IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2020, No. 4, pp. 71–87. DOI:10.46586/tosc.v2020.i4.71-87

Forking Tweakable Even-Mansour Ciphers

Hwigyeom Kim, Yeongmin Lee and Jooyoung Lee

Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea
{buddha93,dudals4780,hicalf}@kaist.ac.kr

Abstract. A forkcipher is a keyed, tweakable function mapping an n-bit input to a $2n$-bit output, which is equivalent to concatenating two outputs from two permutations. A forkcipher can be a useful primitive to design authenticated encryption schemes for short messages. A forkcpher is typically designed within the *iterate-fork-iterate* (IFI) paradigm, while the provable security of such a construction has not been widely explored.
In this paper, we propose a method of constructing a forkcipher using public permutations as its building primitives. It can be seen as applying the IFI paradigm to the tweakable Even-Mansour ciphers. So our construction is dubbed the *forked tweakable Even-Mansour* (FTEM) cipher. Our main result is to prove that a $(1, 1)$-round FTEM cipher (applying a single-round TEM to a plaintext, followed by two independent copies of a single-round TEM) is secure up to $2^{\frac{2n}{3}}$ queries in the ideal permutation model.

Keywords: Forkcipher · tweakable block cipher · indistinguishability · Even-Mansour cipher

1 Introduction

Forkciper. Authenticated encryption (AE) aims at achieving the two fundamental security goals of symmetric key cryptography; it simultaneously assures the confidentiality and authenticity of data. With a significant amount of research in this area, we now have a rich set of general-purpose AE schemes, some already standardized (e.g., GCM and CCM) and some expected to be adopted by new applications and standards (e.g., the CAESAR finalists Ascon [DEMS16], ACORN [Wu16], AEGIS-128 [WP16], OCB [KR16], COLM [ABD+16], Deoxys II [JNPS16], and MORUS [WH16]). However, research efforts are still needed in AE, in particular, for high-performance and low-latency processing of short messages. With this motivation, a new primitive, dubbed a *forkcipher*, has been proposed by Andreeva et. al. [ALP+19]; a forkcipher is a new type of cipher that maps an n-bit input message to an $2n$-bit output. When the left or right half of the output is truncated, one obtains an n-bit permutation. Intuitively, this is equivalent to evaluating two independent (tweakable) permutations. To obtain a forkcipher, they proposed the *iterate-fork-iterate* (IFI) paradigm; for some r_1 and r_2, a plaintext is encrypted by r_1 rounds of the cipher. Then, the output "forks" along two parallel paths with r_2 rounds. A half of the output can be seen as a ciphertext while the other half can be used to authenticate the message. So it might be faster than existing block cipher-based authenticated encryption modes, in particular, for short messages. They also proposed a dedicated forkcipher ForkSkinny by applying the IFI paradigm to the tweakable block cipher Skinny [BJK+16].

In [ALP+19], they proposed a straightforward way of constructing a forkcipher using a secure tweakable block cipher TBC as its building primitive, namely,

$$\mathsf{TBC}(k, t_1, \mathsf{TBC}(k, t_0, \cdot))||\mathsf{TBC}(k, t_2, \mathsf{TBC}(k, t_0, \cdot))$$

Received: 2020-06-01 Revised: 2020-09-01 Accepted: 2020-11-01 Published: 2020-12-10

for a secret key k and three independent tweaks t_0, t_1, t_2. If TBC is modeled as an ideal tweakable permutation, then the three tweaked permutations will behave like independent secret random permutations, say p_0, p_1, p_2, where $p_1(p(\cdot))||p_2(p(\cdot))$ will be perfectly secure, namely, the concatenation of two independent random permutations.

In this paper, we weaken the ingredients by using three public permutations, where all parties have access to the underlying primitives; we will propose a way of constructing a forkcipher on top of random permutations, and study its provable security in the ideal permutation model. This can be seen as the first step in making the model analyzed in provable security fashion more faithful to an actual iterate-fork-iterate instance, such as ForkSkinny. This approach is also akin to the corpus of work that investigate generic security of various cryptographic constructions such as key alternating ciphers, Feistel ciphers, and so on.

(Tweakable) Iterated Even-Mansour Ciphers. The iterated Even-Mansour (EM) construction [EM97, DR02] is one of the simplest block cipher constructions, abstracting substitution-permutation ciphers. The Even-Mansour construction based on an n-bit permutation P encrypts an n-bit plaintext x with two n-bit keys k and k' by computing

$$\mathsf{EM}[P]((k,k'),x) = k' \oplus P(k \oplus x).$$

It has been proved that EM is secure up to the birthday bound [EM97]. Moreover, its r-round variant is proved to be secure up to $2^{rn/(r+1)}$ queries [CS14].

Cogliati *et al.* [CS15] proposed to tweak EM, and the resulting tweakable cipher is called the tweakable Even-Mansour (TEM) cipher. This construction uses a family of hash functions, where each round key k of EM is replaced by $h(t)$ for a tweak t and a hash key h. They proved that a 2-round TEM is secure up to $2^{\frac{2n}{3}}$ queries when the underlying permutations and the round hash keys are all independent.

1.1 Our Contribution

In this paper, we propose to fork an r-round TEM. Our construction, dubbed FTEM, is parameterized by r_1 and r_2 such that $r_1 + r_2 = r$; an (r_1, r_2)-round FTEM encrypts a plaintext using an r_1-round TEM cipher and the resulting output is encrypted by two independent r_2-round TEM ciphers. In this paper, we focus on a $(1,1)$-round FTEM that encrypts an n-bit plaintext x with key $\mathbf{h} = (h_1, h_2, h_3) \in \mathcal{H}^3$ and tweak t by computing

$$h_2(t) \oplus P_2^{-1}(h_1(t) \oplus h_2(t) \oplus P_1(x \oplus h_1(t)))||h_3(t) \oplus P_3^{-1}(h_1(t) \oplus h_3(t) \oplus P_1(x \oplus h_1(t))),$$

where P_1, P_2, P_3 are n-bit permutations, and $\mathcal{H}$ is a family of hash functions (see Figure 1).

As the main contribution of this paper, we prove that, when $\mathcal{H}$ is a uniform δ-almost XOR-universal family of functions, the distinguishing advantage of any adversary making p primitive queries and q construction queries is upper bounded by

$$\mathcal{O}\left(\delta q^{\frac{3}{2}} + \frac{p\sqrt{q}}{2^n}\right).$$

So, when δ is close to $1/2^n$, a $(1,1)$-round FTEM is secure up to $2^{\frac{2n}{3}}$ adversarial queries in the random permutation model (assuming $p = q$). However, from a practical point of view, one should carefully interpret this bound since p and q, which represent offline and online complexity respectively, may be unbalanced; for example, when FTEM is instantiated with a lightweight permutation with $n = 80$, and when p is as high as 2^{64}, q has to be kept much smaller than 2^{32}.

Proof Technique. It is straightforward to prove the security of a $(1,1)$-round FTEM up to the birthday bound since the three underlying 1-round Even-Mansour ciphers will

behave like independent random permutations in the multi-key setting. In order to prove beyond-birthday security, we moved one step further by extending the security proof of the two-round TEM ciphers (with the standard H-coefficient technique).

For simplicity of proof, we assume that an adversary is given an additional primitive query for free whenever two construction queries make a collision at the input to the underlying permutation. Then we upper bound the probability of two collisions made by three queries. Without such "bad" events, one can prove that the probabilities of obtaining a good transcript are close in the real and in the ideal world.

By taking only a half of the output from a $(1,1)$-round FTEM, one immediately obtains a two-round TEM. Therefore, our result implies that forking does not dilute the security of a two-round TEM, while improving performance by doubling its output size. Besides providing theoretical insights on forkciphers, our result also has a practical interest in the context of permutation-based cryptography. For example, if our construction is instantiated with the Keccak permutation [BDPA09] or with Gimli [BKL+17], then we obtain a wide forkcipher with a huge message space, while achieving provable security beyond the birthday bound.

