Designs, Codes and Cryptography (2024) 92:13–49
https://doi.org/10.1007/s10623-023-01288-4

BBB security for 5-round even-Mansour-based key-alternating Feistel ciphers

Arghya Bhattacharjee[1] · Ritam Bhaumik[2] · Avijit Dutta[3] · Mridul Nandi[1] · Anik Raychaudhuri[1]

Received: 7 December 2022 / Revised: 13 June 2023 / Accepted: 27 July 2023 /
Published online: 4 October 2023

Abstract
In this paper, we study the security of the Key-Alternating Feistel (KAF) ciphers, a class of key alternating ciphers with the Feistel structure, where each round of the cipher is instantiated with n-bit public round permutation P_i, namely the i-th round of the cipher maps

$$(X_L, X_R) \mapsto (X_R, P_i(X_R \oplus K_i) \oplus K_i \oplus X_L).$$

We have shown that our 5 round construction with independent round permutations and independent round keys achieves $2n/3$-bit security in the random permutation model, i.e., the setting where the adversary is allowed to make forward and inverse queries to the round permutations in a black box way.

Keywords Key alternating cipher · Feistel cipher · Even Mansour cipher · H-coefficient technique

Communicated by M. Eichlseder.

✉ Ritam Bhaumik
ritam.bhaumik@epfl.ch

✉ Avijit Dutta
avirocks.dutta13@gmail.com

Arghya Bhattacharjee
bhattacharjeearghya29@gmail.com

Mridul Nandi
mridul.nandi@gmail.com

Anik Raychaudhuri
anikrc1@gmail.com

1 Indian Statistical Institute, Kolkata, India

2 EPFL, Lausanne, Switzerland

3 Institute of Advancing Intelligence, TCG-CREST, Kolkata, India

1 Introduction

A block-cipher is a length-preserving encryption function that takes a k-bit key K and an n-bit message X and outputs an n-bit ciphertext Y. The primary security requirement from a block-cipher is its pseudorandomness. Unfortunately, we cannot establish the theoretical soundness of the security of block-ciphers. Therefore, researchers have focused on proving security results of block-ciphers by idealising some of its components. In this direction, two popular design approaches of block-ciphers have been extensively studied—Feistel networks and Substitution-Permutation networks (SPNs). As of today the design of almost every block-cipher roughly falls into one of the above two categories.

Feistel Scheme. Most of the provable security results for Feistel networks fall under the Luby-Rackoff (LR) framework, in reference to the seminal work by Luby and Rackoff [27], where the round-functions of the Feistel scheme are pseudorandom functions which are idealised as being uniformly random (and secret) via the standard hybrid argument. It was shown in [27] that the 3-round Feistel scheme is a pseudorandom permutation. Later on, Patarin [34] proved that the 4-round Feistel scheme yields a strong pseudorandom permutation, which means that the scheme is secure even if the adversary is allowed to make inverse queries to the permutation oracle. Following [34], a long series of works either have established better security bounds for the Feistel scheme with a larger number of rounds [1, 23, 29, 30, 37] or have reduced the security of the scheme [31, 32, 35, 42]. Ramzan and Reyzin [40] proved that the $(n/2)$-bit security of 4-round Feistel scheme holds even if the adversary has black-box access to the two inner functions of the construction. Naor and Reingold [33] showed that the similar security bound holds even if one replaces the first and last round of the 4-round Feistel construction with pairwise independent permutations, and even weaker constructions were proven secure in [39]. Gentry and Ramzan [19] showed that the public random permutation of the one-round Even-Mansour cipher [18] $X \mapsto K_1 \oplus P(X \oplus K_1)$ can be replaced by a four-round public Feistel scheme, and the resulting construction is still a strong pseudorandom permutation that achieves $O(2^{n/2})$ security bound.

Patarin [36] proved $(3n/4)$-bit strong pseudorandomness security for the 6-round Feistel scheme with the conjecture of proving better bounds of the construction. In [29], Maurer and Pietrzak have proved that the r-round Feistel scheme is secure up to $2^{n(r-1)/r}$ queries. In [37], Patarin analysed the security of Feistel scheme with five or more rounds. He showed that the 5-round Feistel scheme is secure against all attacks that make only the forward queries, as long as the number of queries is less than 2^n. Moreover, he has also showed that 6-round Feistel is secure against all attacks that make both forward and inverse queries to the construction as long as the number of queries is limited to 2^n. Hoang and Rogaway [23] studied the beyond-birthday-bound security of generalised Feistel networks. In 2010 [38], Patarin showed $O(2^n/n)$ security bound for four, five and six rounds of balanced Feistel schemes in Known Plaintext Attack (KPA) model, Chosen Plaintext Attack model against adaptive adversaries (CPA2), and Chosen Plaintext Ciphertext Attack model against adaptive adversaries (CPCA2) respectively. In the same paper, Patarin also proved beyond birthday bound security for unbalanced Feistel scheme with $2n$-bit to n-bit contracting round functions. A detailed literature study on the security of the Feistel scheme can be found in [30].

Substitution-Permutation Networks. Earlier provable security results for SPN ciphers were only limited to resistance to specific attacks such as differential [6] and linear attacks [28]. Recently, a series of works have studied the ideal key-alternating cipher, a.k.a. the Iterated Even-Mansour (IEM) cipher. Chen and Steinberger [10] proved a tight security bound (where the bound matches the best known attack on the construction) of $2^{rn/(r+1)}$ for the r-round

IEM cipher. In the last couple of years research has focussed on analysing the security of the IEM cipher with fewer permutations and keys. Chen et al. [11] have shown a $(2n/3)$-bit security bound for the 2-round IEM cipher based on a single permutation and one n-bit key. This result was extended by Wu et al. [47] to three rounds of the IEM cipher based on a single n-bit public random permutation that was shown secure up to $O(2^{3n/4})$ queries. A recent work by Tessaro and Zhang [45] showed the existence of non-trivial distributions of the limited independence of the round key for which the r-round IEM cipher achieves optimal security. Along with the study of the IEM cipher, security of the tweakable IEM cipher, where the tweak is mixed with each round key of the IEM cipher, has also been extensively studied in [12, 13, 17].

Key-Alternating Feistel Cipher. Despite the extensive research along the line of Luby and Rackoff [27], which has been very generic and covers many possible choices of round functions for the Feistel scheme, a concrete scheme is yet to be established to design a keyed block-cipher from some simple key-less primitive (e.g. unkeyed round function). Therefore, to design a keyed block-cipher, it remains necessary to design some keyed round functions $F_i(K_i, X)$, a task which, unfortunately, is not known to be easier than designing the keyed block-cipher itself. On the other hand, concrete block-ciphers following Feistel designs like DES, GOST, Camellia, LBlock [46], Twine [44] usually employ length-preserving key-less functions in each round by XOR-ing each round-key before applying the corresponding round function. This idea naturally corresponds to the Feistel scheme with round functions instantiated with $F_i(K_i \oplus X_i)$, where F_i is a key-less public round-function and therefore, at the i-th round of the Feistel scheme, the intermediate state is updated as

$$(X_L^i, X_R^i) \mapsto (X_R^i, F_i(X_R^i \oplus K_i) \oplus X_L^i),$$

where X_L and X_R are two n-bit halves of the state. This model of Feistel design was named the Key-Alternating Feistel (KAF) cipher by Lampe and Seurin [26]. One can see that two rounds of a KAF cipher can be rewritten as a single-key one-round EM cipher, where the permutation P is a two-round public and unkeyed Feistel scheme. When the round functions of the KAF cipher are uniform random public functions, we refer to it as an *ideal* KAF cipher. Thus, the ideal KAF cipher differs from the usual LR framework in two ways: (a) first, the ideal KAF cipher considers complex round-functions (i.e., random function oracles) instead of the keyed round-functions in LR framework; (b) second, it considers the simplest keying procedure, namely key-XOR-ing. As a result, KAF is likely to capture well the structural properties of practical Feistel ciphers and the practical security of Feistel designs compared to the LR framework.

However, the security gap between LR and KAF ciphers is non-negligible. The best known generic key-recovery attacks with complexity 2^{2n} break four rounds LR [34], which is in sharp contrast with six rounds KAF [22]. Moreover, Patarin has shown [30, 38] that six (resp. five) rounds of LR achieve optimal pseudorandom (resp. strong-pseudorandom) security. However, Guo and Wang. [20] have shown a generic distinguishing attack against the r-round KAF cipher using $O(2^{n(r-2)/(r-1)})$ queries, which implies that the n-round KAF cipher achieves asymptotically optimal security.

The theoretical security analysis of ideal KAF ciphers is generally done using the random function model, where one models the key-less round-functions F_i as public random functions that can be queried by the adversary in a black-box way, and try to establish the indistinguishability of $(\mathsf{KAF}_{\mathbf{K}}^{F_1,F_2,\ldots,F_r}, F_1, F_2, \ldots, F_r)$ from $(P, F_1, F_2, \ldots, F_r)$ in the random function model, where P is a $2n$-bit uniform random permutation and $\mathbf{K} = (K_1, K_2, \ldots, K_r)$ contains r uniformly random n-bit keys. This indistinguishability notion implies that the ideal

KAF cipher with a secret random key $\mathbf{K}$ is indistinguishable from a $2n$-bit uniform random permutation P, even if the adversary is given access to the r random round-functions $F_1, F_2, \ldots, F_r$. Note that this security model is closely related to the security model used in proving the security of the IEM cipher.

In this direction, the first reported work is by Ramzan and Reyzin [40] who proved the $(n/2)$-bit strong pseudorandom security of the 4-round Feistel scheme even when the adversary has black-box access to the middle two functions of the construction. Gentry and Ramzan [19] showed the $(n/2)$-bit strong pseudorandom security of the one-round EM cipher when its underlying public permutation is replaced by a four-round public Feistel scheme. Lampe and Seurin [26] proved that an r-round ideal KAF cipher achieves security up to $O(2^{tn/(t+1)})$ queries of the adversary, where $t = \lfloor r/3 \rfloor$ in the non-adaptive setting with the adversary prohibited in making inverse queries to the construction, and $t = \lfloor r/6 \rfloor$ in the adaptive setting with the adversary allowed to make bi-directional queries to the construction. More recently, Guo and Wang [20] have shown that a 4-round ideal KAF cipher with a single round function F and four n-bit round keys (K_1, K_2, K_3, K_4) such that K_1, K_4 and $K_2 \oplus K_3$ are all uniform is $(n/2)$-bit secure in the multi-user setting; they have further shown that a 6-round ideal KAF cipher with six independent round functions is $(2n/3)$-bit secure in the multi-user setting as long as the six round keys $(K_1, K_2, K_3, K_4, K_5, K_6)$ are all uniform and adjacent round keys are independent. In a follow up work of [20], Shen et al. [43] have studied a 4-round ideal KAF cipher with an even more optimised key schedule, in which an n-bit master key K is XORed only in the first and last rounds of the cipher and a one-bit rotation is applied on the output of the first layer round function, and proved the $(n/2)$-bit strong pseudorandom security of the construction.

