = ((N - q_p)_M)^{r-1}(N - q_p)_{M-q_e}. \tag{2}$$

Let ψ_τ be the following mapping:

The mapping $\psi_\tau(Q_{P_1}, \ldots, Q_{P_r})$

1. For each RK query in $\mathcal{R}(\tau)$, begin making hidden queries to $P_1, \ldots, P_r$, in order to recover a τ_{ext}, with the P_2 procedure (not during computation of $\phi(k)$) made *last*.
2. Hidden queries are answered in the following way: If the query already appears in τ, or has already been answered, answer as before. If the query is a query to P_2 during the encrypt/decrypt procedure, its answer is determined by previous queries. For all other queries, use the next value in the corresponding tuple $Q_{P_1}, \ldots, Q_{P_r}$ to answer the query.
3. If there are not enough values in Q_{P_2} to answer all the hidden queries, then output the lexicographically first response that has not been used yet.
4. If $\mathrm{EV}_{\mathrm{good}}$ occurs, ψ_τ outputs τ_{ext}. Otherwise, ψ_τ outputs $\perp$.

Let $\mathcal{D}_\tau \subseteq \mathcal{D}'_\tau$ be the set of tuples $(Q_{P_1}, \ldots, Q_{P_r})$ such that $\psi_\tau(Q_{P_1}, \ldots, Q_{P_r}) \neq \perp$.

We must now argue that ψ_τ is a bijection, i.e. *one-to-one* and *onto*. We show that ψ_τ has an inverse g such that: for τ_{ext} such that (1) and (2) hold, $\psi_\tau \circ g(\tau_{ext}) = \tau_{ext}$ and for $(Q_{P_1}, \ldots, Q_{P_r}) \in \mathcal{D}_\tau$, $g \circ \psi_\tau(Q_{P_1}, \ldots, Q_{P_r}) = (Q_{P_1}, \ldots, Q_{P_r})$. We define $g(\tau_{ext})$ in the following way: Derive τ from τ_{ext} and run $\mathcal{R}(\tau)$ to obtain a re-ordering of τ. Consider the hidden queries and responses made during RK oracle queries to $P_1, \ldots, P_r$ (as determined by τ_{ext}) occurring in a specific order. g will use these ordered responses to form tuples $(Q_{P_1}, \ldots, Q_{P_r})$ of the correct form. Note that this can always be done as long as at most $M - q_e$ number of queries to P_2 must be determined via Q_{P_2}, while the rest can be determined by τ and/or previous responses to queries to $P_1, \ldots, P_r$. In the following we show that for τ_{ext} such that (1) and (2) hold, this is indeed always the case.

First, since $\mathrm{EV}_{\mathrm{ou1}}$ and $\mathrm{EV}_{\mathrm{cf1}}$ do not occur occur, we have that exactly q_e distinct queries are made to P_2 during the encrypt/decrypt procedure inside an RK query. Moreover, since $\mathrm{EV}_{\mathrm{ord}}$ occurs, we have that these queries to P_2 occur *first* during the encrypt/decrypt procedure (although they may also occur later during a $\phi(k)$ computation). Thus, each time a query to P_2 is made during the encrypt/decrypt procedure, it will be entirely defined by τ and the previous queries made to $P_1, \ldots, P_r$ and so a fresh value from Q_{P_2} does not need to be used in order to respond to these q_e number of queries.

To see that for $(Q_{P_1}, \ldots, Q_{P_r}) \in \mathcal{D}_\tau$, $g \circ \psi_\tau(Q_{P_1}, \ldots, Q_{P_r}) = (Q_{P_1}, \ldots, Q_{P_r})$, we must show that for τ_{ext} such that (1) and (2) hold, there are always *at least* $M - q_e$ number of hidden queries to P_2 that are not determined by previous queries. This immediately follows from the fact that

τ_{ext} is defined in such a way that it always contains exactly M new hidden queries to each P_i (if less queries are made during the computation, then we simply add "dummy" queries to τ_{ext} at the end of the computation). Thus, given τ_{ext}, g returns the unique tuple $(Q_{P_1}, \ldots, Q_{P_r})$ consistent with this extended transcript.