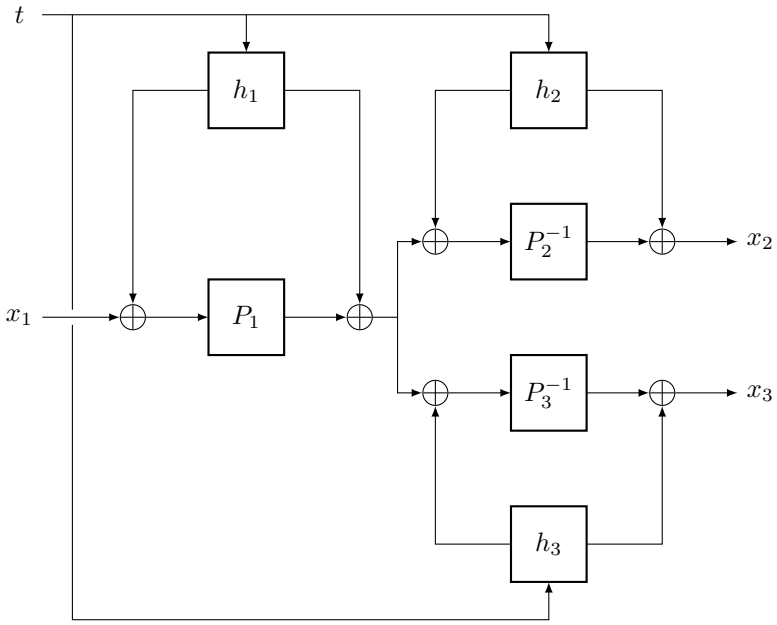

Figure 1: Tweakable Even-Mansour forkcipher of (1,1)-round, based on public permutations P_1, P_2, P_3 and hash functions h_1, h_2, h_3.

2 Preliminaries

2.1 Notation

In all of the following, we fix a positive integer n such that $n \geq 3$, and write $N = 2^n$. For a positive integer q, we write $[q] = \{1, \ldots, q\}$.

Given a non-empty finite set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$, and the set of all permutations of $\mathcal{X}$ is denoted $\mathsf{Perm}(\mathcal{X})$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. The set of all sequences that consist of b pairwise distinct elements of $\mathcal{X}$ is denoted $\mathcal{X}^{*b}$. The set of all subsets of $\mathcal{X}$ with b elements is denoted $\mathcal{X}^{\#b}$. For

example, for distinct elements a, $b \in \mathcal{X}$, (a, b) and (b, a) are distinguished in $\mathcal{X}^{*2}$, while $\{a, b\} = \{b, a\}$ in $\mathcal{X}^{\#2}$. For integers $1 \leq b \leq a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0 = 1$ by convention. If $|\mathcal{X}| = a$, then $(a)_b$ becomes the size of $\mathcal{X}^{*b}$. When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, their (disjoint) union is denoted $\mathcal{X} \sqcup \mathcal{Y}$.

2.2 Uniform and XOR-Universal Hash Functions

Let $\delta > 0$, and let $\mathcal{H}$ be a family of functions $h : \mathcal{T} \to \{0,1\}^n$ for a non-empty set $\mathcal{T}$.

1. $\mathcal{H}$ is said to be *uniform* if for any $x \in \mathcal{T}$ and any $y \in \{0,1\}^n$,
$$\Pr\left[h \leftarrow_{\$} \mathcal{H} : h(x) = y\right] = \frac{1}{2^n}.$$
2. $\mathcal{H}$ is said to be *δ-almost XOR-universal (δ-AXU)* if for any distinct $x, x' \in \mathcal{T}$ and any $y \in \{0,1\}^n$,
$$\Pr\left[h \leftarrow_{\$} \mathcal{H} : h(x) \oplus h(x') = y\right] \leq \delta.$$

A Useful Lemma. The following lemma will be used later in our security proof.

Lemma 1. *Let N, a, b, c, t be positive integers such that $t + a \leq N/2$, $t + b \leq N/2$ and $t + c \leq N/2$. Then, the following inequality holds.*

$$\frac{\left((N)_t\right)^2 (N-a-b-c)_t}{(N-a)_t\,(N-b)_t\,(N-c)_t} \geq 1 - \frac{8t(ab+bc+ca)}{N^2}.$$

Proof. One has

$$\begin{aligned}
\frac{\left((N)_t\right)^2 (N-a-b-c)_t}{(N-a)_t\,(N-b)_t\,(N-c)_t} &= \prod_{i=0}^{t-1} \frac{(N-i)^2\,(N-a-b-c-i)}{(N-a-i)\,(N-b-i)\,(N-c-i)} \\
&= \prod_{i=0}^{t-1} 1 - \frac{(ab+bc+ca)(N-i) - abc}{(N-a-i)\,(N-b-i)\,(N-c-i)} \\
&\geq \prod_{i=0}^{t-1} 1 - \frac{(ab+bc+ca)N}{(N-a-i)\,(N-b-i)\,(N-c-i)} \\
&\geq \prod_{i=0}^{t-1} 1 - \frac{(ab+bc+ca)N}{(N-a-t)\,(N-b-t)\,(N-c-t)} \\
&\geq 1 - \frac{t(ab+bc+ca)N}{(N-a-t)\,(N-b-t)\,(N-c-t)} \\
&\geq 1 - \frac{8t(ab+bc+ca)}{N^2}.
\end{aligned}$$

□

2.3 Tweakable Block Cipher

A *tweakable permutation* TP with tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\mathsf{TP} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any tweak $t \in \mathcal{T}$, $x \mapsto \mathsf{TP}(t, x)$ is a permutation of $\mathcal{X}$. Throughout the paper, we will fix $\mathcal{X} = \{0,1\}^n$, and write $\mathcal{TP}(\mathcal{T}, n)$ to mean the set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^n$.

A *tweakable block cipher* TBC with key space $\mathcal{K}$, tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\mathsf{TBC} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that for any key $k \in \mathcal{K}$, $(t, x) \mapsto \mathsf{TBC}(k, t, x)$ is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$.

A *tweakable Even-Mansour cipher* is a natural construction of a tweakable block cipher using public permutations. Let $\mathcal{H}$ be a family of functions $h : \mathcal{T} \to \{0,1\}^n$ for a non-empty set $\mathcal{T}$. Given an r-tuple $\mathbf{P} = (P_1, \ldots, P_r)$ of permutations of $\{0,1\}^n$ (for some positive integer r), the r-round tweakable Even-Mansour cipher $\mathsf{TEM}^{\mathbf{P}} : \mathcal{H}^r \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ maps a key $\mathbf{h} = (h_1, \ldots, h_r) \in \mathcal{H}^r$, a tweak $t \in \mathcal{T}$, and a plaintext $x \in \{0,1\}^n$ to the following ciphertext.

$$\mathsf{TEM}^{\mathbf{P}}(\mathbf{h}, t, x) = \mathsf{EM}^{P_r}_{h_r,t} \circ \cdots \circ \mathsf{EM}^{P_1}_{h_1,t}(x),$$

where for each $i \in \{1, \ldots, r\}$, $x \in \mathcal{X}$ and $t \in \mathcal{T}$,

$$\mathsf{EM}^{P_i}_{h_i,t}(x) = h_i(t) \oplus P(h_i(t) \oplus x).$$

We will interchangeably write $\mathsf{TEM}^{\mathbf{P}}(\mathbf{h}, t, x)$ and $\mathsf{TEM}^{\mathbf{P}}_{\mathbf{h}}(t, x)$.

2.4 Forkcipher

A (tweakable) *forkcipher* FTBC with key space $\mathcal{K}$, tweak space $\mathcal{T}$, message space $\{0,1\}^n$ and flag $b \in \{0,1,2\}$ is a mapping $\mathsf{FTBC} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \times \{0,1,2\} \to \{0,1\}^n \cup (\{0,1\}^n \times \{0,1\}^n)$. The encryption algorithm takes a key $K \in \mathcal{K}$, a tweak $t \in \mathcal{T}$, a message $x \in \{0,1\}^n$ and an output selector b, and outputs the "left" n-bit ciphertext C_0 if $b = 0$, the "right" n-bit ciphertext C_1 if $b = 1$, and both ciphertexts (C_0, C_1) if $b = 2$.