1.1 Our contribution

All the earlier research on the security of ideal KAF ciphers is largely based on round functions and all these round functions are mostly length-preserving unkeyed functions. In reality, length-preserving unkeyed functions are rarely available unlike compressing unkeyed functions (e.g., [25]); moreover, it is not easy to design the former over the latter. This situation is similar to the fact that designing pseudorandom functions is harder than designing pseudorandom permutations. On the other hand, unkeyed permutations are available in plenty [2, 4, 7, 15, 21] and used in numerous sponge based designs [3, 5, 7–9, 14, 16, 41]. In addition, designing unkeyed permutations is a lot easier than designing unkeyed length-preserving functions: examples include [2, 4, 7, 15, 21]. To the best of our knowledge, there has been no prior security result on permutation-based ideal KAF ciphers. In this paper, we for the first time study the security of an ideal KAF cipher based on unkeyed permutations. In particular, we prove that a five-round ideal KAF cipher based on five independent instances of one-round EM cipher is secure up to $O(2^{2n/3})$ queries in the random permutation model against all adversaries that are allowed to make both encryption and decryption queries to the construction. We depict existing provable security results on idealised KAF cipher in Table 1.

Remark 1 We would like to point out here that Guo and Wang [20] shows that public function based 4-round KAF (resp. 6-round KAF) is birthday-bound (resp. beyond-birthday-bound) secure. However, the security for 5-round KAF based on public functions still remains open. We believe that 5-round KAF based on public round function can achieve beyond-birthday-bound security and the proof should follow the similar technique as adopted in our paper. Moreover, in case of public round function, we do not have to bother about the constraint that distinct inputs should map to distinct outputs, which in turn reduces both the number

Table 1 Existing provable security results for ideal KAF cipher

#Rounds	Key-size	Primitive	#Round-primitives	Bound	Model	Ref
3	n	R	1	$n/2$	CPA	[43]
4	$4n$	R	2	$n/2$	CCA	[19]
4	n	R	1	$n/2$	CCA	[20]
6	$2n$	R	6	$2n/3$	CCA	[20]
12	$12n$	R	12	$2n/3$	CCA	[26]
$6t$	$6tn$	R	$6tn$	$tn/(t+1)$	CCA	[26]
5	$5n$	P	5	$2n/3$	CCA	This Paper

R denotes that the primitive is a function and P denotes that the primitive is a permutation. n denotes the domain size of the primitive. CPA denotes the adversarial model where the adversary can make only encryption queries, and CCA denotes the adversarial model where the adversary can make both encryption and decryption queries

and the complexity of analyzing the bad events. However, as there is almost no practical candidates of length preserving public round functions designed from scratch (as they are hard to design), we chose to analyze the security of the KAF using public round permutation, which are abundance in practice (e.g., Keccak [4], SPONGENT [7], Beetle [8] etc.). It is worth mentioning that constructions based on a permutation with feed-forward (like unkeyed Davies-Meyer) or with the XOR of multiple permutations meets our goal of designing round function, but notice that they are essentially built out of public random permutations as their underlying primitives.

Open problems In this paper, we study the security analysis of a five-round of ideal KAF cipher based on five independent public round permutations and five independent round keys. However, we believe that one can reduce the number of keys and round permutations of the construction and achieve the similar security bound. Unfortunately, the security proof for such a construction will be extremely tedious due to the increased degree of input–output dependency at each round, which forces one to use technical machinery like sum-capture lemma [10] and its variants [45] in the security proof. Establishing the tightness of the proven bound or improving the bound of the construction from $2n/3$-bits to $3n/4$-bits is also left as a future research problem

2 Preliminaries

Notation. We denote integers and indices using lowercase letters, uppercase letters (e.g., X, Y) will be used to denote binary strings and functions, and calligraphic uppercase letters (e.g., $\mathcal{X}$, $\mathcal{Y}$) will be used for denoting sets and spaces. For a given non-empty set $\mathcal{X}$, we write $X \leftarrow_{\$} \mathcal{X}$ to denote that the random variable X is chosen uniformly at random from the set $\mathcal{X}$.

For a natural number m, we write the m-times Cartesian product of the set $\{0,1\}$ with itself as $\{0,1\}^m$, which equivalently denotes the set of all m-bit binary strings. 0^m (resp. 1^m) denotes the concatenation of m 0-bits (resp. m 1-bits). We write $\{0,1\}^{\geq m}$ to denote the set of all binary strings of length at least m and $\{0,1\}^* = \cup_{m=0}^{\infty}\{0,1\}^m$ to denote the set of all binary strings. In this paper we'll fix a natural number n as the width of the primitives, and we'll often refer to an element of $\{0,1\}^n$ as a *block*. For a given subset $\mathcal{X}$ of $\{0,1\}^n$, we write $\mathcal{X}^c$ to denote the complement of $\mathcal{X}$ in $\{0,1\}^n$.

For any $X \in \{0,1\}^*$, $|X|$ denotes the bit-length of X. For two binary strings $X, Y \in \{0,1\}^*$, $X \| Y$ denotes the concatenation of X and Y. For two n-bit binary strings $X, Y \in \{0,1\}^n$, $X+Y$ denotes the field addition of X and Y, equivalent to their bit-wise XOR. For any $X \in \{0,1\}^*$, we denote the parsing of X into n-bit blocks as $X_1 \cdots X_r \leftarrow_n X$, where $|X_i| = n$ for all $1 \leq i < r$ and $1 \leq |X_r| \leq n$ such that $X = X_1 \| \cdots \| X_r$. We write $\|X\| = \lfloor |X|/n \rfloor$ to denote the number of blocks in X.

We write $X = (X_1, X_2, \cdots, X_t) \in (\{0,1\}^n)^t$ to denote a t tuple of n-bit binary strings. Given any such t-tuple of n-bit binary strings $X = (X_1, X_2, \cdots, X_t)$ and for any two integers a, b such that $1 \leq a \leq b \leq t$, we write the subtuple $(X_a, X_{a+1}, \cdots, X_b)$ of length $(b-a+1)$ as $X[a,b]$. For two integers a, b such that $a \leq b$, we write $[a,b]$ to denote the set $\{a, a+1, \cdots, b\}$. Moreover, when $a = 1$, we write $[1,b]$ as $[b]$ to denote the set $\{1, \ldots, b\}$. We write $\mathsf{MSB}_x(X)$ and $\mathsf{LSB}_x(X)$ to denote the most significant x bits and the least significant x bits of the binary string X respectively. For any two integers a, b such that $a \geq b$, we write $(a)_b$ to denote $a(a-1)(a-2)\ldots(a-b+1)$.

We write $\mathcal{F}_n$ to denote the set of all functions F from $\{0,1\}^n$ to $\{0,1\}^n$ and $\mathcal{P}_n$ to denote the set of all permutations P over $\{0,1\}^n$. For a positive integer r, we write $\mathbf{F}^r = (F_1, F_2, \ldots, F_r) \in (\mathcal{F}_n)^r$ to denote a tuple of r n-bit to n-bit functions. Similarly, $\mathbf{P}^r = (P_1, P_2, \ldots, P_r) \in (\mathcal{P}_n)^r$ denotes a tuple of r n-bit permutations. For any two tuples of n-bit binary strings $X = (X_1, X_2, \ldots, X_t)$ and $Y = (Y_1, Y_2, \ldots, Y_t)$ having length t and for any n-bit to n-bit function F, we write $F(X) = Y$ to denote $F(X_i) = Y_i$ for $i \in [t]$. We say that the pair of n-bit binary string tuples (X, Y) is *function compatible*, if there exists at least one function $F : \{0,1\}^n \to \{0,1\}^n$ such that $F(X) = Y$. Note that, for (X, Y) to be a function compatible pair, $X_i = X_j \Rightarrow Y_i = Y_j$. Similarly, for an n-bit permutation P, we write $P(X) = Y$ to denote that $P(X_i) = Y_i$ for $i \in [t]$ and in that case, we say that the pair of n-bit binary string tuples (X, Y) is *permutation compatible*, if there exists at least one n-bit permutation P such that $P(X) = Y$. Note that, for (X, Y) to be a permutation compatible pair, $X_i = X_j \Leftrightarrow Y_i = Y_j$. We write $\mathbf{F}^r(X) = Y$ (resp. $\mathbf{P}^r(X) = Y$) to denote $F_i(X) = Y$ (resp. $P_i(X) = Y$) for $i \in [r]$.

2.1 Definition of EM-based key-alternating Feistel cipher

Given an n-bit public permutation P, and an n-bit key K, the one-round keyed Feistel permutation is the permutation on $\{0,1\}^{2n}$ that is defined as follows:

$$\Psi_K^P(L \| R) = (R, L + P(R + K) + K).$$

Note that, an equivalent way of writing the above permutation $\Psi_K^P(\cdot)$ is as follows:

$$\Psi_K^P(L \| R) = (R, L + \mathsf{EM}_K^P(R)),$$

where $\mathsf{EM}_K^P(R) := P(R + K) + K$ is the one round Even-Mansour (EM) cipher based on n-bit public round permutation P and an n-bit key K. Now, we define r-round EM-based key-alternating Feistel cipher based on r many n-bit public round permutations $\mathbf{P}^r = (P_1, P_2, \ldots, P_r) \in (\mathcal{P}_n)^r$ and a r-tuple of n-bit keys $\mathbf{K} = (K_1, K_2, \ldots, K_r) \in (\{0,1\}^n)^r$, which is denoted as $\mathsf{EM\text{-}KAF}^{\mathbf{P}^r}$. It maps an $2n$-bit plaintext $X \in \{0,1\}^{2n}$ to an $2n$-bit ciphertext as follows:

$$\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}(X) = \Psi_{K_r}^{P_r} \circ \Psi_{K_{r-1}}^{P_{r-1}} \circ \ldots \circ \Psi_{K_1}^{P_1}(X).$$

A pictorial description of EM-based key-alternating cipher is shown in Fig. 1a.

2.2 Security notion of EM-based key-alternating Feistel cipher

We consider distinguisher D interacting with r permutation oracles $\mathbf{P}^r = (P_1, P_2, \ldots, P_r)$, where each P_i is an n-bit random permutation, and a $2n$-bit random permutation oracle (and potentially its inverse), which is either the EM-based KAF cipher $\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}$ specified by a uniformly sampled $\mathbf{P}^r$ from $(\mathcal{P}_n)^r$ with a uniformly random key $\mathbf{K} = (K_1, K_2, \ldots, K_r)$ or a perfectly $2n$-bit random permutation P (independent from $\mathbf{P}^r$). We refer to $\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}$ / P as the construction oracle and $\mathbf{P}^r$ as the primitive oracles. We assume that the distinguisher D is adaptive, i.e., the i-th query of D is determined from the previous query-response and it is also bi-directional (i.e., it can make encryption and decryption queries to its oracles). Moreover, D is also allowed to make bi-directional queries to the primitive oracles (i.e., both forward and inverse queries) in an interleave fashion with the construction oracle queries. We assume that D makes at most q queries to the construction oracle and at most q_i queries to the permutation oracle P_i such that $q_p = q_1 + q_2 + \cdots + q_r$. We call D to be a $(q, q_1, q_2, \ldots, q_r)$ distinguisher. We define the distinguishing advantage of D in distinguishing the outputs of the real oracle $\mathcal{O}_{\mathrm{re}} = (\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}, (\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r})^{-1}, \mathbf{P}^r)$ from the outputs of the ideal oracle $\mathcal{O}_{\mathrm{id}} = (P, P^{-1}, \mathbf{P}^r)$ as follows:

$$\mathbf{Adv}_{\mathcal{O}_{\mathrm{id}}}^{\mathcal{O}_{\mathrm{re}}}(\mathsf{D}) := \Big| \Pr[\mathsf{D}^{\mathcal{O}_{\mathrm{re}}} \Rightarrow 1] - \Pr[\mathsf{D}^{\mathcal{O}_{\mathrm{id}}} \Rightarrow 1] \Big|, \tag{1}$$

where $\mathsf{D}^{\mathcal{O}} \Rightarrow 1$ denotes the event that D outputs 1 after interacting with the oracle $\mathcal{O}$. The first probability in Eq. (1) is defined over the randomness of $\mathbf{K}$ and $\mathbf{P}^r$, whereas the second probability is defined over the randomness of P and $\mathbf{P}^r$. We say that $\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}$ is an *ϵ-strong pseudorandom permutation in the random permutation model* if for each $(q, q_1, q_2, \ldots, q_r)$-distinguisher D, Eq. (1) is upper bounded by ϵ. This is the security notion that we require in the paper. In the rest of the paper we assume that D is computationally unbounded and hence a deterministic distinguisher. We call such a distinguisher an *information theoretic distinguisher*. We also assume that D does not repeat queries and never makes pointless queries, i.e., queries whose answer can be deduced from previous query-responses.