Now, we have that

$$\frac{|\mathcal{D}_\tau|}{|\mathcal{D}'_\tau|} = \Pr_{\text{Ideal}}[\text{EV}^+_{\text{good}} \mid \text{T}_{\text{id}} = \tau], \tag{3}$$

since given $\mathcal{R}(\tau)$, each tuple $(Q_{P_1}, \ldots, Q_{P_r})$ corresponds to a set of oracles P, sampled conditioned on the q_p queries to each $P_1, \ldots, P_r$ contained in τ, whose responses match the first M responses from $P_1, P_3, \ldots, P_r$ and the first $M - q_e$ responses from P_2 generated during computation of $\psi_\tau(Q_{P_1}, \ldots, Q_{P_r})$. Moreover, the size of this set of oracles is the *same* for each tuple $(Q_{P_1}, \ldots, Q_{P_r})$ and the sets corresponding to two distinct tuples are *disjoint*. Therefore, we have

$$\begin{aligned}\Pr_{\text{Real}}[\text{T}_{\text{re}} = \tau \wedge \text{EV}^+_{\text{good}}] = \frac{|\mathcal{D}_\tau|}{N \cdot \left((N)_{q_p+M}\right)^r} &= \frac{|\mathcal{D}_\tau|}{|\mathcal{D}'_\tau|} \cdot \frac{|\mathcal{D}'_\tau|}{N \cdot \left((N)_{q_p+M}\right)^r} \\ &= \Pr_{\text{Ideal}}[\text{EV}^+_{\text{good}} \mid \text{T}_{\text{id}} = \tau] \cdot \frac{((N-q_p)_M)^{r-1}(N-q_p)_{M-q_e}}{N((N)_{q_p+M})^r} \\ &= \Pr_{\text{Ideal}}[\text{EV}^+_{\text{good}} \mid \text{T}_{\text{id}} = \tau] \cdot \frac{1}{N((N)_{q_p})^r(N-q_p-M+q_e)_{q_e}},\end{aligned}$$

where the first equality follows from (1) and the third equality follows from (2) and (3). □

The following corollary is immediate given Claim 3.2, Lemmas 3.3 and 3.4 and Fact 2.1.

Corollary 3.5. *For τ such that $\Pr_{\text{Real}}[\text{T}_{\text{re}} = \tau \wedge \text{EV}^+_{\text{good}}] > 0$ (which implies $\Pr_{\text{Ideal}}[\text{T}_{\text{id}} = \tau \wedge \text{EV}^+_{\text{good}}] > 0$) we have that*

$$\frac{\Pr_{\text{Ideal}}[\text{T}_{\text{id}} = \tau \wedge \text{EV}^+_{\text{good}}]}{\Pr_{\text{Real}}[\text{T}_{\text{re}} = \tau \wedge \text{EV}^+_{\text{good}}]} \geq \text{Val}_l; \qquad \frac{\Pr_{\text{Real}}[\text{T}_{\text{re}} = \tau \wedge \text{EV}^+_{\text{good}}]}{\Pr_{\text{Ideal}}[\text{T}_{\text{id}} = \tau \wedge \text{EV}^+_{\text{good}}]} \geq \text{Val}_u$$

where $\text{Val}_l = 1 - \frac{q_e(q_p+M)}{N} - \rho = 1 - \frac{q_e(q_p+(m+1)\cdot q_e)}{N} - \rho$ *and* $\text{Val}_u = 1 - \frac{(q_e)^2}{N}$.

The following lemma shows that if the probability of bad events occurring in the Ideal experiment, $\mathsf{Expt}^{\text{Ideal}}_{\mathcal{A},\mathcal{R}}$, is small, then the probability of bad events occurring in the Real experiment, $\mathsf{Expt}^{\text{Real}}_{\mathcal{A},\mathcal{R}}$, is also small.

Lemma 3.6. *If* $\text{Adv}^{\text{EV}}_{\Phi,\text{Ideal}}(\mathcal{A}, \mathcal{R}) \leq \rho$ *then* $\text{Adv}^{\text{EV}}_{\Phi,\text{Real}}(\mathcal{A}, \mathcal{R}) \leq \rho'$, *where* $\rho' = \rho + \frac{2m(q_e)^2}{N} + \frac{(q_e)^2}{N}$.