Let $\mathcal{H}$ be a family of functions $h : \mathcal{T} \to \{0,1\}^n$ for a tweak space $\mathcal{T}$. For positive integers r_1 and r_2, the (r_1, r_2)-round *tweakable Even-Mansour forkcipher* $\mathsf{FTEM}^{\mathbf{P}_1,\mathbf{P}_2,\mathbf{P}_3}$ based on an r_1-tuple $\mathbf{P}_1$ and r_2-tuples $\mathbf{P}_2$ and $\mathbf{P}_3$ of n-bit permutations operates on message space $\{0,1\}^n$ with key space $\mathcal{H}^{r_1} \times \mathcal{H}^{r_2} \times \mathcal{H}^{r_2}$ and tweak space $\mathcal{T}$, where

$$\begin{aligned}
\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x, 0) &= \mathsf{TEM}^{\mathbf{P}_2}_{\mathbf{h}_2} \circ \mathsf{TEM}^{\mathbf{P}_1}_{\mathbf{h}_1}(t, x), \\
\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x, 1) &= \mathsf{TEM}^{\mathbf{P}_3}_{\mathbf{h}_3} \circ \mathsf{TEM}^{\mathbf{P}_1}_{\mathbf{h}_1}(t, x), \\
\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x, 2) &= \left(\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x, 0), \mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x, 1)\right),
\end{aligned}$$

for a key $\mathbf{h} = (\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3) \in \mathcal{H}^{r_1} \times \mathcal{H}^{r_2} \times \mathcal{H}^{r_2}$, a tweak $t \in \mathcal{T}$ and a plaintext $x \in \{0,1\}^n$.

2.5 Indistinguishability

The focus of this paper will be put on the case that $r_1 = r_2 = 1$. In this case, the tweakable Even-Mansour forkcipher is based on a set of three independent permutations, denoted $\mathbf{P} = (P_1, P_2^{-1}, P_3^{-1})$[1]; precisely, let

$$\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x) = \left(\mathsf{TEM}^{P_2^{-1}}_{h_2} \circ \mathsf{TEM}^{P_1}_{h_1}(t, x), \mathsf{TEM}^{P_3^{-1}}_{h_3} \circ \mathsf{TEM}^{P_1}_{h_1}(t, x)\right),$$

for $\mathbf{h} = (h_1, h_2, h_3) \in \mathcal{H}^3$, $t \in \mathcal{T}$ and $x \in \{0,1\}^n$.

In the *real* world, a secret key $\mathbf{h} = (h_1, h_2, h_3) \in \mathcal{H}^3$ is chosen uniformly at random. A set of three permutations P_1, P_2, and P_3 are also chosen independently at random from $\mathsf{Perm}(n)$. A distinguisher $\mathcal{A}$ is given access to a construction oracle, denoted $\mathsf{CONS}^{\mathsf{re}}$, as well as $\mathbf{P} = (P_1, P_2, P_3)$; the oracle $\mathsf{CONS}^{\mathsf{re}}$ takes as input a tweak $t \in \mathcal{T}$, $x \in \{0,1\}^n$ which is either a plaintext or a (partial) ciphertext, and $j \in \{1,2,3\}$, and returns

$$\mathsf{CONS}^{\mathsf{re}}(t, x, j) \stackrel{\text{def}}{=} \left(\mathsf{TEM}^{P_{j+1}^{-1}}_{h_{j+1}} \circ \mathsf{TEM}^{P_j}_{h_j}(t, x), \mathsf{TEM}^{P_{j+2}^{-1}}_{h_{j+2}} \circ \mathsf{TEM}^{P_j}_{h_j}(t, x)\right)$$

[1] We use the inverses of P_2 and P_3 for convenience of notation in our security proof. It makes no difference in the security proof since they are modeled as random permutations.

with indices taken modulo 3.[2]

In the *ideal* world, tweakable permutations $\widetilde{Q}$ and $\widetilde{R}$ are chosen from $\mathcal{TP}(\mathcal{T}, n)$ independently at random; a distinguisher $\mathcal{A}$ is given access to a construction oracle (with the same interface as $\mathsf{CONS}^{\mathsf{re}}$), denoted $\mathsf{CONS}^{\mathsf{id}}$, defined as follows.

$$\begin{aligned}
\mathsf{CONS}^{\mathsf{id}}(t, x, 1) &\stackrel{\text{def}}{=} \left(\widetilde{Q}(t, x), \widetilde{R}(t, x)\right), \\
\mathsf{CONS}^{\mathsf{id}}(t, x, 2) &\stackrel{\text{def}}{=} \left(\widetilde{R}(t, \widetilde{Q}^{-1}(t, x)), \widetilde{Q}^{-1}(t, x)\right), \\
\mathsf{CONS}^{\mathsf{id}}(t, x, 3) &\stackrel{\text{def}}{=} \left(\widetilde{R}^{-1}(t, x), \widetilde{Q}(t, \widetilde{R}^{-1}(t, x))\right).
\end{aligned}$$

On the other hand, oracle access to $\mathbf{P} = (P_1, P_2, P_3)$ is still allowed in this world.

The adversarial goal is to tell apart the two worlds by adaptively making oracle queries to the construction and each of the permutations. Formally, $\mathcal{A}$'s distinguishing advantage is defined by

$$\begin{aligned}
\mathsf{Adv}_{\mathsf{FTEM}}(\mathcal{A}) = \Pr\left[\widetilde{Q}, \widetilde{R} \leftarrow_{\$} \mathcal{TP}(\mathcal{T}, n), P_1, P_2, P_3 \leftarrow_{\$} \mathsf{Perm}(n) : 1 \leftarrow \mathcal{A}^{\mathsf{CONS}^{\mathsf{id}}, P_1, P_2, P_3}\right] \\
- \Pr\left[h_1, h_2, h_3 \leftarrow_{\$} \mathcal{H}, P_1, P_2, P_3 \leftarrow_{\$} \mathsf{Perm}(n) : 1 \leftarrow \mathcal{A}^{\mathsf{CONS}^{\mathsf{re}}, P_1, P_2, P_3}\right].
\end{aligned}$$

For p, $q > 0$, we define

$$\mathsf{Adv}_{\mathsf{FTEM}}(p, q) = \max_{\mathcal{A}} \mathsf{Adv}_{\mathsf{FTEM}}(\mathcal{A})$$

where the maximum is taken over all adversaries $\mathcal{A}$ making at most p queries to each of the inner permutations and at most q queries to the construction oracle.

2.6 H-coefficient Technique

Suppose that a distinguisher $\mathcal{A}$ makes p queries to each of the permutations, and q queries to the construction oracle. The queries made to the construction oracle are recorded in a query history

$$\mathcal{Q}_C = (t^i, x_1^i, x_2^i, x_3^i)_{1 \le i \le q}.$$

According to the instantiation, it would imply either $\mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}](t^i, x_1^i) = (x_2^i, x_3^i)$ or $(x_2^i, x_3^i) = (\widetilde{Q}(t^i, x_1^i), \widetilde{R}(t^i, x_1^i))$. For $j = 1, 2, 3$, the queries made to P_j are recorded in a query history

$$\mathcal{Q}_{P_j} = (j, u_j^i, v_j^i)_{1 \le i \le p},$$

where (j, u_j^i, v_j^i) represents the evaluation $P_j(u_j^i) = v_j^i$ obtained by the i-th query to P_j. We will often omit the index j when it is clear from context. Let

$$\mathcal{Q}_P = \mathcal{Q}_{P_1} \cup \mathcal{Q}_{P_2} \cup \mathcal{Q}_{P_3}.$$

At the end of the interaction, we will provide the adversary $\mathcal{A}$ with the actual key $\mathbf{h}$. In the ideal world, a dummy key $\mathbf{h}$ will be selected uniformly at random from $\mathcal{H}^3$, and given to $\mathcal{A}$. This will not degrade the adversarial distinguishing advantage since the distinguisher is free to ignore this additional information. We will call

$$\tau = (\mathbf{h}, \mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$$

the *transcript* of the attack; it contains all the information that $\mathcal{A}$ has obtained at the end of the attack. When we consider an information theoretic distinguisher, we can assume that the distinguisher is deterministic without making any redundant query.

[2] In this paper, an adversary is allowed only a single type of construction query. This assumption is only for simplicity of proof, while it is equivalent to the original definition.

Given a permutation oracle transcript $\mathcal{Q}$ and a permutation P, we will write $P \vdash \mathcal{Q}$ if $P(u) = v$ for every $(u, v) \in \mathcal{Q}$. Similarly, given a tuple of permutation oracle transcripts $\mathcal{Q} = (\mathcal{Q}_1, \ldots, \mathcal{Q}_r)$ and a tuple of permutations $\mathbf{P} = (P_1, \ldots, P_r)$ for some r, we will write $\mathbf{P} \vdash \mathcal{Q}$ if $P_i \vdash \mathcal{Q}_i$ for every $i = 1, \ldots, r$. This notation naturally extends to construction oracle transcripts; for $\mathsf{CONS} \in \{\mathsf{CONS}^{\mathsf{id}}, \mathsf{CONS}^{\mathsf{re}}\}$, we will write $\mathsf{CONS} \vdash \mathcal{Q}_C$ if $\mathsf{CONS}(t, x_1, 1) = (x_2, x_3)$ for every $(t, x_1, x_2, x_3) \in \mathcal{Q}_C$.