2.3 H-coefficient technique

We consider an information theoretic deterministic distinguisher D with access to the following tuple of oracles: in the real world, it interacts with the oracle $\mathcal{O}_{\mathrm{re}} := (\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^r}, \mathbf{P}^r)$ for an uniformly chosen $\mathbf{P}^r$ from $(\mathcal{P}_n)^r$ and uniformly chosen key $\mathbf{K}$ from $(\{0,1\}^n)^r$. In the ideal world, it interacts with the oracle $\mathcal{O}_{\mathrm{id}} := (P, \mathbf{P}^r)$, where P is a $2n$-bit to $2n$-bit uniformly sampled permutation from $\mathcal{P}_{2n}$ and $\mathbf{P}^r$ is uniformly chosen from $(\mathcal{P}_n)^r$. After this interaction is over, D outputs a decision bit $b \in \{0, 1\}$. The collection of all queries and responses that is made by D to and from the oracle $\mathcal{O}$ during the interaction is summarized in a transcript (ρ, τ), where ρ summarizes the overall interaction of the distinguisher D with all the primitive oracles and τ is the transcript that summarizes the interaction with the construction oracle. More formally, $\tau = \{(L_1, R_1, S_1, T_1), (L_2, R_2, S_2, T_2), \ldots, (L_q, R_q, S_q, T_q)\}$ is the set of all construction queries and responses and

$$\rho = \bigcup_{i=1}^{r} \{(U_1^i, V_1^i), (U_2^i, V_2^i), \ldots, (U_{q_i}^i, V_{q_i}^i)\}$$

is the set of all primitive queries and responses across all the primitive oracles, where we assume that D makes q construction queries and q_i for $i \in [r]$ primitive queries to the i-th

primitive oracle P_i. We define for $j \in [r]$, dom_j and ran_j be the sets of inputs and outputs of the primitive queries respectively to P_j, which we enumerate as $\mathsf{dom}_j = \{U_j^1, \ldots, U_j^{q_j}\}$ and $\mathsf{ran}_j = \{V_j^1, \ldots, V_j^{q_j}\}$. Since D is bidirectional, D can make either forward construction query (L, R) and receives response (S, T) or can make inverse construction query (S, T) and receives response (L, R). Similarly, for primitive query D can either make forward query U_j^i to its primitive P_i and receives response V_j^i or can make inverse query V_j^i to P_i^{-1} and receives response U_j^i. Since, we assume that D never makes pointless queries, none of the transcripts contain any duplicate elements.

We modify the experiment by releasing internal information to D after it has finished the interaction but has not output yet the decision bit. In the real world, we reveal the key $\mathbf{K} = (K_1, K_2, \ldots, K_r)$ which is used in the construction and in the ideal world, we sample a dummy key $\mathbf{K}$ uniformly at random from $(\{0,1\}^n)^r$ and reveal it to the distinguisher. [1] In all the following, the complete transcript is $(\rho, \tau, \mathbf{K})$. Note that, the modified experiment only makes the distinguisher more powerful and hence the distinguishing advantage of D in this experiment is no way less than its distinguishing advantage in the former one.

Let X_{re} (resp. X_{id}) denote the random variable representing the real world and the ideal world transcript respectively. The probability of realizing a transcript $(\rho, \tau, \mathbf{K})$ in the ideal (resp. real) world is called ideal (resp. real) interpolation probability. A transcript $(\rho, \tau, \mathbf{K})$ is said to be *attainable* with respect to D if its ideal interpolation probability is non zero. We denote the set of all such attainable transcripts by Ω. Following these notations, we state the main theorem of H-Coefficient Technique as follows.

Theorem 1 (H-Coefficient Technique) *Let $\Omega = \Omega_{\mathrm{g}} \sqcup \Omega_{\mathrm{b}}$ be some partition of the set of attainable transcripts. Suppose there exists $\epsilon_{\mathrm{ratio}} \geq 0$ such that for any $\eta = (\rho, \tau, \mathbf{K}) \in \Omega_{\mathrm{g}}$,*

$$\mathsf{H}[\eta] := \frac{\Pr[\mathsf{X}_{\mathrm{re}} = \eta]}{\Pr[\mathsf{X}_{\mathrm{id}} = \eta]} \geq 1 - \epsilon_{\mathrm{ratio}},$$

and there exists $\epsilon_{\mathrm{bad}} \geq 0$ such that $\Pr[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{b}}] \leq \epsilon_{\mathrm{bad}}$. Then,

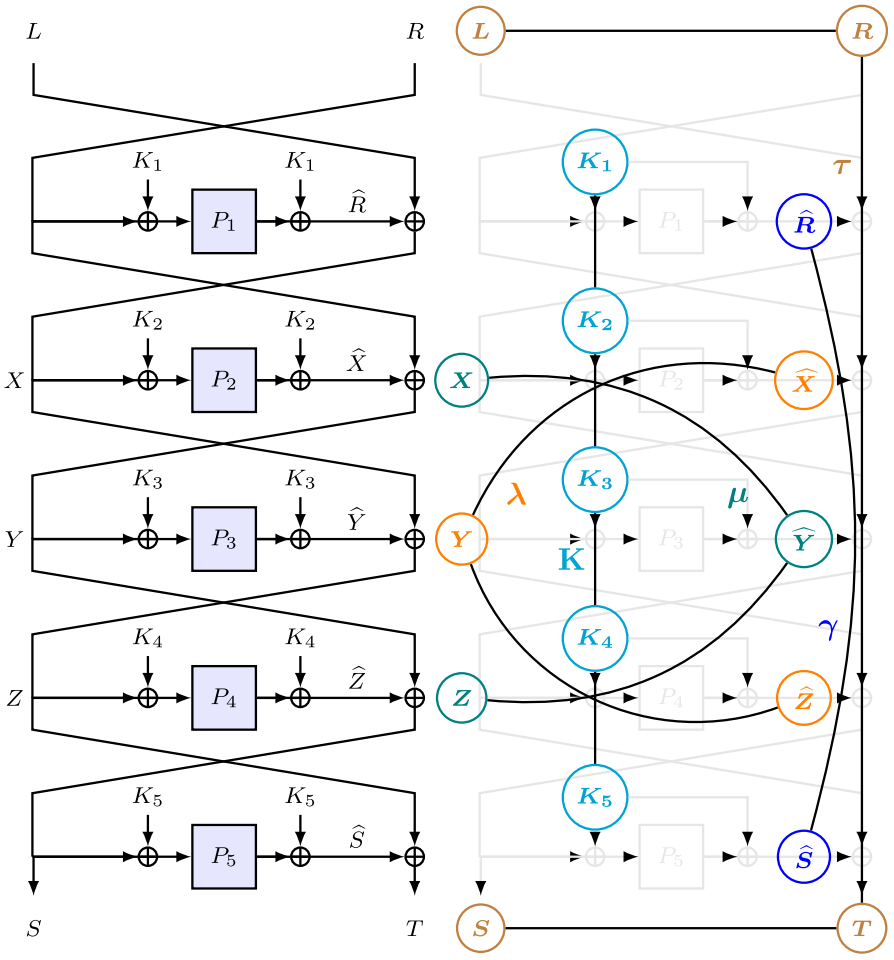
$$\mathbf{Adv}_{\mathcal{O}_{\mathrm{id}}}^{\mathcal{O}_{\mathrm{re}}}(\mathsf{D}) \leq \epsilon_{\mathrm{ratio}} + \epsilon_{\mathrm{bad}}.$$

3 Security result of 5-round EM-KAF

Here we formally state the main finding of this paper: the five-round key-alternating Feistel cipher based on Even-Mansour, which is depicted in Fig. 1a, and its encryption and the decryption steps are listed in Fig. 2, is a strong pseudorandom permutation, secure against all adversaries that make $O(N^{2/3})$ construction and primitive queries in the random permutation model, where $N = 2^n$, n being the state size of each permutation and the size of each key. We formally state this as the following theorem, the proof of which is deferred to Sect. 4.

Theorem 2 (Security Result of $\mathsf{EM\text{-}KAF}_{\mathbf{K}}^{\mathbf{P}^5}$) *Let $\mathbf{P}^5 = (P_1, P_2, P_3, P_4, P_5)$ be five independent n-bit public random permutations and $\mathbf{K} = (K_1, K_2, K_3, K_4, K_5)$ be five independent n-bit keys. Then the strong pseudorandom permutation advantage for any $(q, q_1, q_2, q_3, q_4, q_5)$-distinguisher against the construction in the random permutation model making at most q queries to the construction and q_i primitive queries to P_i, where $q_1 + 2(\sqrt{q}+1) \leq q_2 + q_3 + q_4$,*

[1] Depending on the context, oracle may also release some additional internal information.



(a) Even-Mansour Based 5-round Key-Alternating Feistel Cipher. (Diagram adapted from an example on [Jea16].)

(b) Splitting the construction transcript into τ, K, γ, μ and γ. (The primitive transcript ρ is not shown here.)

Fig. 1 **a** Even-Mansour based 5-round key-alternating Feistel cipher. (Diagram adapted from an example on [24]). **b** Splitting the construction transcript into τ, K, γ, μ and γ. (The primitive transcript ρ is not shown here)

$q_5 + 2(\sqrt{q}+1) \le q_2 + q_3 + q_4$ *and* $q + (q_1 + q_2 + \cdots + q_5) \le N/2$, *is given by*

$$\mathbf{Adv}^{\text{sprp-rp}}_{\text{EM-KAF}^{\mathbf{P}^5}_{\mathbf{K}}}(q, q_1, \ldots, q_5) \le \epsilon,$$

where

$$\epsilon = \frac{6q^2}{N^2} + \frac{20q^3}{N^2} + \frac{2qq_1q_5}{N^2} + \frac{q^2}{N^2}(11q_1 + 16q_2 + 16q_3 + 16q_4 + 11q_5) + \frac{4q^4}{N^3}$$
$$+ \frac{q}{N^2}(2q_1q_2 + q_1q_5 + 5q_2q_3 + 4q_2q_4 + 3q_2q_5 + 2q_1q_3 + 5q_3q_4 + 2q_3q_5 + 3q_1q_4 + 2q_4q_5)$$
$$+ \frac{2q^3}{N^3}(q_1 + q_5) + \frac{q^{1/2}}{N}(q_2 + q_3 + q_4) + \frac{10q^{3/2}}{N}.$$