Proof. Recall that the assumption of Lemma 3.6 implies that $\Pr_{\text{Ideal}}[\text{EV}^+_{\text{good}}] \geq 1 - \rho - \frac{2m(q_e)^2}{N}$. We would like to prove that $\Pr_{\text{Real}}[\text{EV}^+_{\text{good}}] \geq 1 - \rho'$, which immediately implies the conclusion of Lemma 3.6. We have the following sequence of equations and inequalities:

$$\begin{aligned}
\Pr_{\mathrm{Real}}[\mathrm{EV}^+_{\mathrm{good}}] &= \sum_{\tau:\Pr_{\mathrm{Real}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]>0} \Pr_{\mathrm{Real}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}] \\
&= \sum_{\tau:\Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]>0} \Pr_{\mathrm{Real}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}] \qquad (4) \\
&= \sum_{\tau:\Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]>0} \Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\cdot\frac{\Pr_{\mathrm{Real}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]}{\Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]} \\
&\geq \mathrm{Val}_u\cdot\sum_{\tau:\Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]>0} \Pr_{\mathrm{Ideal}}[\tau\wedge\mathrm{EV}^+_{\mathrm{good}}] \qquad (5) \\
&= \mathrm{Val}_u\cdot\Pr_{\mathrm{Ideal}}[\mathrm{EV}^+_{\mathrm{good}}] \\
&\geq \mathrm{Val}_u\cdot(1-\rho-\frac{2m(q_e)^2}{N}) \qquad (6) \\
&\geq 1-(\rho+\frac{(q_e)^2}{N}+\frac{2m(q_e)^2}{N}).
\end{aligned}$$

where (4) follows from Claim 3.2, (5) from Corollary 3.5 and (6) from the hypothesis. □

We are now ready to complete the proof of Theorem 3.1.

Proof of Theorem 3.1. Fix an adversary $\mathcal{A}$ making q_e, q_p queries to RK and each $P_i \in \mathrm{P}$ respectively. Let $\mathcal{R}$ be a re-ordering function at which $\mathrm{Adv}^{\mathrm{EV}}_{\Phi^m_\rho,\mathrm{Ideal}}(\mathcal{A},\mathcal{R})$ attains its minimum. We upper bound the statistical distance between $\mathrm{T}_{\mathrm{re}}, \mathrm{T}_{\mathrm{id}}$, which upper bounds $\mathrm{Adv}^{\Phi^{\mathrm{m}}_\rho}_{\mathrm{EM}[n,r]}(q_e,q_p)$.

$$\begin{aligned}
\Delta(\mathrm{T}_{\mathrm{re}},\mathrm{T}_{\mathrm{id}}) &= \sum_{\tau,\Pr[\mathrm{T}_{\mathrm{re}}=\tau]>\Pr[\mathrm{T}_{\mathrm{id}}=\tau]} (\Pr[\mathrm{T}_{\mathrm{re}}=\tau]-\Pr[\mathrm{T}_{\mathrm{id}}=\tau]) \\
&= \sum_{\tau:\Pr[\mathrm{T}_{\mathrm{re}}=\tau]>\Pr[\mathrm{T}_{\mathrm{id}}=\tau]} \Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]+\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\overline{\mathrm{EV}^+_{\mathrm{good}}}] \\
&\qquad -\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]-\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\overline{\mathrm{EV}^+_{\mathrm{good}}}] \\
&\leq \sum_{\tau}\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\overline{\mathrm{EV}^+_{\mathrm{good}}}]+\sum_{\substack{\tau:\Pr[\mathrm{T}_{\mathrm{re}}=\tau]\\>\Pr[\mathrm{T}_{\mathrm{id}}=\tau]}}\left(\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]-\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\right) \\
&= \Pr_{\mathrm{Real}}[\overline{\mathrm{EV}^+_{\mathrm{good}}}]+\sum_{\substack{\tau:\Pr[\mathrm{T}_{\mathrm{re}}=\tau]\\>\Pr[\mathrm{T}_{\mathrm{id}}=\tau]}}\left(\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]-\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\right) \\
&\leq \rho'+\sum_{\substack{\tau:\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\\>\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]}}\left(\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]-\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\right) \qquad (7) \\
&= \rho'+\sum_{\substack{\tau:\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\\>\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]}}\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]\left(1-\frac{\Pr_{\mathrm{Ideal}}[\mathrm{T}_{\mathrm{id}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]}{\Pr_{\mathrm{Real}}[\mathrm{T}_{\mathrm{re}}=\tau\wedge\mathrm{EV}^+_{\mathrm{good}}]}\right) \\
&\leq \rho'+(1-\mathrm{Val}_l) \qquad (8) \\
&= 2\rho+\frac{2m(q_e)^2}{N}+\frac{(q_e)^2}{N}+\frac{q_e(q_p+(m+1)\cdot q_e)}{N}.
\end{aligned}$$