Fix a transcript $\tau = (\mathbf{h}, \mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$. We will call the transcript τ *attainable* if the probability that $\mathsf{CONS}^{\mathsf{id}} \vdash \mathcal{Q}_C$ and $(P_1, P_2, P_3) \vdash (\mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$ is nonzero in the ideal world. We also denote T_{id}(resp. T_{re}) the probability distribution of the transcript τ induced by the ideal world (resp. the real world). By extension, we use the same notation to denote a random variable distributed according to each distribution.

In order to upper bound the advantage of the distinguisher, we will partition the set of attainable transcripts Γ into a set of "good" transcripts Γ_{good} such that the probabilities to obtain some transcript $\tau \in \Gamma_{\mathsf{good}}$ are close in the real and in the ideal world, and a set Γ_{bad} of "bad" transcripts such that the probability to obtain any $\tau \in \Gamma_{\mathsf{bad}}$ is small in the ideal world, and use the following theorem.

Lemma 2 (H-coefficient Technique [Pat08])**.** *Fix a distinguisher $\mathcal{A}$. Let $\Gamma = \Gamma_{\mathsf{good}} \sqcup \Gamma_{\mathsf{bad}}$ be a partition of the set of attainable transcripts. Assume that there exists ε_1 such that for any $\tau \in \Gamma_{\mathsf{good}}$,*

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

and that there exists ε_2 such that $\Pr[\mathsf{T}_{\mathrm{id}} \in \Gamma_{\mathsf{bad}}] \leq \varepsilon_2$. Then one has

$$\mathsf{Adv}^{\mathbf{P}}_{\mathsf{FTEM}_{\mathbf{h}}}(\mathcal{A}) \leq \varepsilon_1 + \varepsilon_2.$$

3 Security of FTEM

In this section, we prove the security of a $(1, 1)$-round FTEM cipher based on a triple of public permutations $\mathbf{P} = (P_1, P_2, P_3) \in \mathsf{Perm}(n)^3$ using a family $\mathcal{H}$ of hash functions from $\mathcal{T}$ to $\{0,1\}^n$ as the key space; for $\mathbf{h} = (h_1, h_2, h_3) \in \mathcal{H}^3$,

$$\begin{aligned}\mathsf{FTEM}^{\mathbf{P}}(\mathbf{h}, t, x) =& (h_2(t) \oplus P_2^{-1}(h_1(t) \oplus h_2(t) \oplus P_1(x \oplus h_1(t))),\\ & h_3(t) \oplus P_3^{-1}(h_1(t) \oplus h_3(t) \oplus P_1(x \oplus h_1(t)))).\end{aligned}$$

The provable security of this cipher is summarized by the following theorem.

Theorem 1. *For $\delta > 0$, let $\mathcal{H}$ be a uniform δ-AXU family of functions from $\mathcal{T}$ to $\{0,1\}^n$. Then, for any integers p and q such that $p + 2q \leq N/2$, one has*

$$\begin{aligned}\mathsf{Adv}_{\mathsf{FTEM}}(p, q) \leq & \frac{12(p + \sqrt{q})^2 q}{N^2} + 3\delta q\\ & + \frac{3\delta(p + \sqrt{q})^2 q^2}{2N^2} + \frac{3p\sqrt{q}}{N} + \frac{3\delta q\sqrt{q}}{2} + \frac{24q(p + 2q)^2}{N^2} + \frac{6q\sqrt{q}}{N}.\end{aligned}$$

Proof. As a preliminary step, we extend a transcript τ by including additional information in it; after $\mathcal{A}$ has finished the interactions with its oracles but before it outputs its decision bit, it is provided with the hash keys $\mathbf{h} = (h_1, h_2, h_3)$ (as discussed in Section 2.6). Moreover, we employ a trick to simplify the proof: for $i \in \{1, 2, 3\}$, if there exist any pairs (t, x_1, x_2, x_3), $(t', x_1', x_2', x_3') \in \mathcal{Q}_C$ such that $x_i \oplus h_i(t) = x_i' \oplus h_i(t')$ and $(x_i \oplus h_i(t), \cdot) \notin \mathcal{Q}_{P_i}$, $\mathcal{A}$ is given an additional primitive query $(x_i \oplus h_i(t), P_i(x_i \oplus h_i(t)))$ by lazy sampling P_i (in both the ideal and the real worlds). This additional information is included in $\mathcal{Q}_{P_i}$, and this step will be called the *collision-giving phase*.

The next step of the proof is to define bad events; they are typically related to collisions of queries on the input to the construction or any underlying permutation. For $i \in \{1,2,3\}$, we define

$$
\begin{aligned}
U_i &= \{u : (u,v) \in \mathcal{Q}_{P_i}\},\\
V_i &= \{v : (u,v) \in \mathcal{Q}_{P_i}\},\\
\alpha_i &= \left|\{(t,x_1,x_2,x_3) \in \mathcal{Q}_C : \exists (t',x_1',x_2',x_3') \neq (t,x_1,x_2,x_3), x_i \oplus h_i(t) = x_i' \oplus h_i(t')\}\right|,\\
\beta_i &= \left|\{(t,x_1,x_2,x_3) \in \mathcal{Q}_C : x_i \oplus h_i(t) \in U_i\}\right|.
\end{aligned}
$$

By definition, we see that $|\mathcal{Q}_{P_i}| = p + \alpha_i$ and $\alpha_i \leq \beta_i$. We will call an attainable transcript τ *bad* if one of the following conditions is satisfied:

- $\mathsf{bad1} \Leftrightarrow \bigvee_{\{i,j\} \in [3]^{\#2}} \mathsf{bad1}_{\{i,j\}}$, where
  - $\mathsf{bad1}_{\{i,j\}} \Leftrightarrow$ there exist $(t,x_1,x_2,x_3) \in \mathcal{Q}_C$, $u_i \in U_i$, $u_j \in U_j$ such that $x_i \oplus h_i(t) = u_i$ and $x_j \oplus h_j(t) = u_j$.
- $\mathsf{bad2} \Leftrightarrow \bigvee_{(i,j) \in [3]^{*2}} \mathsf{bad2}_{(i,j)}$, where
  - $\mathsf{bad2}_{(i,j)} \Leftrightarrow$ there exist $(t,x_1,x_2,x_3) \in \mathcal{Q}_C$, $(u_i,v_i) \in \mathcal{Q}_{P_i}$, $v_j \in V_j$ such that $x_i \oplus h_i(t) = u_i$ and $v_i \oplus h_i(t) = v_j \oplus h_j(t)$.
- $\mathsf{bad3} \Leftrightarrow \bigvee_{(i,j) \in [3]^{*2}} \mathsf{bad3}_{(i,j)}$, where
  - $\mathsf{bad3}_{(i,j)} \Leftrightarrow$ there exist distinct $(t,x_1,x_2,x_3), (t',x_1',x_2',x_3') \in \mathcal{Q}_C$ and (not necessarily distinct) $(u_i,v_i), (u_i',v_i') \in \mathcal{Q}_{P_i}$ such that $x_i \oplus h_i(t) = u_i$, $x_i' \oplus h_i(t') = u_i'$ and $v_i \oplus h_i(t) \oplus h_j(t) = v_i' \oplus h_i(t') \oplus h_j(t')$.
- $\mathsf{bad4} \Leftrightarrow \bigvee_{i \in [3]} \mathsf{bad4}_i$, where
  - $\mathsf{bad4}_i \Leftrightarrow$ for $j,k \in [3] \setminus \{i\}$ such that $j \neq k$, there exist distinct (t,x_1,x_2,x_3), $(t',x_1',x_2',x_3') \in \mathcal{Q}_C$, $(u_j,v_j) \in \mathcal{Q}_{P_j}$ and $(u_k,v_k) \in \mathcal{Q}_{P_k}$ such that $x_j \oplus h_j(t) = u_j$, $x_k' \oplus h_k(t') = u_k$ and $v_j \oplus h_j(t) \oplus h_i(t) = v_k \oplus h_k(t') \oplus h_i(t')$.
- $\mathsf{bad5} \Leftrightarrow \beta_i > \sqrt{q}$ for some $i \in \{1,2,3\}$.