$\mathsf{EM\text{-}KAF}^{\mathbf{P}^5}_{\mathbf{K}}(L, R)$	$(\mathsf{EM\text{-}KAF}^{\mathbf{P}^5}_{\mathbf{K}})^{-1}(S, T)$
1. $X \leftarrow P_1(R + K_1) + K_1 + L$;	1. $Z \leftarrow P_5(S + K_5) + K_5 + T$;
2. $\hat{X} \leftarrow P_2(X + K_2) + K_2$;	2. $\hat{Z} \leftarrow P_4(Z + K_4) + K_4$;
3. $Y \leftarrow \hat{X} + R$;	3. $Y \leftarrow S + \hat{Z}$;
4. $\hat{Y} \leftarrow P_3(Y + K_3) + K_3$;	4. $\hat{Y} \leftarrow P_3(Y + K_3) + K_3$;
5. $Z \leftarrow \hat{Y} + X$;	5. $X \leftarrow Z + \hat{Y}$;
6. $\hat{Z} \leftarrow P_4(Z + K_4) + K_4$;	6. $\hat{X} \leftarrow P_2(X + K_2) + K_2$;
7. $S \leftarrow \hat{Z} + Y$;	7. $R \leftarrow Y + \hat{X}$;
8. $\hat{S} \leftarrow P_5(S + K_5) + K_5$;	8. $\hat{R} \leftarrow P_1(R + K_1) + K_1$;
9. $T \leftarrow \hat{S} + Z$;	9. $L \leftarrow X + \hat{R}$;
10. **return** (S, T);	10. **return** (L, R);

Fig. 2 Encryption (left) and decryption (right) algorithm of 5-round Even-Mansour Based Key-Alternating Feistel Cipher with five independent round permutations and five independent round keys

The implication of the conditions $q_1+2(\sqrt{q}+1) \leq q_2+q_3+q_4$, $q_5+2(\sqrt{q}+1) \leq q_2+q_3+q_4$ *is that the security holds if the total number of primitive queries to the permutation* P_2, P_3 *and* P_4 *is at least the total number of queries to permutation* P_1 *and the square root of the construction queries and it is also at least the total number of queries to permutation* P_5 *and the square root of the construction queries. With the simplifying assumption* q_1, q_2, q_3, q_4 *and* q_5 *roughly in the order of* q*, we have*

$$\mathbf{Adv}^{\text{sprp-rp}}_{\mathsf{EM\text{-}KAF}^{\mathbf{P}^5}_{\mathbf{K}}}(q, q_1, \ldots, q_5) \leq \frac{6q^2}{N^2} + \frac{121q^3}{N^2} + \frac{8q^4}{N^3} + \frac{10q^{3/2}}{N}.$$

Remark 2 From the above two conditions (i.e., $q_1+2(\sqrt{q}+1) \leq q_2+q_3+q_4$, and $q_5+2(\sqrt{q}+1) \leq q_2+q_3+q_4$), one can ask what would happen to the bound if the adversary does not make any primitive queries to the underlying permutations P_2, P_3 and P_4. We would like to mention here that we have considered an adversary that queries to the underlying permutations over an adversary that does not. Since the distinguishing advantage of the former is always greater than the distinguishing advantage of the latter, we only focus on bounding the distinguishing advantage against an adversary that makes queries to the permutations. In particular, if the above conditions do not hold for an adversary, we ask the adversary to make some dummy queries to P_2, P_3 and P_4, till the conditions hold.

Proof of Theorem 2 is the technical core of this paper. In the remainder of this section, we give an overview of our proof technique, following which the rest of the paper is devoted to the formal proof.

3.1 Computation order in the real world and transcript notation

For each $j \in [5]$, let $\mathcal{J}_j^f$ denote the set of forward queries to P_j and $\mathcal{J}_f^b$ denote the set of backward queries to P_j, so that $\mathcal{J}_j^f \sqcup \mathcal{J}_j^b = [q_j]$. Similarly we split the set of construction queries into the set of encryption queries $\mathcal{I}_{\mathsf{enc}}$ and the set of decryption queries $\mathcal{I}_{\mathsf{dec}}$, with $\mathcal{I}_{\mathsf{enc}} \sqcup \mathcal{I}_{\mathsf{dec}} = [q]$. For each $i \in \mathcal{I}_{\mathsf{enc}}$, the computation proceeds from the query (L^i, R^i) as shown on the left side of Fig. 2 to obtain (S^i, T^i), which is returned to D immediately as the response to the i-th query, while the intermediate variables $\widehat{R}^i$, X^i, $\widehat{X}^i$, Y^i, $\widehat{Y}^i$, Z^i, $\widehat{Z}^i$, and $\widehat{S}^i$ are stored in a cache. Similarly, for each $i \in \mathcal{I}_{\mathsf{dec}}$, the computation proceeds from the query (S^i, T^i) as shown on the right side of Fig. 2 to obtain (L^i, R^i), which is returned to D immediately as the response to the i-th query, while the intermediate variables are stored in a cache.

For the transcript $\tau := \{(L^i, R^i, S^i, T^i) \mid i \in [q]\}$, we define the transcript *slices* $\tau^i := (L^i, R^i, S^i, T^i)$ for each $i \in [q]$, and $\tau^{\mathcal{I}} := \{\tau^i \mid i \in \mathcal{I}\}$ for each $\mathcal{I} \subseteq [q]$. At the end of the online phase, $\mathbf{K}$ is revealed to D, along with all the cached intermediate variables for each $i \in [q]$. This we call the *internal transcript*, which we split into a few parts for ease of reference. For $i \in [q]$, define $\gamma^i := (\widehat{R}^i, \widehat{S}^i)$, $\mu^i := (X^i, \widehat{Y}^i, Z^i)$, and $\lambda^i := (\widehat{X}^i, Y^i, \widehat{Z}^i)$. Analogous to τ, we define $\gamma := \{\gamma^i \mid i \in [q]\}$, $\mu := \{\mu^i \mid i \in [q]\}$, and $\lambda := \{\lambda^i \mid i \in [q]\}$ as well as the slices $\gamma^{\mathcal{I}} := \{\gamma^i \mid i \in \mathcal{I}\}$, $\mu^{\mathcal{I}} := \{\mu^i \mid i \in \mathcal{I}\}$, and $\lambda^{\mathcal{I}} := \{\lambda^i \mid i \in \mathcal{I}\}$ for each $\mathcal{I} \subseteq [q]$. The division is illustrated in Fig. 1b.

For each $i \in [q]$, μ^i is related to γ^i and τ^i through the equations $X^i = \widehat{R}^i + L^i = \widehat{Y}^i + Z^i$ and $Z^i = \widehat{Y}^i + X^i = \widehat{S}^i + T^i$, and λ^i is related to τ^i through the equations $Y^i = \widehat{X}^i + R^i = \widehat{Z}^i + S^i$. Thus, μ^i can be computed from τ^i and γ^i, while λ^i still retains one degree of freedom when all of τ^i, γ^i, and μ^i are fixed. Thus, in some sense, λ is the *innermost* part of the transcript, and the one that we sample at the very end in the ideal world, as described in Sect. 4.1.

For $\mathcal{I} \subseteq [q]$, we also define the following counting sets (along with their sizes) on the $\tau^{\mathcal{I}}$ and $\mu^{\mathcal{I}}$, which will help us in describing the ideal-world sampling mechanism in Sect. 4.1, as well as in analysing various sampling probabilities:

- $\mathcal{R}^{\mathcal{I}} := \{R^i \mid i \in \mathcal{I}\}$;
- $\mathcal{S}^{\mathcal{I}} := \{S^i \mid i \in \mathcal{I}\}$;
- $\mathcal{X}^{\mathcal{I}} := \{X^i \mid i \in \mathcal{I}\}$;
- $\widehat{\mathcal{Y}}^{\mathcal{I}} := \{\widehat{Y}^i \mid i \in \mathcal{I}\}$;
- $\mathcal{Z}^{\mathcal{I}} := \{Z^i \mid i \in \mathcal{I}\}$;
- $q_R^{\mathcal{I}} := |\mathcal{R}^{\mathcal{I}}|$;
- $q_S^{\mathcal{I}} := |\mathcal{S}^{\mathcal{I}}|$;
- $q_X^{\mathcal{I}} := |\mathcal{X}^{\mathcal{I}}|$;
- $q_{\widehat{Y}}^{\mathcal{I}} := |\widehat{\mathcal{Y}}^{\mathcal{I}}|$;
- $q_Z^{\mathcal{I}} := |\mathcal{Z}^{\mathcal{I}}|$.

Maintaining notational consistency with $\tau, \ldots, \lambda$, when $\mathcal{I} = [q]$ we drop the superscript and simply call the counting sets $\mathcal{R}, \ldots, \mathcal{Z}$ and their sizes $q_R, \ldots, q_Z$.

3.2 A brief overview of the proof strategy

We use a standard approach to bound the advantage of D with the H-Coefficient Technique. As discussed in Sect. 3.1, in the real world, at the end of the online phase, all the internal variables are released to D. In the ideal world, we need to *sample* these internal variables so that their distribution is close to that in the real world. Our proof hinges on this sampling mechanism, discussed at length in Sect. 4.1.

The basic idea behind our approach to sampling is as follows: when the online phase ends, we first sample the keys $K_1, \ldots, K_5$ randomly, so that all the inputs to P_1 and P_5 are determined. We next check for collisions with dom_1 and dom_5, and mark these collision sets as $\mathcal{I}_R$ and $\mathcal{I}_S$. We also mark the queries where an R (resp. S) in the output has collided with a previous R (resp. S). The rest of the queries we bunch together as $\mathcal{I}_*$.

The next step is to sample γ. We need to do this carefully on $\mathcal{I}_*$, since if two queries have the same R (resp. S), the Y's are forced to be different, but the $\widehat{Y}$'s can collide depending on the choice of $\widehat{S}$'s (resp. $\widehat{R}$'s). For this, we arrange the queries in a tree (we can do this since we have left the collision indices out of $\mathcal{I}_*$), and sample along this tree avoiding the $\widehat{Y}$-collision described above. For the indices outside $\mathcal{I}_*$ we can choose γ randomly, since a $\widehat{Y}$-collision together with the previous collisions will constitute a low probability event, which we classify as bad.

Once we have sampled γ for all indices, we can compute μ, which can be seen as one of the two internal strands. Here we repeat what we did in the outer layer, marking all collision indices (both with primitives and among themselves) into separate sets, and putting the remaining indices into $\mathcal{I}_{**}$. We avoid the same index lying in two distinct collision sets, which needs the careful bounding of a large number of bad events.

Then we come to the final step of the sampling, where we need to sample λ, maintaining consistency over P_2, P_3 and P_4. Again the set where we need to be cautious is $\mathcal{I}_{**}$, since the consistency being accidentally violated on any of the collision sets can be classified as a bad event. Since we have kept all the collisions out of $\mathcal{I}_{**}$, we have all the μ variables distinct. Thus, the task boils down to sampling three sets of distinct variables, each of size $q_{**} = |\mathcal{I}_{**}|$, subject to $2q_{**}$ bi-variate equations. Again we sample along the tree previously formed, manually avoiding collisions on any of the three variables. Outside $\mathcal{I}_{**}$, we again choose λ randomly.

The proof is then broken into two parts: bounding the probability of the bad events, and bounding the ratio of the good probabilities. The first task is long and tedious, but not too challenging. For lack of space, we have put these calculations in the appendix. For bounding the ratio of good probabilities, the challenge is to find a tight enough bound for probabilities of $\gamma^{\mathcal{I}_*}$ and $\lambda^{\mathcal{I}_{**}}$. Handling them separately does not give us a good enough bound. The key idea of the proof is the observation that the two balance each other in a way: for each previous query with the same R or same S, we have an extra constraint to take care of on γ, but we have one fewer constraint to worry about on λ, since we get the distinctness of Y for free when we ensure $\widehat{X}$ and $\widehat{Z}$ are distinct. We bank on this observation to bound the two together, and successfully arrive at the desired bound.