where (7) follows from Lemma 3.6 and (8) follows from Corollary 3.5. □

4 A new RKD class Φ

In this section, we define a new RKD class Φ and show that the 2-round Even-Mansour cipher is secure against related-key attacks restricted to Φ. It can be checked by inspection that Φ does not satisfy the requirements on RKD classes as required by Farshim and Proctor. Nevertheless, Φ fulfills the requirements of our result in the previous section.

Theorem 4.1. *Let $N = 2^n$, q_e, q_p be positive integers, I the identity function, and Φ the RKD set such that*

$$\Phi = \begin{cases} \phi_\Delta, & \Delta \in \{0,1\}^n \\ I \end{cases}$$

where $\phi_\Delta(k) := P_2(P_1(k \oplus \Delta) \oplus k) \oplus P_1(k \oplus \Delta)$. Then

$$\mathrm{Adv}^{\Phi}_{\mathrm{EM}[n,2]}(q_e, q_p) \leq \frac{13(q_e)^2}{N} + \frac{9q_e \cdot q_p}{N} + \frac{4(q_e)^2 \cdot q_p}{N} + \frac{8(q_e)^3}{N}.$$

It will be assumed, without loss of generality, that for each query of the form $(\mathsf{RK}, \phi_\Delta, x, y) \in \tau$, there is a corresponding query $(\mathsf{RK}, I, \Delta, y) \in \tau$, and vice versa. Given this assumption, $\phi_\Delta(k)$ can also be expressed as $c_\Delta \oplus P_1(k \oplus \Delta)$ where c_Δ is a constant determined by the transcript. Specifically, for each Δ such that there is a corresponding query $(\mathsf{RK}, I, \Delta, y) \in \tau$, $c_\Delta := P_2(P_1(k \oplus \Delta) \oplus k)$. Note that given $(\mathsf{RK}, I, \Delta, y)$ and the key k (which are both contained in the transcript), $c_\Delta = y \oplus k$ can be derived. We also assume without loss of generality, that for each RK query with RKD function ϕ (where $\phi = \phi_\Delta$ or $\phi = I$) there is a corresponding RK query with the same RKD function ϕ and x or y set to 0.

By Theorem 3.1, we have that in order to prove Theorem 4.1, it is sufficient to define a re-ordering function $\mathcal{R}$ and to upperbound $\mathrm{Adv}^{\mathrm{EV}}_{\Phi^m_\rho,\mathrm{Ideal}}(\mathcal{A}, \mathcal{R}) \leq \rho$, where $\rho = \rho_1 + \rho_2 = \frac{2q_e q_p}{N} + \frac{q_e(2q_p + q_e + 2q_e q_p + 4{q_e}^2)}{N} = \frac{q_e(4q_p + q_e + 2q_e q_p + 4{q_e}^2)}{N}$, or equivalently lowerbound $\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}}] \geq 1 - \rho$. In particular, we will define a set $\mathcal{T}_{\mathrm{bad}}$ and show that (1) probability over choice of transcript that $\tau \in \mathcal{T}_{\mathrm{bad}}$ is at most ρ_1; (2) For each $\tau \notin \mathcal{T}_{\mathrm{bad}}$, we have $\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{id}} = \tau] \geq 1 - \rho_2$. Thus, $\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}}] \geq 1 - (\rho_1 + \rho_2)$ and so $\mathrm{Adv}^{\mathrm{EV}}_{\Phi^m_\rho,\mathrm{Ideal}}(\mathcal{A}, \mathcal{R}) \leq \rho_1 + \rho_2 = \rho$.