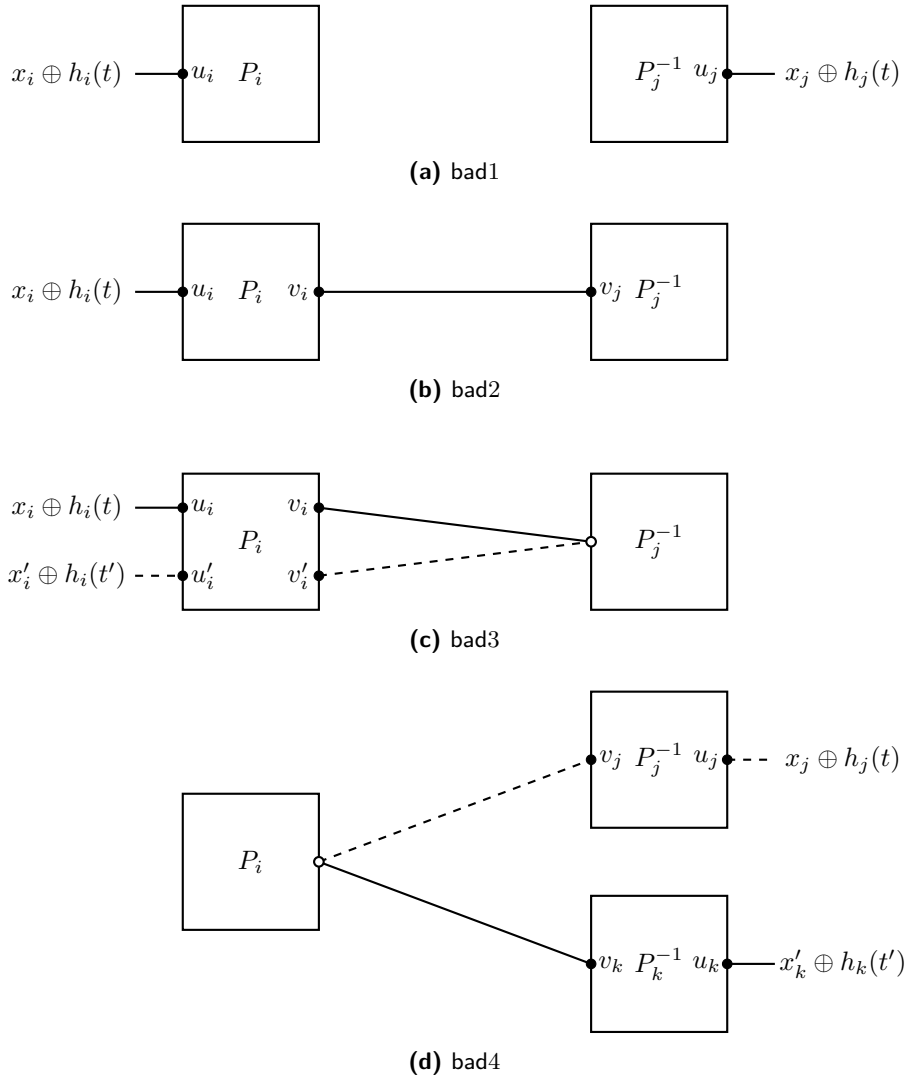

Figure 2: Bad events bad1, bad2, bad3 and bad4. Black dots represent values fixed by permutation queries, while white dots are "free". Two distinct dots on each side do not necessarily correspond to distinct values.

Remark 1. By bad5, we limit the number of collisions between queries. On the other hand, if bad$i$ happens for some $i \in \{1,2,3,4\}$, then an adversary is able to distinguish FTEM from its ideal counterpart. For example, suppose that a transcript satisfies bad1; it means that the transcript contains $(t, x_1, x_2, x_3) \in \mathcal{Q}_C, u_i \in U_i$ and $u_j \in U_j$ such that $x_i \oplus h_i(t) = u_i$ and $x_j \oplus h_j(t) = u_j$. In the real world, one always has $v_i \oplus v_j = h_i(t) \oplus h_j(t)$, while this equation holds with negligible probability in the ideal world.

If a transcript τ is not bad, then it will be called a *good* transcript. With the definition of bad transcripts as above, we can prove the following lemmas, whose proof is deferred to the end of this section.

Lemma 3. *One has*

$$\Pr[\mathsf{T}_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}] \leq \frac{12(p+\sqrt{q})^2 q}{N^2} + 3\delta q + \frac{3\delta(p+\sqrt{q})^2 q^2}{2N^2} + \frac{3p\sqrt{q}}{N} + \frac{3\delta q\sqrt{q}}{2}.$$

Lemma 4. *Let p and q be nonnegative integers such that $p + 5\sqrt{q} \leq N/2$. For any $\tau \in \Gamma_{\mathsf{good}}$, one has*

$$\frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]} \geq 1 - \left(\frac{24q(p+2q)^2}{N^2} + \frac{6q\sqrt{q}}{N}\right).$$

Theorem 1 follows by combining Lemma 3 and Lemma 4 with Lemma 2. □

3.1 Proof of Lemma 3

For an event E, we will write $\mathsf{p}_{\mathsf{id}}[E]$ (resp. $\mathsf{p}_{\mathsf{re}}[E]$) to denote the probability that T_{id} (resp. T_{re}) satisfies E. By the union bound, we have

$$\begin{aligned}
\mathsf{p}_{\mathsf{id}}[\tau \in \tau_{\mathsf{bad}}] &= \mathsf{p}_{\mathsf{id}}[\mathsf{bad1} \vee \mathsf{bad2} \vee \mathsf{bad3} \vee \mathsf{bad4} \vee \mathsf{bad5}] \\
&\leq \mathsf{p}_{\mathsf{id}}[\mathsf{bad5}] + \mathsf{p}_{\mathsf{id}}[\mathsf{bad1} \vee \mathsf{bad2} \vee \mathsf{bad3} \vee \mathsf{bad4} \mid \neg\mathsf{bad5}] \\
&\leq \mathsf{p}_{\mathsf{id}}[\mathsf{bad1} \mid \neg\mathsf{bad5}] + \mathsf{p}_{\mathsf{id}}[\mathsf{bad2} \mid \neg\mathsf{bad5}] + \mathsf{p}_{\mathsf{id}}[\mathsf{bad3} \mid \neg\mathsf{bad5}] \\
&\quad + \mathsf{p}_{\mathsf{id}}[\mathsf{bad4} \mid \neg\mathsf{bad5}] + \mathsf{p}_{\mathsf{id}}[\mathsf{bad5}]
\end{aligned}$$

In the following, we will bound the probability of each bad event in the ideal world. Without $\mathsf{bad5}$, we can assume that $\alpha_i \leq \beta_i \leq \sqrt{q}$ and $|U_i| \leq p + \sqrt{q}$ for $i = 1, 2, 3$.

Upper bounding $\mathsf{p}_{\mathsf{id}}[\mathsf{bad1}]$ and $\mathsf{p}_{\mathsf{id}}[\mathsf{bad2}]$. Assuming that $\mathsf{bad5}$ does not hold, fix $\{i, j\} \in [3]^{\#2}$. For any $(t, x_1, x_2, x_3) \in \mathcal{Q}_C$, $u_i \in U_i$ and $u_j \in U_j$,

$$\mathsf{p}_{\mathsf{id}}[h_i(t) = x_i \oplus u_i \wedge h_j(t) = x_j \oplus u_j] = \frac{1}{N^2}$$

by $\mathcal{H}$ is uniform and since h_i and h_j are chosen independently. Since $|\mathcal{Q}_C| \leq q$ and $|U_i|, |U_j| \leq p + \sqrt{q}$, we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad1}_{\{i,j\}} \mid \neg\mathsf{bad5}\right] \leq \frac{(p+\sqrt{q})^2 q}{N^2},$$

and hence,

$$\mathsf{p}_{\mathsf{id}}[\mathsf{bad1} \mid \neg\mathsf{bad5}] \leq \frac{3(p+\sqrt{q})^2 q}{N^2}.$$

Similarly, we obtain

$$\mathsf{p}_{\mathsf{id}}[\mathsf{bad2} \mid \neg\mathsf{bad5}] \leq \frac{6(p+\sqrt{q})^2 q}{N^2}.$$