BBB Security of 5-round KAF Based on Public Random Functions from Our Results. The security bound of 5-round KAF based on public random function cannot be directly derived from our security result. Nonetheless, the proof approach for proving the security of 5-round KAF based on public random function closely follow that of ours and we believe that 5-round KAF based on public round function can be proven secured upto $2^{2n/3}$ queries. First of all, we would like to mention that masking round keys at the output of every round is not required in KAF based on public random function, because in the security analysis of public random function based KAF, adversary would not make any inverse primitive queries. Therefore, we only care about the input collision to the round function. As before, we sample the keys $K_1, \ldots, K_5$ randomly and check for collisions with dom_1 and dom_5, and mark these collision sets as $\mathcal{I}_R$ and $\mathcal{I}_S$. We also mark the queries where an R (resp. S) in the output has collided with a previous R (resp. S). The rest of the queries we bunch together as $\mathcal{I}_*$. Then one needs to accordingly compute γ and μ. Note that, in the computation of γ, we cannot say that Y values will be distinct for two different queries with same R. Similarly, for computing μ, we repeat the computation that we did in the outer layer. Moreover, we avoid the same index lying in two distinct collision sets, which needs the careful bounding of a large number of bad events. Then, our analysis is splitted into two parts, where we upper bound the probability of several bad events in the ideal world and lower bound the ratio of the real to ideal interpolation probability for a good transcript.

4 Proof of Theorem 2

We deal with three principal components in the proof: (i) the sampling procedure in the ideal world which enables us to define the transcript, (ii) defining and bounding the probability of bad transcripts and (iii) finally, lower bounding the ratio of the real to ideal interpolation

Table 2 Sampling steps in the ideal world and the corresponding bad events that can be triggered

Step name	Sampling	Bad events triggered
Step-τa	$\forall i \in \mathcal{I}_{\mathsf{enc}}, (S^i, T^i) \leftarrow_{\$} \{0,1\}^{2n}$	
Step-τb	$\forall i \in \mathcal{I}_{\mathsf{dec}}, (L^i, R^i) \leftarrow_{\$} \{0,1\}^{2n}$	
		badτ-switch, badτ-$\widehat{Y}$, badτ-3path, badτ-3coll
Step-K	$\mathbf{K} \leftarrow_{\$} \{0,1\}^{5n}$	
		bad$K$-outer, bad$K$-source
Step-γa	$\forall d \in [q_*], \gamma_*^d \leftarrow_{\$} \Gamma_*^d$	
Step-γb	$\forall S \in \mathcal{S}^{\mathcal{I}_{R*}}, \widehat{S} \leftarrow_{\$} \{0,1\}^n$	
Step-γc	$\forall R \in \mathcal{R}^{\mathcal{I}_{S*}}, \widehat{R} \leftarrow_{\$} \{0,1\}^n$	
		badγ-prim, badγ-coll, badγ-$\widehat{Y}$, badμ-in&out, badμ-source, badμ-inner, badμ-3coll, badμ-size
Step-λa	$\forall h \in [q_{**}], \lambda_{**}^h \leftarrow_{\$} \Lambda_{**}^h$	
Step-λb	$\forall X \in \mathcal{X}^{\mathcal{I}_R \sqcup \mathcal{I}_{XX}}, \widehat{X} \leftarrow_{\$} \{0,1\}^n$	
Step-λc	$\forall Z \in \mathcal{Z}^{\mathcal{I}_S \sqcup \mathcal{I}_{ZZ}}, \widehat{Z} \leftarrow_{\$} \{0,1\}^n$	
Step-λd	$\forall \widehat{Y} \in \widehat{\mathcal{Y}}^{\mathcal{I}_{\widehat{Y}\widehat{Y}}}, Y \leftarrow_{\$} \{0,1\}^n$	
Step-λe	$\forall i \in \mathcal{I}_{RR} \sqcup \mathcal{I}_{SS}, Y^i \leftarrow_{\$} \{0,1\}^n$	
		badλ-prim, badλ-coll

probability for any good transcript. We begin with the sampling procedure in the ideal world in Sect. 4.1.

4.1 Sampling procedure in the ideal world

In the online phase, every query from D is answered with a response sampled uniformly at random from $\{0,1\}^{2n}$, as shown in Step-τa and Step-τb in Table 2. (We'll refer to this table throughout this section for the exact description of the sampling steps.) This leaves D with τ at the end of the online phase. Next begins the offline sampling phase of the ideal oracle, during which $K_1, K_2, K_3, K_4, K_5, \gamma, \mu$ and λ are sampled and released to D, such that they bear the same relations between them as their counterparts in the real world, as described in Sect. 3.1.

In the rest of this section, we describe step-by-step the sampling procedure in the offline phase of the ideal world. The sampling steps are intertwined with checking for several bad events. Whenever we delineate a bad event and then either resume our description of the sampling procedure or proceed to describe further bad events, we implicitly assume that we are in the scenario where the bad event just described and all bad events described before that have not happened. Other than the usual bad events involving one or several undesirable collisions of the sampled intermediate variables either with primitive queries or between themselves, there is one specific bad event that we are keen on avoiding: for a pair of queries, say the i-th and the j-th query, with $R^i = R^j$ or $S^i = S^j$, Y^i can never equal Y^j without breaking consistency with the internal relations described earlier; however, if for the same pair of queries $\widehat{R}^i + \widehat{R}^j + \widehat{S}^i + \widehat{S}^j = L^i + L^j + T^i + T^j$, $\widehat{Y}^i$ is forced to be equal to $\widehat{Y}^j$, leading to an inconsistency in P_3. We'll avoid scenarios where this can happen, and we'll indicate this by including a $\widehat{Y}$ in the name of the corresponding bad event.

Fig. 3: badτ

badτ-switch: $\exists i, j \in [q], i < j,\ [j \in \mathcal{I}_{\mathsf{enc}}, (S^i, T^i) = (S^j, T^j)] \vee [j \in \mathcal{I}_{\mathsf{dec}}, (L^i, R^i) = (L^j, R^j)]$.

badτ-$\widehat{Y}$: $\exists i, j \in [q], i < j,\ [R^i = R^j] \wedge [S^i = S^j] \wedge [L^i + T^i = L^j + T^j]$.

badτ-3path: $\exists i, j, l \in [q], i < j < l,\ [R^i = R^j = R^l] \wedge [S^i = S^j = S^l]$.

badτ-3coll: $\exists i, j, l \in [q], i < j < l,\ [j, l \in \mathcal{I}_{\mathsf{dec}}, R^i = R^j = R^l] \vee [j, l \in \mathcal{I}_{\mathsf{enc}}, S^i = S^j = S^l]$.

Fig. 3 badτ.

Fig. 4: bad$K$

bad$K$-outer: $\mathcal{I}_R, \mathcal{I}_{RR}, \mathcal{I}_S$, and $\mathcal{I}_{SS}$ are not pairwise disjoint.

bad$K$-source: $\exists i, j \in [q], i < j,\ [i \in \mathcal{I}_S \sqcup \mathcal{I}_{SS}, j \in \mathcal{I}_{RR}, R^i = R^j] \vee [i \in \mathcal{I}_R \sqcup \mathcal{I}_{RR}, j \in \mathcal{I}_{SS}, S^i = S^j]$.

Fig. 4 bad$K$.

4.1.1 Bad events on τ

Before moving on to the online part of the sampling, we check for some bad events on τ itself. The event badτ-switch comes from the PRP-PRF switch we perform when we respond to the adversaries queries with replacement, instead of without replacement, as a permutation would do. The event badτ-$\widehat{Y}$ is the forced collision on $\widehat{Y}$ we mentioned earlier. badτ-3path involves a simultaneous 3-collision on R and S, which must involve a *path* of length 3. (For instance, one way to achieve this is as follows: an encryption query (L_1, R) giving (S, T_1); then a decryption query (S, T_2) yielding (L_2, R), making a path of length 2; and finally, a second encryption query with (L_3, R) giving (S, T_3), extending the path to length 3.) Finally, the event badτ-3coll involves a 3-collision on R or S where the last two come from oracle outputs. The precise definitions of these bad events are given in Fig. 3.

4.1.2 Sampling K and bad events thereof

Once none of the bad events on τ has happened, we move on to the offline phase of the sampling. Let $\mathcal{I}_{RR} := \{i \in \mathcal{I}_{\mathsf{dec}} \mid R^i = R^j \text{ for some } j \in [i-1]\}$ and $\mathcal{I}_{SS} := \{i \in \mathcal{I}_{\mathsf{enc}} \mid S^i = S^j \text{ for some } j \in [i-1]\}$ be the index-sets where an R or S obtained from an oracle response collides with a previously seen one (either as part of a query or as part of a response).

The first step in the offline phase is to sample the keys K_1, K_2, K_3, K_4 and K_5 independently and uniformly at random from $\{0,1\}^n$. This determines all the inputs to P_1 and P_5. We define the index-sets $\mathcal{I}_R := \{i \in [q] \mid R^i + K_1 \in \mathsf{dom}_1\}$ and $\mathcal{I}_S := \{i \in [q] \mid S^i + K_5 \in$

$\mathsf{dom}_5\}$, where the outputs of P_1 and P_5 are already determined from ρ, where recall that ρ is the tuple of the primitive queries and responses.

Sampling the keys can trigger two bad events: bad$K$-outer is the event when an encryption query index lies in two of the sets $\mathcal{I}_R$, $\mathcal{I}_S$, and $\mathcal{I}_{SS}$ at the same time, or a decryption query index lies in two of the sets $\mathcal{I}_R$, $\mathcal{I}_S$, and $\mathcal{I}_{RR}$ at the same time; and bad$K$-source, where the *source* of a collision index in $\mathcal{I}_{RR}$ (resp. $\mathcal{I}_{SS}$) (the earlier R (resp. S) value where it collided) lies in one of $\mathcal{I}_R$, $\mathcal{I}_S$, and $\mathcal{I}_{SS}$ (resp. $\mathcal{I}_{RR}$). The definitions can be found in Fig. 4.

4.1.3 Defining and computing $G[\tau_*]$

When sampling γ, we begin with $\mathcal{I}_*$. Since queries in $\mathcal{I}_*$ do not come from another collision event, we need to avoid bad collision events manually while sampling $\gamma^{\mathcal{I}_*}$.

Define $\tau_* := \tau^{\mathcal{I}_*}$, $\mathcal{R}_* := \mathcal{R}^{\mathcal{I}_*}$, $\mathcal{S}_* := \mathcal{S}^{\mathcal{I}_*}$. Consider the directed bipartite graph $G[\tau_*]$ with vertices in $\mathcal{R}_*$ and $\mathcal{S}_*$, where we put an edge between $R \in \mathcal{R}_*$ and $S \in \mathcal{S}_*$ if there is a query $i \in \mathcal{I}_*$ with $R^i = R$ and $S^i = S$; the direction of the edge is from R to S if $i \in \mathcal{I}_{\mathsf{enc}}* := \mathcal{I}_{\mathsf{enc}} \cap \mathcal{I}_*$ and S to R if $i \in \mathcal{I}_{\mathsf{dec}}* := \mathcal{I}_{\mathsf{dec}} \cap \mathcal{I}_*$.