Definition 4.2 (Bad Transcripts)**.** *Let $\tau = (\mathcal{S}_\tau,\ k)$ be an attainable transcript. k is bad if*

$$k \in \mathsf{BadK} = \bigcup_{1 \leq i \leq 2} \mathsf{BadK_i}$$

where:

$$k \in \mathsf{BadK}_1 \Leftrightarrow \exists(\mathsf{RK}, I, x, y) \in \tau \textit{ and } (P_1, \perp, u_1, v_1) \in \tau \textit{such that } k \oplus x = u_1$$

$$k \in \mathsf{BadK}_2 \Leftrightarrow \exists(\mathsf{RK}, I, x, y) \in \tau \textit{ and } (P_2, \perp, u_2, v_2) \in \tau \textit{such that } k \oplus y = v_2$$

Otherwise, k is good. $\mathcal{T}_{\mathrm{bad}}$ is the set of transcripts $\tau = (\mathcal{S}_\tau,\ k)$, such that $k \in \mathsf{BadK}$ and $\mathcal{T}_{\mathrm{good}} = \mathcal{T} \setminus \mathcal{T}_{\mathrm{bad}}$ is the set of good transcripts.

The following lemma upper bounds the probability of getting a bad transcript in the ideal world.

Lemma 4.3.

$$\Pr[T_{\mathrm{id}} \in \mathcal{T}_{\mathrm{bad}}] \leq \rho_1,$$

where $\rho_1 = \frac{2q_eq_p}{N}$.

Proof. Since this is the ideal case, the key k is drawn uniformly at the end of every query phase. Therefore, only an upper bound is needed of the possible bad values for k for every attainable query transcript $\mathcal{S}_\tau$. Fix a query transcript $\mathcal{S}_\tau$. For every distinct (RK, I, x, y) $\in \tau$ and every ($P_1, \perp$, u_1, v_1) $\in \tau$, there is exactly one key k such that $k \oplus x = u_1$. Similarly, for every distinct (RK, I, x, y) $\in \tau$ and every ($P_2, \perp$, u_2, v_2) $\in \tau$, there is exactly one key k such that $k \oplus y = v_2$. Hence, $|\mathsf{BadK}_1| \leq q_eq_p$. Similarly, $|\mathsf{BadK}_2| \leq q_eq_p$. Hence,

$$\Pr[k \leftarrow \{0,1\}^n : k \in \mathsf{BadK_i}, i = 1,2] \leq \frac{q_eq_p}{N}$$

The lemma follows. □

We next lowerbound the probability of $\mathrm{EV}_{\mathrm{good}}$ occurring in the Ideal experiment conditioned on $\mathrm{T}_{\mathrm{re}} = \tau$ and $\tau \in \mathcal{T}_{\mathrm{good}}$.

Lemma 4.4. *Let* $\tau \in \mathcal{T}_{\mathrm{good}}$. *Then*

$$\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{re}} = \tau] \geq 1 - \rho_2,$$

where $\rho_2 = \frac{q_e(2q_p + q_e + 2q_eq_p + 4{q_e}^2)}{N}$.

Proof. Let

$$U_1 = \{u_1 \in \{0,1\}^n : (P_1, \perp, u_1, v_1) \in \tau\}, \qquad V_1 = \{v_1 \in \{0,1\}^n : (P_1, \perp, u_1, v_1) \in \tau\}$$

$$U_2 = \{u_2 \in \{0,1\}^n : (P_2, \perp, u_2, v_2) \in \tau\}, \qquad V_2 = \{v_2 \in \{0,1\}^n : (P_2, \perp, u_2, v_2) \in \tau\}$$

denote the sets of queries and responses made by the adversary to P_1 and P_2, respectively.