Upper bounding $\mathsf{p}_{\mathsf{id}}[\mathsf{bad3}]$. Assuming that $\mathsf{bad5}$ does not hold, fix $(i, j) \in [3]^{*2}$. For any $(t, x_1, x_2, x_3) \neq (t', x_1', x_2', x_3') \in \mathcal{Q}_C$ and $(u_i, v_i), (u_i', v_i') \in \mathcal{Q}_{P_i}$ such that $x_i \oplus h_i(t) = u_i$ and $x_i' \oplus h_i(t') = u_i'$, one has the following statement. By the δ-AXU property of $\mathcal{H}$ and the fact that h_i and h_j are picked independently from $\mathcal{H}$, for some fixed $h' \in \mathcal{H}$,

$$\mathsf{p}_{\mathsf{id}}[h_i = h' \wedge h_j(t) \oplus h_j(t') = v_i \oplus v_i' \oplus h'(t) \oplus h'(t')] \leq \frac{\delta}{|\mathcal{H}|}.$$

Summing over all possible h' and all such tuple of queries, we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad3}_{(i,j)} \mid \neg\mathsf{bad5}\right] \leq \frac{\delta\beta_i^2}{2} \leq \frac{\delta q}{2},$$

since $\beta_i < \sqrt{q}$ without $\mathsf{bad5}$. Hence,

$$\mathsf{p}_{\mathsf{id}}[\mathsf{bad3} \mid \neg\mathsf{bad5}] \leq 3\delta q.$$

Upper bounding $\mathsf{p}_{\mathsf{id}}[\mathsf{bad4}]$. Assuming that $\mathsf{bad5}$ does not hold, consider $\mathsf{bad4}_i$ for a fixed $i \in \{1, 2, 3\}$.

1. Assume that $t \neq t'$. For any $(t, x_1, x_2, x_3) \neq (t', x'_1, x'_2, x'_3) \in \mathcal{Q}_C$, $(u_j, v_j) \in \mathcal{Q}_{P_j}$ and $(u_k, v_k) \in \mathcal{Q}_{P_k}$, by the uniformity of $\mathcal{H}$ and the δ-AXU property of $\mathcal{H}$ and the fact that h_i, h_j, h_k are picked independently from $\mathcal{H}$,

$$\mathsf{p}_{\mathsf{id}}\left[h_j(t) = x_j \oplus u_j \wedge h_k(t') = x'_k \oplus u' \wedge h_i(t) \oplus h_i(t') = v_j \oplus h_j(t) \oplus v_k \oplus h_k(t')\right] \leq \frac{\delta}{N^2}.$$

   Therefore we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad}4_i \wedge (t \neq t') \mid \neg\mathsf{bad}5\right] \leq \frac{\delta(p+\sqrt{q})^2 q^2}{2N^2}.$$

2. Assume that $t = t'$. We only consider $(t, x_1, x_2, x_3) \neq (t', x'_1, x'_2, x'_3) \in \mathcal{Q}_C$, $(u_j, v_j) \in \mathcal{Q}_{P_j}$ and $(u_k, v_k) \in \mathcal{Q}_{P_k}$ such that $x_j \oplus x'_k = u_j \oplus v_j \oplus u_k \oplus v_k$. Given $(t, x_1, x_2, x_3), (u_j, v_j)$ and (u_k, v_k), there exists only one (t, x'_1, x'_2, x'_3) which satisfies the above equation. So, the number of such tuples is upper bounded by $(p+\sqrt{q})^2 q$. It is trivial that any tuples that do not satisfy the above equation cannot make $\mathsf{bad}4$. By the uniformity of $\mathcal{H}$ and the fact that h_j and h_k are picked independently from $\mathcal{H}$,

$$\mathsf{p}_{\mathsf{id}}\left[h_j(t) = x_j \oplus u_j \wedge h_k(t') = x'_k \oplus u_k\right] \leq \frac{1}{N^2}.$$

   Therefore, we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad}4_i \wedge (t = t') \mid \neg\mathsf{bad}5\right] \leq \frac{(p+\sqrt{q})^2 q}{N^2}.$$

Considering three possibilities of choosing i, we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad}4 \mid \neg\mathsf{bad}5\right] \leq \frac{3\delta(p+\sqrt{q})^2 q^2}{2N^2} + \frac{3(p+\sqrt{q})^2 q}{N^2}.$$

Upper bounding $\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad}5\right]$. For $i \in [3]$, α_i and β_i can be seen as a random variable using the randomness of h_i. Then we have

$$\mathrm{Ex}\left[\alpha_i\right] = \mathrm{Ex}\left[h_i(t) \oplus h_i(t') = x_i \oplus x'_i\right] \leq \frac{\delta q^2}{2}.$$

For any $(t, x_1, x_2, x_3) \in \mathcal{Q}_C$, it collides with primitive query only if an adversary gets $(x_i \oplus h_i(t), \cdot) \in \mathcal{Q}_{P_i}$ in the querying phase or the collision-giving phase. Then we have

$$\mathrm{Ex}\left[\beta_i\right] = \mathrm{Ex}\left[h_i(t) = x_i \oplus u\right] \leq \frac{pq}{N} + \mathrm{Ex}\left[\alpha_i\right] \leq \frac{pq}{N} + \frac{\delta q^2}{2}.$$

By Markov's inequality,

$$\mathsf{p}_{\mathsf{id}}\left[\beta_i > \sqrt{q}\right] \leq \frac{p\sqrt{q}}{N} + \frac{\delta q\sqrt{q}}{2}.$$

Therefore we have

$$\mathsf{p}_{\mathsf{id}}\left[\mathsf{bad}5\right] \leq \frac{3p\sqrt{q}}{N} + \frac{3\delta q\sqrt{q}}{2}.$$

Summing up all the upper bounds for the probabilities of individual bad events, we can conclude the proof of Lemma 3.

3.2 Proof of Lemma 4

Fix a good transcript $\tau = (\mathbf{h}, \mathcal{Q}_C, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$. We will partition $\mathcal{Q}_C$ into the following subsets.

$$\begin{aligned}
\mathcal{Q}_{U_1} &= \{(t, x_1, x_2, x_3) \in \mathcal{Q}_C : x_1 \oplus h_1(t) \in U_1\},\\
\mathcal{Q}_{U_2} &= \{(t, x_1, x_2, x_3) \in \mathcal{Q}_C : x_2 \oplus h_2(t) \in U_2\},\\
\mathcal{Q}_{U_3} &= \{(t, x_1, x_2, x_3) \in \mathcal{Q}_C : x_3 \oplus h_3(t) \in U_3\},\\
\mathcal{Q}_0 &= \{(t, x_1, x_2, x_3) \in \mathcal{Q}_C : x_1 \oplus h_1(t) \notin U_1, x_2 \oplus h_2(t) \notin U_2, x_3 \oplus h_3(t) \notin U_3\}.
\end{aligned}$$

Note that $|\mathcal{Q}_{U_1}| = \beta_1$, $|\mathcal{Q}_{U_2}| = \beta_2$ and $|\mathcal{Q}_{U_3}| = \beta_3$. Furthermore, we have

$$\mathcal{Q}_C = \mathcal{Q}_{U_1} \sqcup \mathcal{Q}_{U_2} \sqcup \mathcal{Q}_{U_3} \sqcup \mathcal{Q}_0$$

since for $(i, j) \in [3]^{*2}$,

- $\mathcal{Q}_{U_i} \cap \mathcal{Q}_{U_j} = \varnothing$ without $\mathsf{bad1}_{(i,j)}$,
- $\mathcal{Q}_{U_i} \cap \mathcal{Q}_0 = \varnothing$ by definition.