Since we are in $\mathcal{I}_*$, we know that there are no cycles in $G[\tau_*]$, making it a forest. Let M be the number of trees in $G[\tau_*]$. Define $q_* := |\mathcal{I}_*|$, $q_{R*} := |\mathcal{R}_*|$, $q_{S*} := |\mathcal{S}_*|$. Since $G[\tau_*]$ has $q_{S*} + q_{R*}$ vertices and q_* edges, we have

$$q_{R*} + q_{S*} = q_* + M. \tag{2}$$

We observe further that a new tree is added to this forest exactly on each query in the set $\{i \in \mathcal{I}_{\mathsf{enc}}* \mid R^i \notin \mathcal{R}^{[i-1]}\} \sqcup \{i \in \mathcal{I}_{\mathsf{dec}}* \mid S^i \notin \mathcal{S}^{[i-1]}\}$, i.e., on each encryption query in $\mathcal{I}_*$ with a fresh R and each decryption query in $\mathcal{I}_*$ with a fresh S; we call the resulting trees R-rooted (with root R^i) and S-rooted (with root S^i) respectively.

We label $\mathcal{R}_*$ and $\mathcal{S}_*$ as follows: first, the trees are arranged in query order of the roots; next, within each tree, we begin with the root and do a breadth-first traversal, discovering R-generations and S-generations alternately. Finally, we order $\mathcal{R}_*$ and $\mathcal{S}_*$ separately, first by trees, then within the same tree by generations, then within the same generation by parents' order, and finally among siblings by order of appearance. This gives us a total order on both $\mathcal{R}_*$ and $\mathcal{S}_*$, and allow us to label them $R_1, \ldots, R_{q_{R*}}$ and $S_1, \ldots, S_{q_{S*}}$ respectively. We also extend the notation $\widehat{R}_\ell := \widehat{R^i}$ for i such that $R_\ell = R^i$, and $\widehat{S}_m := \widehat{S^i}$ for i such that $S_m = S^i$.

We will also find it convenient to refer to the queries by the end-labels of the edge it corresponds to: a query $i \in \mathcal{I}_{\mathsf{enc}}*$ with $R^i = R_\ell$ and $S^i = S_m$ will be referred to as (ℓ, m), while a query $i \in \mathcal{I}_{\mathsf{dec}}*$ with $S^i = S_m$ and $R^i = R_\ell$ will be referred to as (m, ℓ). We order the queries as follows: two encryption queries (ℓ, m) and (ℓ', m') have the same order as m and m', while two decryption queries (m, ℓ) and (m', ℓ') have the same order as ℓ and ℓ'; finally, to compare an encryption query (ℓ, m) and a decryption query (m', ℓ') we note that they must be either in different trees, or in different generations of the same tree, and order them as we ordered the vertices in the corresponding cases. Figure 5 illustrates the forest structure.

For each $i \in \mathcal{I}_*$, let d_i denote the rank of i in the new ordering. Then $i \mapsto d_i$ is a bijection from $\mathcal{I}_*$ to $[q_*]$. We'll use $d = d_i$ interchangeably with the end-labels (ℓ, m) or (m, ℓ) to refer to a query in $\mathcal{I}_*$. We write ℓ^d and m^d to denote the end-labels of d, irrespective of the direction of the query. (Note that we'll often write rank to mean the rank of some node in this ordering; it is not to be confused with the rank of a matrix.)

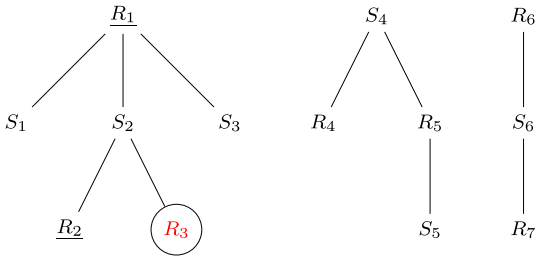


Fig. 5 The forest structure on $\mathcal{I}_*$. For instance, the node R_3 (here circled) represents a decryption query (S_2, T) for some T, that outputs (L, R_3) for some L. This is the first query where R_3 appears, and to count the number of earlier queries in which S_2 appears, we only need to look at this node's grandparent and elder siblings (R_1 and R_2 respectively, here underlined)

4.1.4 Sampling γ

Before sampling γ, we set the values already determined from primitive collisions: for each $i \in \mathcal{I}_R$ we set $\widehat{R}^i \leftarrow V_1^j + K_1$ where j is such that $U_1^j = R^i + K_1$; and for each $i \in \mathcal{I}_S$ we set $\widehat{S}^i \leftarrow V_5^j + K_5$ where j is such that $U_5^j = S^i + K_5$. Using the graph $G[\tau_*]$, we describe a sampling mechanism for $\gamma^{\mathcal{I}_*}$. For $\mathcal{I} \subseteq \mathcal{I}_*$ we call a $\gamma^{\mathcal{I}}$ *valid* if it satisfies the following conditions:

- $\widehat{R}^i + K_1 \notin \mathsf{ran}_1$ for each $i \in \mathcal{I} \backslash \mathcal{I}_R$;
- $\widehat{S}^i + K_5 \notin \mathsf{ran}_5$ for each $i \in \mathcal{I} \backslash \mathcal{I}_S$;

and for each distinct $i, j \in \mathcal{I}$:

- $R^i = R^j \iff \widehat{R}^i = \widehat{R}^j$;
- $S^i = S^j \iff \widehat{S}^i = \widehat{S}^j$;
- $R^i = R^j \implies \widehat{S}^i + \widehat{S}^j \neq L^i + T^i + L^j + T^j$;
- $S^i = S^j \implies \widehat{R}^i + \widehat{R}^j \neq L^i + T^i + L^j + T^j$.

Let $d_{\mathcal{I}} := \{d_i \mid i \in \mathcal{I}\}$. Let $\gamma_*^{d_i} := \gamma^i$ for each $i \in \mathcal{I}_*$, and $\gamma_*^{d_{\mathcal{I}}} := \gamma^{\mathcal{I}}$ for any $\mathcal{I} \subseteq \mathcal{I}_*$. Let Γ_{good} be the set $\{\gamma^{\mathcal{I}} \mid \mathcal{I} \subseteq \mathcal{I}_*, \gamma^{\mathcal{I}} \text{ is valid}\}$. Given a $\gamma_*^{[d-1]} \in \Gamma_{\mathsf{good}}$, let $\Gamma_*^d := \Gamma_*^d[\gamma_*^{[d-1]}]$ be the set of values that γ_*^d can take, such that $\gamma_*^{[d]}$ remains in Γ_{good}. We note that unless the edge corresponding to query d begins in a root node, one half of γ_*^d will already be fixed from $\gamma_*^{[d-1]}$. For instance, for a query (ℓ^d, m^d) with a non-root source R_{ℓ^d}, there is a previous query (m^c, ℓ^c) with $c < d$ such that $R_{\ell^c} = R_{\ell^d}$, so $\widehat{R}_{\ell^d}$ is determined from γ_*^c. For this case, each value in Γ_*^d will look like $(\widehat{R}_{\ell^c}, \widehat{S})$ for some candidate value $\widehat{S}$ for $\widehat{S}_{m^d}$.

Then we sample $\gamma^{\mathcal{I}_*} = \gamma_*^{[q_*]}$ as follows: for each $d \in [q*]$, having sampled $\gamma_*^{[d-1]}$, we sample γ_*^d uniformly at random from Γ_*^d. This is shown as Step-γa in Table 2. Then we proceed to compute the index sets $\mathcal{I}_{R*} := \{i \in \mathcal{I}_R \sqcup \mathcal{I}_{RR} \mid S^i \notin \mathcal{S}_*\}$ and $\mathcal{I}_{S*} := \{i \in \mathcal{I}_S \sqcup \mathcal{I}_{SS} \mid R^i \notin \mathcal{R}_*\}$. Finally, for each $S \in \mathcal{S}^{\mathcal{I}_{R*}}$ (resp. $R \in \mathcal{R}^{\mathcal{I}_{S*}}$), we sample $\widehat{S}$ (resp. $\widehat{R}$) uniformly at random from $\{0,1\}^n$, as shown in Step-γb (resp. Step-γc) in Table 2. This completes our sampling of γ.

4.1.5 Bad events on γ

The bad events on γ come from evaluating the conditions for $\gamma^{\mathcal{I}_*}$ being valid on the entire γ. badγ-prim arises from a primitive collision outside on the range of P_1 (resp. P_5) outside

Fig. 6: badγ

badγ-prim: $\exists i \in [q],\ [i \in \mathcal{I}_R^c, \widehat{R}^i + K_1 \in \mathsf{ran}_1] \vee [i \in \mathcal{I}_S^c, \widehat{S}^i + K_5 \in \mathsf{ran}_5]$.

badγ-coll: $\exists i, j \in [q], i < j,\ [[R^i \neq R^j] \wedge [\widehat{R}^i = \widehat{R}^j]] \vee [[S^i \neq S^j] \wedge [\widehat{S}^i = \widehat{S}^j]]$.

badγ-$\widehat{Y}$: $\exists i, j \in [q], i < j,\ [[R^i = R^j] \wedge [\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j]] \vee [[S^i = S^j] \wedge [\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j]]$.

Fig. 6 badγ.

Fig. 7: badμ

badμ-in&out: $\mathcal{I}_{\text{outer}} \cap \mathcal{I}_{\text{inner}} \neq \emptyset$.

badμ-source: $\exists i, j \in [q],\ [i \in \mathcal{I}_R, j \in \mathcal{I}_{XX}, X^i = X^j] \vee [i \in \mathcal{I}_S, j \in \mathcal{I}_{ZZ}, Z^i = Z^j]$.

badμ-inner: $\mathcal{I}_X$, $\mathcal{I}_{XX}$, $\mathcal{I}_{\widehat{Y}}$, $\mathcal{I}_{\widehat{Y}\widehat{Y}}$, $\mathcal{I}_Z$ and $\mathcal{I}_{ZZ}$ are not pairwise disjoint.

badμ-3coll: $\exists i, j, l \in \mathcal{I}_{\text{inner}}, i < j < l,\ [X^i = X^j = X^l] \vee [\widehat{Y}^i = \widehat{Y}^j = \widehat{Y}^l] \vee [Z^i = Z^j = Z^l]$.

badμ-size: $|\mathcal{I}_{\text{inner}}| > \sqrt{q}$.

Fig. 7 badμ.

$\mathcal{I}_R$ (resp. $\mathcal{I}_S$). badγ-coll is the event of a collision of $\widehat{R}$ (resp. $\widehat{S}$) on two distinct values of R (resp. S). Finally, badγ-$\widehat{Y}$ is the event of a collision on $\widehat{R} + \widehat{S} + L + T$ on two queries with the same R or same S (both of which forces Y to be distinct on these two queries). The definitions can be found in Fig. 6.