We begin by defining the re-ordering function $\mathcal{R}$ which does the following: $\mathcal{R}(\tau)$ re-orders the queries in $\mathcal{S}_\tau$ so that the set of queries to RK with RKD function $\phi = I$ precedes the set of queries to RK with RKD function $\phi = \phi_\Delta$.
For $u' \in \{0,1\}^n$, let $X(u') = \{(\mathsf{RK}, I, \Delta, y) \in \tau : k \oplus \Delta = u'\}$, and let $U' = \{u' \in \{0,1\}^n : X(u') \neq \emptyset\}$. For $u'' \in \{0,1\}^n$, let $X(u'') = \{(\mathsf{RK}, \Delta, x, y) \in \tau : \phi_\Delta(k) \oplus x = u''\}$, and let $U'' = \{u'' \in \{0,1\}^n : X(u'') \neq \emptyset\}$. By definition of a good transcript, $U \cap U' = \emptyset$. One can denote

$$U' = \{u'_{\Delta_1}, \ldots, u'_{\Delta_\mu}\} \text{ and}$$

$$U'' = \{u''_{\Delta_1,1}, \ldots, u''_{\Delta_1,q_1}, \ldots, u''_{\Delta_\mu,1}, \ldots, u''_{\Delta_\mu,q_\mu}\}.$$

Also let

$$\alpha = \sum_{i=1}^{\mu}\left(\left|X(u'_{\Delta_i})\right| + \sum_{j=1}^{q_i}\left|X(u''_{\Delta_{i,j}})\right|\right). \tag{9}$$

It is now sufficient to lower bound the number of possible tuples of values $(v'_{\Delta_1}, \ldots, v'_{\Delta_\mu})$ and $(v''_{\Delta_1,1}, \ldots, v''_{\Delta_1,q_1}, \ldots, v''_{\Delta_m,1}, \ldots, v''_{\Delta_\mu,q_\mu})$ such that event $\mathrm{EV}_{\mathrm{good}}$ occurs.

In the following, $x_{\Delta_i,j}$ (resp. x_{Δ_i}) denotes the x-value of the j-th query that uses the RKD function ϕ_{Δ_i} (resp. the x-value of the i-th query that uses RKD function I), and $y_{\Delta_i,j}$ (resp. y_{Δ_i}) denotes the y-value of the j-th query that uses RKD function ϕ_{Δ_i} (resp. the y-value of the i-th query that uses RKD function I). We argue that if the following conditions are met then the event $\mathrm{EV}_{\mathrm{good}}$ occurs where $\mathrm{EV}_{\mathrm{good}} = \overline{\mathrm{EV}_{\mathrm{ou1}}} \wedge \overline{\mathrm{EV}_{\mathrm{cf1}}} \wedge \overline{\mathrm{EV}_{\mathrm{ord}}}$.
For $v'_{\Delta_i}, i \in [\mu]$:

(1-1) $v'_{\Delta_i} \neq v_1$ for all $v_1 \in V_1$.

(1-2) $v'_{\Delta_i} \neq u_2 \oplus k$ for all $u_2 \in U_2$.

(1-3) $v'_{\Delta_i} \neq v'_{\Delta_j}$ for all $j < i$.

(2-1) $v'_{\Delta_i} \neq c_{\Delta_i} \oplus x_{\Delta_i,j} \oplus u_1$ for all $j \in [q_i]$, $u_1 \in U_1$.

(2-2) $v'_{\Delta_i} \neq c_{\Delta_i} \oplus y_{\Delta_i,j} \oplus v_2$ for all $j \in [q_i]$, $v_2 \in V_2$.

(3-1) $v'_{\Delta_i} \neq c_{\Delta_i} \oplus x_{\Delta_i,j} \oplus u'_{\Delta_\ell}$ for all $j \in [q_i]$ and $\ell < i$.

(3-2) $v'_{\Delta_i} \neq k \oplus y_{\Delta_\ell} \oplus c_{\Delta_i} \oplus y_{\Delta_i,j}$ for all $j \in [q_i]$ and $\ell < i$.

(4-1) $v'_{\Delta_i} \neq c_{\Delta_i} \oplus x_{\Delta_i,j} \oplus c_{\Delta_\ell} \oplus v'_{\Delta_\ell} \oplus x_{\Delta_\ell,w}$ for all $j \in [q_i]$, $w \in [q_\ell]$ and $\ell < i$.