Since P_1, P_2, P_3 and h_1, h_2, h_3 are all independent in both the real and the ideal worlds, we have

$$\begin{aligned}
\frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]} &= \frac{\Pr[\mathbf{h}] \Pr[\mathbf{P} \vdash \tau_p] \Pr[\mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p]}{\Pr[\mathbf{h}] \Pr[\mathbf{P} \vdash \tau_p] \Pr\left[(\widetilde{Q}, \widetilde{R}) \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right]}\\
&= \frac{\Pr[\mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p]}{\Pr\left[(\widetilde{Q}, \widetilde{R}) \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right]},
\end{aligned}$$

where we write $\tau_p = (\mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, \mathcal{Q}_{P_3})$. Let

$$\begin{aligned}
p(\tau) &= \Pr[\mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p],\\
p_U(\tau) &= \Pr\left[\bigwedge_{i=1}^{3} \mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_{U_i} \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right],\\
p_0(\tau) &= \Pr\left[\mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_0 \mid \mathbf{h}, \mathbf{P} \vdash \tau_p, \bigwedge_{i=1}^{3} \mathsf{FTEM}_{\mathbf{h}}[\mathbf{P}] \vdash \mathcal{Q}_{U_i}\right].
\end{aligned}$$

Then we have

$$\frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]} = \frac{p(\tau)}{\Pr\left[(\widetilde{Q}, \widetilde{R}) \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right]} = \frac{p_U(\tau) p_0(\tau)}{\Pr\left[(\widetilde{Q}, \widetilde{R}) \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right]}. \quad (1)$$

We will now lower bound $p_U(\tau)$ and $p_0(\tau)$.

Lower Bounding $p_U(\tau)$. For $(i, j) \in [3]^{*2}$, let

$$\begin{aligned}
\widetilde{U}_i^j &= \{x_i \oplus h_i(t) : (t, x_1, x_2, x_3) \in \mathcal{Q}_{U_j}\},\\
\widetilde{V}_i^j &= \{P_j(x_j \oplus h_j(t)) \oplus h_j(t) \oplus h_i(t) : (t, x_1, x_2, x_3) \in \mathcal{Q}_{U_j}\}.
\end{aligned}$$

Then for $(i, j, k) \in [3]^{*3}$,

- $U_i, \widetilde{U}_i^j, \widetilde{U}_i^k$ are pairwise disjoint since otherwise at least one of $\mathsf{bad1}_{\{i,j\}}$ and $\mathsf{bad1}_{\{i,k\}}$ holds;

- $V_i, \widetilde{V}_i^j, \widetilde{V}_i^k$ are pairwise disjoint since otherwise at least one of $\mathsf{bad2}_{(i,j)}$, $\mathsf{bad2}_{(i,k)}$, and $\mathsf{bad4}_j$ holds;
- $\left|\widetilde{U}_j^i\right| = \left|\widetilde{V}_j^i\right| = \left|\widetilde{U}_k^i\right| = \left|\widetilde{V}_k^i\right| = \beta_i$ since otherwise at least one of $\mathsf{bad1}_{\{i,j\}}$, $\mathsf{bad3}_{(i,j)}$, $\mathsf{bad1}_{\{i,k\}}$, and $\mathsf{bad3}_{(i,k)}$ holds.

Therefore, P_1 should satisfy additional $\beta_2 + \beta_3$ equations that map $\widetilde{U}_1^2$ to $\widetilde{V}_1^2$ and map $\widetilde{U}_1^3$ to $\widetilde{V}_1^3$, in order to satisfy all $\mathcal{Q}_{P_1}$, $\mathcal{Q}_{P_2}$ and $\mathcal{Q}_{P_3}$. The same argument applies to P_2 and P_3. Overall, we have

$$p_U(\tau) = \frac{1}{(N-p_1)_{\beta_2+\beta_3}(N-p_2)_{\beta_3+\beta_1}(N-p_3)_{\beta_1+\beta_2}}. \tag{2}$$

Lower Bounding $p_0(\tau)$. For $i = 1, 2, 3$, P_i is fixed on p_i' elements, where

$$\begin{aligned} p_1' &= p_1 + \beta_2 + \beta_3, \\ p_2' &= p_2 + \beta_3 + \beta_1, \\ p_3' &= p_3 + \beta_1 + \beta_2. \end{aligned}$$

Let $q' = q - \beta_1 - \beta_2 - \beta_3$, and let m be the number of distinct tweaks appearing in $\mathcal{Q}_C$; they will be denoted $t_1, \ldots, t_m$. For $i = 1, \ldots, m$, let $\mathcal{Q}_{0,i}$ denote a subset of $\mathcal{Q}_0$ whose tweak is t_i, and let $q_i' = |\mathcal{Q}_{0,i}|$. Then we have $\sum_{i=1}^{m} q_i' = q'$.

Without loss of generality, we can assume that the first q_1' queries use tweak t_1, and the next q_2' queries use tweak t_2, and so on. Hence, we can write

$$\mathcal{Q}_0 = \left\{ (t_1, x_1^{1,1}, x_2^{1,1}, x_3^{1,1}), \ldots, (t_1, x_1^{1,q_1'}, x_2^{1,q_1'}, x_3^{1,q_1'}), \ldots, (t_m, x_1^{m,q_m'}, x_2^{m,q_m'}, x_3^{m,q_m'}) \right\}.$$

For $i = 1, \ldots, m$, and $j = 1, \ldots, q_i'$, let

$$\begin{aligned} \hat{u}_1^{i,j} &= x_1^{i,j} \oplus h_1(t_i), \\ \hat{u}_2^{i,j} &= x_2^{i,j} \oplus h_2(t_i), \\ \hat{u}_3^{i,j} &= x_3^{i,j} \oplus h_3(t_i). \end{aligned}$$

By the definition of $\mathcal{Q}_0$, for each $k = 1, 2, 3$, all $\hat{u}_k^{i,j}$ are distinct and not included in $U_k \cup \widetilde{U}_k^{k+1} \cup \widetilde{U}_k^{k+2}$ with indices taken modulo 3. Let N_0 be the number of tuples $(\hat{v}_1^{1,1}, \ldots, \hat{v}_1^{1,q_1'}, \ldots, \hat{v}_1^{m,q_m'})$ satisfying the following conditions:

- for each (i,j), $\hat{v}_1^{i,j} \notin V_1 \cup \widetilde{V}_1^2 \cup \widetilde{V}_1^3$ where $\left|V_1 \cup \widetilde{V}_1^2 \cup \widetilde{V}_1^3\right| = p_1'$;
- for each (i,j), $\hat{v}_1^{i,j} \oplus h_1(t_i) \oplus h_2(t_i) \notin V_2 \cup \widetilde{V}_2^3 \cup \widetilde{V}_2^1$ where $\left|V_2 \cup \widetilde{V}_2^3 \cup \widetilde{V}_2^1\right| = p_2'$;
- for each (i,j), $\hat{v}_1^{i,j} \oplus h_1(t_i) \oplus h_3(t_i) \notin V_3 \cup \widetilde{V}_3^1 \cup \widetilde{V}_3^2$ where $\left|V_3 \cup \widetilde{V}_3^1 \cup \widetilde{V}_3^2\right| = p_3'$;
- for each (i,j), $\hat{v}_1^{i,j} \oplus h_1(t_i) \oplus h_2(t_i)$ is distinct from any value $\hat{v}_1^{k,\ell} \oplus h_1(t_k) \oplus h_2(t_k)$ such that $k < i$ and $\ell = 1, \ldots, q_k'$, which excludes at most $\sum_{k=1}^{i-1} q_k'$ values for $\hat{v}_1^{i,j}$;
- for each (i,j), $\hat{v}_1^{i,j} \oplus h_1(t_i) \oplus h_3(t_i)$ is distinct from any value $\hat{v}_1^{k,\ell} \oplus h_1(t_k) \oplus h_3(t_k)$ such that $k < i$ and $\ell = 1, \ldots, q_k'$, which excludes at most $\sum_{k=1}^{i-1} q_k'$ values for $\hat{v}_1^{i,j}$.