4.1.6 Bad events on μ

Next we compute μ from τ and γ using the equations in Sect. 3.1. Define the collision sets $\mathcal{I}_X := \{i \in [q] \mid X^i + K_2 \in \mathsf{dom}_2\}$, $\mathcal{I}_{\widehat{Y}} := \{i \in [q] \mid \widehat{Y}^i + K_3 \in \mathsf{ran}_3\}$, $\mathcal{I}_Z := \{i \in [q] \mid Z^i + K_4 \in \mathsf{dom}_4\}$, $\mathcal{I}_{XX} := \{i \in \mathcal{I}_R^c \mid X^i = X^j \text{ for some } j \in [q]\}$, $\mathcal{I}_{\widehat{Y}\widehat{Y}} := \{i \in [q] \mid \widehat{Y}^i = \widehat{Y}^j \text{ for some } j \in [q]\}$, $\mathcal{I}_{ZZ} := \{i \in \mathcal{I}_S^c \mid Z^i = Z^j \text{ for some } j \in [q]\}$. Further define $\mathcal{I}_{\text{outer}} := \mathcal{I}_R \cup \mathcal{I}_{RR} \cup \mathcal{I}_S \cup \mathcal{I}_{SS}$ and $\mathcal{I}_{\text{inner}} := \mathcal{I}_X \cup \mathcal{I}_{XX} \cup \mathcal{I}_{\widehat{Y}} \cup \mathcal{I}_{\widehat{Y}\widehat{Y}} \cup \mathcal{I}_Z \cup \mathcal{I}_{ZZ}$, and $\mathcal{I}_{**} := \mathcal{I}_* \backslash \mathcal{I}_{\text{inner}}$. The event bad$\mu$-in&out occurs when one of the outer collision indices in $\mathcal{I}_{\text{outer}}$ is also in $\mathcal{I}_{\text{inner}}$. The event bad$\mu$-inner occurs when an index lies at once in two inner collision sets $\mathcal{I}_X$, $\mathcal{I}_{XX}$, $\mathcal{I}_{\widehat{Y}}$, $\mathcal{I}_{\widehat{Y}\widehat{Y}}$, $\mathcal{I}_Z$ and $\mathcal{I}_{ZZ}$. badμ-source checks for a collision index in $\mathcal{I}_{XX}$ (resp. $\mathcal{I}_{ZZ}$) with its source index in $\mathcal{I}_R$ (resp. $\mathcal{I}_S$). (Note that unlike in bad$K$-source, the

query-order of these two indices is not important here.) badμ-3coll captures 3-collisions on any of the variables X, $\widehat{Y}$ or Z. Finally, badμ-size is the event that the set of inner collisions grows too big. The definitions can be found in Fig. 7.

4.1.7 Sampling $\boldsymbol{\lambda}$

Before sampling λ, we set the values already determined from primitive collisions: for each $i \in \mathcal{I}_X$ we set $\widehat{X}^i \leftarrow V_2^j + K_2$ where j is such that $U_2^j = X^i + K_2$; for each $i \in \mathcal{I}_{\widehat{Y}}$ we set $Y^i \leftarrow V_3^j + K_3$ where j is such that $U_3^j = \widehat{Y}^i + K_3$; and for each $i \in \mathcal{I}_Z$ we set $\widehat{Z}^i \leftarrow V_4^j + K_4$ where j is such that $U_4^j = Z^i + K_4$. To describe a sampling mechanism for $\lambda^{\mathcal{I}_{**}}$, we return to the graph $G[\tau_*]$. For $\mathcal{I} \subseteq \mathcal{I}_{**}$ we call a $\lambda^{\mathcal{I}}$ *valid* if it satisfies the following conditions:

- $\widehat{X}^i + K_2 \notin \mathsf{ran}_2$ for each $i \in \mathcal{I} \setminus \mathcal{I}_X$;
- $Y^i + K_3 \notin \mathsf{dom}_3$ for each $i \in \mathcal{I} \setminus \mathcal{I}_{\widehat{Y}}$;
- $\widehat{Z}^i + K_4 \notin \mathsf{ran}_4$ for each $i \in \mathcal{I} \setminus \mathcal{I}_Z$.
- $\widehat{X}^i + Y^i = R^i$ for each $i \in \mathcal{I}$;
- $Y^i + \widehat{Z}^i = S^i$ for each $i \in \mathcal{I}$;

and for each distinct $i, j \in \mathcal{I}$:

- $X^i = X^j \iff \widehat{X}^i = \widehat{X}^j$;
- $\widehat{Y}^i = \widehat{Y}^j \iff Y^i = Y^j$;
- $Z^i = Z^j \iff \widehat{Z}^i = \widehat{Z}^j$.

Define $q_{**} := |\mathcal{I}_{**}|$. Suppose we take the relabeled queries $1, \ldots, q_*$, drop the queries pertaining to $\mathcal{I}_* \setminus \mathcal{I}_{**}$, and renumber the remaining indices $1, \ldots, q_{**}$. We call h_i the index of query i under this new renumbering. Thus, h_i is obtained by subtracting from d_i the number of queries in $[d_i - 1]$ that come from outside $\mathcal{I}_{**}$. Let $h_{\mathcal{I}} := \{h_i \mid i \in \mathcal{I}\}$. Let $\lambda_{**}^{h_i} := \lambda^i$ for any $i \in \mathcal{I}_{**}$, and $\lambda_{**}^{h_{\mathcal{I}}} := \lambda^{\mathcal{I}}$ for any $\mathcal{I} \subseteq \mathcal{I}_{**}$. Let Λ_{good} be the set $\{\lambda^{\mathcal{I}} \mid \mathcal{I} \subseteq \mathcal{I}_{**}, \lambda^{\mathcal{I}} \text{ is valid}\}$. Given a $\lambda_{**}^{[h-1]} \in \Lambda_{\mathsf{good}}$, let $\Lambda_{**}^h := \Lambda_{**}^h[\lambda_{**}^{[h-1]}]$ be the set of values λ_{**}^h can take such that $\lambda_{**}^{[h]}$ remains in Λ_{good}.

Then we sample $\lambda^{\mathcal{I}_{**}} = \lambda_{**}^{[q_{**}]}$ as follows: for each $h \in [q_{**}]$, having sampled $\lambda_{**}^{[h-1]}$, we sample λ_{**}^h uniformly at random from Λ_{**}^h. This is shown as Step-λa in Table 2. Sampling the rest of λ is straightforward: for each distinct X on $\mathcal{I}_R \sqcup \mathcal{I}_{XX}$, $\widehat{X}$ is sampled uniformly at random from $\{0,1\}^n$ (Step-λb); and we similarly sample $\widehat{Z}$ for each distinct Z on $\mathcal{I}_S \sqcup \mathcal{I}_{ZZ}$ (Step-λc) and Y for each distinct $\widehat{Y}$ on $\mathcal{I}_{\widehat{Y}\widehat{Y}}$ (Step-λd). Finally, for each query in $\mathcal{I}_{RR} \sqcup \mathcal{I}_{SS}$, we sample Y^i uniformly at random. Since fixing one of the variables in λ^i determines the other two, this completes the sampling of λ, and brings us to the end of our sampling procedure.

4.1.8 Bad events on $\boldsymbol{\lambda}$

The bad events on λ come from evaluating the conditions for $\lambda^{\mathcal{I}_*}$ being valid on the entire λ. badλ-prim arises from a primitive collision outside on the range of P_2 (resp. domain of P_3; range of P_4) outside $\mathcal{I}_X$ (resp. $\mathcal{I}_{\widehat{Y}}$; $\mathcal{I}_Z$). badλ-coll is the event of a collision of $\widehat{X}$ (resp. Y; $\widehat{Z}$) on two distinct values of X (resp. $\widehat{Y}$; Z). The definitions can be found in Fig. 8.

Fig. 8: badλ

badλ-prim: $\exists i \in [q], [i \in \mathcal{I}^c_{\widehat{X}}, \widehat{X}^i + K_2 \in \mathsf{ran}_2] \vee [i \in \mathcal{I}^c_{\widehat{Y}}, Y^i + K_3 \in \mathsf{dom}_3] \vee [i \in \mathcal{I}^c_{\widehat{Z}}, \widehat{Z}^i + K_4 \in \mathsf{ran}_4]$.

badλ-coll: $\exists i, j \in [q], i < j, [[X^i \neq X^j] \wedge [\widehat{X}^i = \widehat{X}^j]] \vee [[\widehat{Y}^i \neq \widehat{Y}^j] \wedge [Y^i = Y^j]] \vee [[Z^i \neq Z^j] \wedge [\widehat{Z}^i = \widehat{Z}^j]]$.

Fig. 8 badλ.

4.1.9 Definition of bad transcripts, bad lemma and good lemma

In this sampling procedure, if none of the above bad events happen, we release all the internal variables, i.e., γ, μ, λ and the round keys $(K_1, K_2, K_3, K_4, K_5)$ along with the input–output query responses (L, R, S, T) to the adversary. After the interaction is over with the construction oracle and the primitive oracles, we summarize the interaction in a *transcript* that records all the inputs and outputs of the interaction along with the corresponding internal variables, i.e, $\eta = (\rho, \tau, \mathbf{K}, \gamma, \mu, \lambda)$, where $\tau = \{(L^i, R^i, S^i, T^i) : i \in [q]\}$ and $\rho = \{(U^i_1, V^i_1), (U^i_2, V^i_2), \ldots, (U^i_{q_i}, V^i_{q_i}) : i \in [5]\}$, where U^i_j (resp. V^i_j) is the j-th primitive input (resp. primitive output) to the i-th permutation P_i.

Definition 1 (*Bad Transcript*) A transcript $\eta = (\rho, \tau, \mathbf{K}, \gamma, \mu, \lambda)$ is said to be bad if any of the above bad events i.e., badτ, badK, badγ, badμ, badλ happen.

Lemma 1 (Bad Lemma) *Let $\eta = (\rho, \tau, \mathbf{K}, \gamma, \mu, \lambda)$ be any attainable transcript. Let X_{id} and Θ_{b} be defined as above. Then*

$$\begin{aligned}\Pr[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{b}}] \leq\ & \frac{6q^2}{N^2} + \frac{14q^3}{N^2} + \frac{4q^4}{N^3} + \frac{2q^3}{N^3}(q_1 + q_5) + \frac{q^{1/2}}{N}(q_2 + q_3 + q_4) + \frac{2q^{3/2}}{N} \\ & + \frac{2qq_1q_5}{N^2} + \frac{q^2}{N^2}(11q_1 + 12q_2 + 12q_3 + 12q_4 + 11q_5) \\ & + \frac{q}{N^2}(2q_1q_2 + q_1q_5 + 3q_2q_3 + 2q_2q_4 + 3q_2q_5 + 2q_1q_3 + 3q_3q_4 \\ & + 2q_3q_5 + 3q_1q_4 + 2q_4q_5).\end{aligned}$$

By assuming q_1, q_2, q_3, q_4 and q_5 roughly in the order of q, then we have

$$\Pr[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{b}}] \leq \frac{6q^2}{N^2} + \frac{97q^3}{N^2} + \frac{8q^4}{N^3} + \frac{5q^{3/2}}{N}.$$

This lemma is proved by an exhaustive case-by-case analysis of all the listed bad events and all possible sub-events that give rise to them. The trickiest part of the proof is to bound the probability of badγ, which is given below. Due to the limits on the number of pages, we have postponed the (more straightforward) remainder of the proof of the bad lemma to Appendix A.

4.2 Bounding badγ-prim

Proposition 1 *Having defined the bad event* badγ-prim *in Fig. 6, we have*

$$\Pr[bad\gamma - prim] \leq \frac{qq_5(q_1+q_2)}{N^2} + \frac{(q_1+q_5)\binom{q}{2}}{N^2}.$$

Now, to bound badγ-prim, we further split it into the following two cases:

- badγ-prim-1. $\exists i \in \mathcal{I}_{R*}$ and $j \in [q_5]$ such that $\widehat{S}^i + K_1 = V_5^j$.
- badγ-prim-2. $\exists i \in \mathcal{I}_{S*}$ and $j \in [q_1]$ such that $\widehat{R}^i + K_1 = V_1^j$.

4.2.1 Bounding badγ-prim-1

We split the event into the following sub-cases and bound the probabilities of each of them.