(4-2) $v'_{\Delta_i} \neq c_{\Delta_i} \oplus y_{\Delta,i,j} \oplus c_{\Delta_\ell} \oplus v'_{\Delta_\ell} \oplus y_{\Delta_\ell,w}$ for all $j \in [q_i]$, $w \in [q_\ell]$ and $\ell < i$.

For $v''_{\Delta_i,j}, i \in [\mu], j \in [q_i]$:

(5-1) $v''_{\Delta_i,j} \neq v_1$ for all $v_1 \in V_1$.

(5-2) $v''_{\Delta_i,j} \neq v'_{\Delta_\ell}$ for all $\ell \in [\mu]$.

(5-3) $v''_{\Delta_i,j} \neq v''_{\Delta_\ell,w}$ for all $(\ell||w) < (i||j)$.

(6-1) $v''_{\Delta_i,j} \neq v'_{\Delta_i} \oplus c_{\Delta_i} \oplus u_2$ for all $u_2 \in U_2$.

(7-1) $v''_{\Delta_i,j} \neq v'_{\Delta_\ell} \oplus k \oplus v'_{\Delta_i} \oplus c_{\Delta_i}$ for all $\ell \in [\mu]$.

(8-1) $v''_{\Delta_i,j} \neq c_{\Delta_i} \oplus v'_{\Delta_i} \oplus v''_{\Delta_\ell,w} \oplus c_{\Delta_\ell} \oplus v'_{\Delta_\ell}$ for all $j \in [q_i], w \in [q_\ell]$ and $\ell < i$.

Note that:

- Conditions (1-1), (1-3), (5-1), (5-2), (5-3) are required to ensure that $(v'_{\Delta_1}, \ldots, v'_{\Delta_\mu})$, $(v''_{\Delta_1,1}, \ldots, v''_{\Delta_1,q_1}, \ldots, v''_{\Delta_\mu,1}, \ldots, v''_{\Delta_\mu,q_\mu})$ are a valid sequence of outputs.
- Conditions (2-1), (3-1), (4-1) are required to ensure that $(u''_{\Delta_1,1}, \ldots, u''_{\Delta_1,q_1}, \ldots, u''_{\Delta_\mu,1}, \ldots, u''_{\Delta_\mu,q_\mu})$ are pairwise distinct and distinct from $(u'_{\Delta_1}, \ldots, u'_{\Delta_\mu})$, $u_1 \in U_1$. (Note that $(u'_{\Delta_1}, \ldots, u'_{\Delta_\mu})$ are pairwise distinct by definition and distinct from $u_1 \in U_1$ since $\tau \in \mathcal{T}_{\mathrm{good}}$.)
- Conditions (1-2), (2-2), (6-1) are required to ensure $\overline{\mathrm{EV}_{\mathrm{ou1}}}$.
- Conditions (3-2), (4-2), (7-1), (8-1) are required to ensure $\overline{\mathrm{EV}_{\mathrm{cf1}}}$.
- $\overline{\mathrm{EV}_{\mathrm{ord}}}$ is ensured since each $\phi_{\Delta_i}(k)$ makes only a single P_2 query, $P_2(v'_{\Delta_i} \oplus k)$, and this query must have already been made during the encryption procedure of RK query (I, Δ_i).

Additionally, note that the above conditions ensure that $\left|X(u''_{\Delta_i,j})\right| = 1$, and so $q_e = \alpha$. Let N_1 denote the number of tuples of pairwise distinct values $\{v'_{\Delta_1}, \ldots, v'_{\Delta_\mu}\}$ such that conditions 1 through 4 are satisfied. Let N_2 denote the number of tuples of pairwise distinct values $\{v''_{\Delta_1,1}, \ldots, v''_{\Delta_1,q_1}, \ldots, v''_{\Delta_\mu,1}, \ldots, v''_{\Delta_\mu,q_\mu}\}$ such that conditions 5 through 8 are satisfied. One has:

$$
\begin{aligned}
N_1 &\geq \prod_{i=1}^{\mu}(N - q_p - q_p - i + 1 - q_i q_p - q_i q_p - q_i(i-1) - q_i(i-1) - q_i \sum_{\ell=1}^{i-1} q_\ell - q_i \sum_{\ell=1}^{i-1} q_\ell) \\
&\geq \prod_{i=1}^{\mu}(N - 2q_p - \mu - 2q_e q_p - 2q_e \mu - 2{q_e}^2) \\
&\geq \prod_{i=1}^{\mu}(N - 2q_p - q_e - 2q_e q_p - 4{q_e}^2)
\end{aligned}
$$

where the second to last line follows from (9) and the last line follows since $\mu \leq q_e$.