In order to evaluate the number of tuples, for each (i,j), $\hat{v}_1^{i,j}$ must be chosen distinct from the previous $\sum_{k=1}^{i-1} q'_k + (j-1)$ values. Therefore, one has

$$\begin{aligned} N_0 &\geq \prod_{i=1}^{m}\prod_{j=1}^{q'_i}\left(N - p'_1 - p'_2 - p'_3 - 3\sum_{k=1}^{i-1} q'_k - (j-1)\right) \\ &= \prod_{i=1}^{m}\left(N - p'_1 - p'_2 - p'_3 - 3\sum_{k=1}^{i-1} q'_k\right)_{q'_i}. \end{aligned} \tag{3}$$

Given that T_{id} satisfies $(\mathcal{Q}_{U_1}, \mathcal{Q}_{U_2}, \mathcal{Q}_{U_3})$ and τ_p, the condition $P_1(\hat{u}_1^{i,j}) = \hat{v}_1^{i,j}$ requires q' distinct fresh equations on P_1, P_2, P_3. Therefore we have

$$p_0(\tau) = N_0 \cdot \frac{1}{(N-p'_1)_{q'}} \cdot \frac{1}{(N-p'_2)_{q'}} \cdot \frac{1}{(N-p'_3)_{q'}}. \tag{4}$$

Putting The Pieces Together. Combining (2) and (4), we have

$$p(\tau) = \frac{N_0}{(N-p_1)_{q'+\beta_2+\beta_3}(N-p_2)_{q'+\beta_3+\beta_1}(N-p_3)_{q'+\beta_1+\beta_2}}. \tag{5}$$

It is also obvious that

$$\Pr\left[(\widetilde{Q},\widetilde{R}) \vdash \mathcal{Q}_C \mid \mathbf{h}, \mathbf{P} \vdash \tau_p\right] = \frac{1}{\left(\prod_{i=1}^{m}(N)_{q_i}\right)^2}. \tag{6}$$

Then, by (1), (5) and (6), we have

$$\begin{aligned} \frac{\mathsf{p}_{\mathsf{re}}[\tau]}{\mathsf{p}_{\mathsf{id}}[\tau]} &\geq \frac{N_0 \cdot \left(\prod_{i=1}^{m}(N)_{q_i}\right)^2}{(N-p_1)_{q'+\beta_2+\beta_3}(N-p_2)_{q'+\beta_3+\beta_1}(N-p_3)_{q'+\beta_1+\beta_2}} \\ &= \underbrace{\frac{N_0 \cdot \left(\prod_{i=1}^{m}(N)_{q'_i}\right)^2}{(N-p'_1)_{q'}(N-p'_2)_{q'}(N-p'_3)_{q'}}}_{R_0} \\ &\quad \times \underbrace{\frac{\left(\prod_{i=1}^{m}(N)_{q_i}\right)^2}{\left(\prod_{i=1}^{m}(N)_{q_i}\right)^2 (N-p_1)_{\beta_2+\beta_3}(N-p_2)_{\beta_3+\beta_1}(N-p_3)_{\beta_1+\beta_2}}}_{R'} \end{aligned}$$

It remains to lower bound R_0 and R'; by (3), we have

$$\begin{aligned} R_0 &= \frac{N_0 \cdot \left(\prod_{i=1}^{m}(N)_{q'_i}\right)^2}{(N-p'_1)_{q'}(N-p'_2)_{q'}(N-p'_3)_{q'}} \\ &\geq \prod_{i=1}^{m} \frac{\left((N)_{q'_i}\right)^2 \left(N - p'_1 - p'_2 - p'_3 - 3\sum_{k=1}^{i-1} q'_k\right)_{q'_i}}{\left(N - p'_1 - \sum_{k=1}^{i-1} q'_k\right)_{q'_i}\left(N - p'_2 - \sum_{k=1}^{i-1} q'_k\right)_{q'_i}\left(N - p'_3 - \sum_{k=1}^{i-1} q'_k\right)_{q'_i}} \\ &\geq \prod_{i=1}^{m}\left(1 - \frac{8q'_i\left((p'_1+t)(p'_2+t) + (p'_3+t)(p'_1+t) + (p'_3+t)(p'_1+t)\right)}{N^2}\right), \end{aligned} \tag{7}$$

where the last inequality follows from Lemma 1 with $t = \sum_{k=1}^{i-1} q'_k$. For $j = 1, 2, 3$ (without bad5), $p'_j + t$ is upper bounded as follows.

$$p'_1 + t = p'_1 + \sum_{k=1}^{i-1} q'_k \le p'_1 + q' \le p_1 + q - \beta_1 \le p + 2q,$$
$$p'_2 + t = p'_2 + \sum_{k=1}^{i-1} q'_k \le p'_2 + q' \le p_2 + q - \beta_2 \le p + 2q,$$
$$p'_3 + t = p'_3 + \sum_{k=1}^{i-1} q'_k \le p'_3 + q' \le p_3 + q - \beta_3 \le p + 2q.$$

By combining the above upper bounds with (7), and since $\sum_{i=1}^{m} q'_i \le q$, we have

$$R_0 \ge 1 - \frac{24q(p+2q)^2}{N^2}. \tag{8}$$

On the other hand, since $\beta_i \le \sqrt{q}$ for $i = 1, 2, 3$ (without bad5), we have

$$\begin{aligned} R' &\ge \frac{\left(\prod_{i=1}^{m}(N-q'_i)_{q_i-q'_i}\right)^2}{N^{2(\beta_1+\beta_2+\beta_3)}} \ge \frac{\left((N-q)^{\sum_{i=1}^{m}(q_i-q'_i)}\right)^2}{N^{2(\beta_1+\beta_2+\beta_3)}} \ge \frac{\left((N-q)^{q-q'}\right)^2}{N^{2(\beta_1+\beta_2+\beta_3)}} \\ &\ge \frac{\left((N-q)^{(\beta_1+\beta_2+\beta_3)}\right)^2}{N^{2(\beta_1+\beta_2+\beta_3)}} \ge \left(1-\frac{q}{N}\right)^{6\sqrt{q}} \ge 1 - \frac{6q\sqrt{q}}{N}. \end{aligned} \tag{9}$$

Combining (8) and (9), we can conclude the proof of Lemma 4.

4 Conclusion

In this paper, we have proposed to apply the IFI paradigm to tweakable Even-Mansour ciphers, and proved that a $(1,1)$-round FTEM cipher is secure up to $2^{\frac{2n}{3}}$ queries in the ideal permutation model.

Compared to the straightforward construction using three independent tweakable block ciphers (as discussed in [ALP+19]), our construction is a public-permutation based counterpart with a weaker provable security bound, while using weaker primitives as well, distinguishing permutations, keys and tweaks.

It is an interesting open question whether the same level of security is possible with a smaller number of keys and permutations. We expect that this question might be resolved by using (advanced) Mirror theory and the sum-capture lemma. Another open question is to apply the *iterate-multifork-iterarte* paradigm [ALP+19] to the TEM ciphers. Our conjecture is that the resulting permutation-based forkcipher will enjoy almost the same level of security.

Acknowledgments

The authors would like to thank the anonymous reviewers of FSE 2020 for valuable comments that helped improving this paper. Jooyoung Lee was supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (Ministry of Science and ICT), No. NRF-2017R1E1A1A03070248.

References

[ABD+16] Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennick, Mridul Nandi, Elmar Tischhauser, and Kan Yasuda. COLM v1. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/colmv1.pdf.

[ALP+19] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 (Proceedings, Part II)*, volume 11922 of *LNCS*, pages 153–182. Springer, 2019. Full version available at http://eprint.iacr.org/2019/1004.

[BDPA09] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak Sponge Function Family Main Document. Submission to the CAESAR competition, 2009. Available at http://keccak.noekeon.org/Keccak-main-2.0.pdf.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part II)*, volume 9815 of *LNCS*, pages 123–153. Springer, 2016.

[BKL+17] Daniel J. Bernstein, Stefan Kölbl, Stefan Lucks, Pedro Maat Costa Massolino, Florian Mendel, Kashif Nawaz, Tobias Schneider, Peter Schwabe, François-Xavier Standaert, Yusuke Todo, and Benoît Viguier. GIMLI: A Cross-Platform Permutation. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017*, volume 10529 of *LNCS*, pages 299–320. Springer, 2017.

[CS14] Shan Chen and John P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014.

[CS15] Benoît 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 (Proceedings, Part I)*, volume 9056 of *LNCS*, pages 584–613. Springer, 2015.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/asconv12.pdf.

[DR02] Joan Daemen and Vincent Rijmen. AES and the Wide Trail Design Strategy. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 108–109. Springer, 2002.

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

[JNPS16] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, and Yannick Seurin. Deoxys v1.41. Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/deoxysv141.pdf.

[KR16] Ted Krovetz and Phillip Rogaway. OCB (v1.1). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/ocbv11.pdf.

[Pat08] Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *International Workshop on Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.

[WH16] Hongjun Wu and Tao Huang. The Authenticated Cipher MORUS (v2). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/morusv2.pdf.

[WP16] Hongjun Wu and Bart Preneel. AEGIS: A Fast Authenticated Encryption Algorithm (v1.1). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/aegisv11.pdf.

[Wu16] Hongjun Wu. ACORN: A Lightweight Authenticated Cipher (v3). Submission to the CAESAR competition, 2016. Available at https://competitions.cr.yp.to/round3/acornv3.pdf.