And

$$
\begin{aligned}
N_2 &\geq \prod_{i\in[\mu], j\in[q_i]} (N - q_p - \mu - j - 1 - \sum_{\ell=1}^{i-1} q_\ell - q_p - \mu - q_i \sum_{\ell=1}^{i-1} q_\ell) \\
&\geq \prod_{i=1}^{\alpha-\mu} (N - 2q_p - 2\mu - q_e^2) \\
&\geq \prod_{i=1}^{q_e-\mu} (N - 2q_p - 2q_e - q_e^2)
\end{aligned}
$$

Finally, we compute the following lower bound on $\frac{N_1 \cdot N_2}{(N-q_p)_{q_e}}$, which gives a lower bound on $\Pr_{\mathrm{Ideal}}[\mathrm{EV}_{\mathrm{good}} \mid \mathrm{T}_{\mathrm{re}} = \tau]$:

$$
\begin{aligned}
\frac{N_1 \cdot N_2}{(N-q_p)_{q_e}} &\geq \frac{(N - 2q_p - q_e - 2q_e q_p - 4{q_e}^2)^{q_e}}{N^{q_e}} \\
&\geq 1 - \frac{q_e(2q_p + q_e + 2q_e q_p + 4{q_e}^2)}{N},
\end{aligned}
$$

where the second inequality follows from Fact 2.1. □

References

[1] Martin R. Albrecht, Pooya Farshim, Kenneth G. Paterson, and Gaven J. Watson. On cipher-dependent related-key attacks in the ideal-cipher model. In Antoine Joux, editor, *Fast Software Encryption – FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 128–145. Springer, Heidelberg, February 2011.

[2] Mihir Bellare and David Cash. Pseudorandom functions and permutations provably secure against related-key attacks. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 666–684. Springer, Heidelberg, August 2010.

[3] Mihir Bellare, David Cash, and Rachel Miller. Cryptography secure against related-key attacks and tampering. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 486–503. Springer, Heidelberg, December 2011.

[4] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 491–506. Springer, Heidelberg, May 2003.

[5] Eli Biham. New types of cryptanalytic attacks using related keys. *Journal of Cryptology*, 7(4):229–246, 1994.

[6] Eli Biham. New types of cryptoanalytic attacks using related keys (extended abstract). In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 398–409. Springer, Heidelberg, May 1994.

[7] Benoit Cogliati and Yannick Seurin. On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 584–613. Springer, Heidelberg, April 2015.

[8] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even-Mansour scheme revisited. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, Heidelberg, April 2012.

[9] EMVCo. Emv integrated circuit card specifications for payment systems. Book 2, Security and Key Management, June 2008. Version 4.2.

[10] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology – ASIACRYPT'91*, volume 739 of *Lecture Notes in Computer Science*, pages 210–224. Springer, Heidelberg, November 1993.

[11] Pooya Farshim and Gordon Procter. The related-key security of iterated Even-Mansour ciphers. In Gregor Leander, editor, *Fast Software Encryption – FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 342–363. Springer, Heidelberg, March 2015.

[12] Tetsu Iwata and Tadayoshi Kohno. New security proofs for the 3GPP confidentiality and integrity algorithms. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption – FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 427–445. Springer, Heidelberg, February 2004.

[13] Lars R. Knudsen. Cryptanalysis of LOKI91. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology – AUSCRYPT'92*, volume 718 of *Lecture Notes in Computer Science*, pages 196–208. Springer, Heidelberg, December 1993.

[14] Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008: 15th Annual International Workshop on Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, Heidelberg, August 2009.