- badγ-prim-1a. $\exists i \in \mathcal{I}_{R*} \cap \mathcal{I}_R$ and $j \in [q_5]$ such that $\widehat{S}^i + k_5 = V_5^j$.
  In other words, $\exists i \in q$, $j \in [q_5]$ and $l \in [q_2]$ such that $R^i + K_1 = U_1^l$ and $\widehat{S}^i + K_5 = V_5^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events comes out to be $(1/N)$ due to the n-bit randomness over the keys K_1 and K_5 respectively. As we can choose the indices i, j and l in q, q_5 and q_2 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 1a] \leq \frac{qq_2q_5}{N^2}. \tag{3}$$

- badγ-prim-1b. $\exists i \in \mathcal{I}_{R*} \cap \mathcal{I}_{RR}$ and $j \in [q_5]$ such that $\widehat{S}^i + K_5 = V_5^j$.
  In other words, $\exists i \in \mathcal{I}_{\mathsf{dec}}$, $j \in [q_5]$ and $l \in [i-1]$ such that $R^i = R^l$ and $\widehat{S}^i + K_5 = V_5^j$. Let's first fix the values for the indices i, j and l. The probability of the event $R^i = R^l$ comes out to be $(1/N)$ due to the n-bit randomness over R^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{dec}}$. The probability of the event $\widehat{S}^i + K_5 = V_5^j$ comes out to be $(1/N)$ due to the n-bit randomness over the key K_5. As we can choose the pair of indices (i,l) in $\binom{q}{2}$ ways and the index j in q_5 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 1b] \leq \frac{q_5\binom{q}{2}}{N^2}. \tag{4}$$

Adding the probabilities of the above two cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 1] \leq \frac{qq_2q_5}{N^2} + \frac{q_5\binom{q}{2}}{N^2}. \tag{5}$$

4.2.2 Bounding badγ-prim-2

As before, we split the event into the following sub-cases and bound the probabilities of each of them.

- badγ-prim-2a. $\exists i \in \mathcal{I}_{S*} \cap \mathcal{I}_S$ and $j \in [q_1]$ such that $\widehat{R}^i + K_1 = V_1^j$.
  In other words, $\exists i \in q$, $j \in q_1$ and $l \in q_2$ such that $S^i + K_5 = V_5^l$ and $\widehat{R}^i + K_1 = V_1^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events comes out to be $(1/N)$ due to the n-bit randomness over the keys K_1 and K_5 respectively.

As we can choose the indices i, j and l in q, q_5 and q_1 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 2a] \leq \frac{qq_1q_5}{N^2}. \tag{6}$$

– $\mathsf{bad}\gamma$-prim-2b. $\exists i \in \mathcal{I}_{S*} \cap \mathcal{I}_{SS}$ and $j \in [q_1]$ such that $\widehat{R}^i + K_1 = V_1^j$.
In other words, $\exists i \in \mathcal{I}_{\mathsf{enc}}$, $j \in [q_1]$ and $l \in [i-1]$ such that $S^i = S^l$ and $\widehat{R}^i + K_1 = V_1^j$. Let's first fix the values for the indices i, j and l. The probability of the event $S^i = S^l$ comes out to be $(1/N)$ due to the n-bit randomness over S^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{enc}}$. The probability of the event $\widehat{R}^i + K_1 = V_1^j$ comes out to be $(1/N)$ due to the n-bit randomness over the key K_1. As we can choose the pair of indices (i, l) in $\binom{q}{2}$ ways and the index j in q_1 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 2b] \leq \frac{q_1\binom{q}{2}}{N^2}. \tag{7}$$

Adding the probabilities of the above two cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim} - 2] \leq \frac{qq_1q_5}{N^2} + \frac{q_1\binom{q}{2}}{N^2}. \tag{8}$$

By combining Eqs. (5) and (8), we have

$$\Pr[\mathsf{bad}\gamma - \mathsf{prim}] \leq \frac{qq_5(q_1+q_2)}{N^2} + \frac{(q_1+q_5)\binom{q}{2}}{N^2}. \tag{9}$$

4.3 Bounding badγ-coll

Proposition 2 *Having defined the bad event* $\mathsf{bad}\gamma$*-coll in Fig. 6, we have*

$$\Pr[bad\gamma - coll] \leq \frac{q^2(q_1+q_5)}{N^2} + \frac{4q^4}{N^3} + \frac{2q^3(q_1+q_5)}{N^3}.$$

As before, to bound $\mathsf{bad}\gamma$-coll, we further split it into the following two cases:

– $\mathsf{bad}\gamma$-coll-1. $\exists i, j \in \mathcal{I}_{R*}$ and $i \neq j$ such that $S^i \neq S^j$ and $\widehat{S}^i = \widehat{S}^j$.
– $\mathsf{bad}\gamma$-coll-2. $\exists i, j \in \mathcal{I}_{S*}$ and $i \neq j$ such that $R^i \neq R^j$ and $\widehat{R}^i = \widehat{R}^j$.

4.3.1 Bounding badγ-coll-1

As before, we split the event into the following sub-cases and bound the probabilities of each of them.

– $\mathsf{bad}\gamma$-coll-1a. $\exists i, j \in \mathcal{I}_{R*} \cap \mathcal{I}_R$ and $i \neq j$ such that $S^i \neq S^j$ and $\widehat{S}^i = \widehat{S}^j$.
In other words, $\exists i, j \in \mathcal{I}_R$, such that $i \neq j$, and $k, l \in [q_1]$ such that

$$R^i + K_1 = U_1^k, R^j + K_1 = U_1^l, \widehat{S}^i = \widehat{S}^j.$$

We can write the above event in an equivalent way as

$$R^i + K_1 = U_1^k, R^i + R^j = U_1^k + U_1^l, \widehat{S}^i = \widehat{S}^j.$$

Let's first fix the values for the indices i, j, k and l and without loss of generality, we assume that $i > j$. The probability of the event $R^i + K_1 = U_1^k$ comes out to be $(1/N)$

due to the n-bit randomness over the key K_1. Moreover, the probability of the event $\widehat{S}^i = \widehat{S}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{S}^i$. However, the number of choices of indices (i, j, k, l) such that $R^i + R^j = U_1^k + U_1^l$ holds is at most $\binom{q}{2} q_1$. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 1a] \leq \frac{2q_1\binom{q}{2}}{N^2} \leq \frac{q^2 q_1}{N^2}\,. \tag{10}$$

– $\mathsf{bad}\gamma$-coll-1b. $\exists i, j \in \mathcal{I}_{R*} \cap \mathcal{I}_{RR}$ and $i \neq j$ such that $S^i \neq S^j$ and $\widehat{S}^i = \widehat{S}^j$.
In other words, $\exists i, j \in \mathcal{I}_{RR}$, such that $i \neq j \in \mathcal{I}_{\mathsf{dec}}$, and $k \in [i-1], l \in [j-1]$ such that

$$R^i = R^k, R^j = R^l, \widehat{S}^i = \widehat{S}^j.$$

Let's first fix the values for the indices i, j, k and l. The probability of the first two events $R^i = R^k$ and $R^j = R^l$ comes out to be $(1/N^2)$ due to the n-bit randomness over R^i and R^j. Moreover, the probability of the event $\widehat{S}^i = \widehat{S}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{S}^i$. However, the number of choices of indices (i, j, k, l) is at most q^4. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 1b] \leq \frac{2q^4}{N^3}\,. \tag{11}$$

– $\mathsf{bad}\gamma$-coll-1c. $\exists i \in \mathcal{I}_{R*} \cap \mathcal{I}_R$ and $j \in \mathcal{I}_{R*} \cap \mathcal{I}_{RR}$ such that $S^i \neq S^j$ and $\widehat{S}^i = \widehat{S}^j$.
In other words, $\exists i \in \mathcal{I}_R$, $j \in \mathcal{I}_{RR}$, such that $i \neq j$ and $j \in \mathcal{I}_{\mathsf{dec}}$, and $k \in [q_1], l \in [j-1]$ such that

$$R^i + K_1 = U_1^k, R^j = R^l, \widehat{S}^i = \widehat{S}^j.$$

Let's first fix the values for the indices i, j, k and l. The probability of the first two events $R^i + K_1 = U_1^k$ and $R^j = R^l$ comes out to be $(1/N^2)$ due to the n-bit randomness over k_1 and R^j. Moreover, the probability of the event $\widehat{S}^i = \widehat{S}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{S}^i$. However, the number of choices of indices (i, j, l) is at most q^3 and the number of choices for k is at most q_1. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 1c] \leq \frac{2q^3 q_1}{N^3}\,. \tag{12}$$

Adding the probabilities of the above three cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 1] \leq \frac{q^2 q_1}{N^2} + \frac{2q^4}{N^3} + \frac{2q^3 q_1}{N^3}\,. \tag{13}$$

4.3.2 Bounding **badγ-coll-2**

As before, we split the event into the following sub-cases and bound the probabilities of each of them.

– $\mathsf{bad}\gamma$-coll-2a. $\exists i, j \in \mathcal{I}_{S*} \cap \mathcal{I}_S$ and $i \neq j$ such that $R^i \neq R^j$ and $\widehat{R}^i = \widehat{R}^j$.
In other words, $\exists i, j \in \mathcal{I}_S$, such that $i \neq j$, and $k, l \in [q_5]$ such that

$$S^i + K_5 = U_5^k, S^j + K_5 = U_5^l, \widehat{R}^i = \widehat{R}^j.$$

We can write the above event in an equivalent way as

$$S^i + K_5 = U_5^k, S^i + S^j = U_5^k + U_5^l, \widehat{R}^i = \widehat{R}^j.$$

Let's first fix the values for the indices i, j, k and l and without loss of generality, we assume that $i > j$. The probability of the event $S^i + K_5 = U_5^k$ comes out to be $(1/N)$ due to the n-bit randomness over the key K_5. Moreover, the probability of the event $\widehat{R}^i = \widehat{R}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{R}^i$. However, the number of choices of indices (i, j, k, l) such that $S^i + S^j = U_5^k + U_5^l$ holds is at most $\binom{q}{2} q_5$. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 2a] \leq \frac{2q_5\binom{q}{2}}{N^2} \leq \frac{q^2 q_5}{N^2}. \tag{14}$$

– $\mathsf{bad}\gamma$-coll-$2b$. $\exists i, j \in \mathcal{I}_{S*} \cap \mathcal{I}_{SS}$ and $i \neq j$ such that $R^i \neq R^j$ and $\widehat{R}^i = \widehat{R}^j$.
In other words, $\exists i, j \in \mathcal{I}_{SS}$, such that $i \neq j \in \mathcal{I}_{\mathsf{enc}}$, and $k \in [i-1], l \in [j-1]$ such that

$$S^i = S^k, S^j = S^l, \widehat{R}^i = \widehat{R}^j.$$

Let's first fix the values for the indices i, j, k and l. The probability of the first two events $S^i = S^k$ and $S^j = S^l$ comes out to be $(1/N^2)$ due to the n-bit randomness over S^i and S^j. Moreover, the probability of the event $\widehat{R}^i = \widehat{R}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{R}^i$. However, the number of choices of indices (i, j, k, l) is at most q^4. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 2b] \leq \frac{2q^4}{N^3}. \tag{15}$$

– $\mathsf{bad}\gamma$-coll-$2c$. $\exists i \in \mathcal{I}_{S*} \cap \mathcal{I}_S$ and $j \in \mathcal{I}_{S*} \cap \mathcal{I}_{SS}$ such that $R^i \neq R^j$ and $\widehat{R}^i = \widehat{R}^j$.
In other words, $\exists i \in \mathcal{I}_S, j \in \mathcal{I}_{SS}$, such that $i \neq j$ and $j \in \mathcal{I}_{\mathsf{enc}}$, and $k \in [q_5], l \in [j-1]$ such that

$$S^i + K_5 = U_5^k, S^j = S^l, \widehat{R}^i = \widehat{R}^j.$$

Let's first fix the values for the indices i, j, k and l. The probability of the first two events $S^i + K_5 = U_5^k$ and $S^j = S^l$ comes out to be $(1/N^2)$ due to the n-bit randomness over K_5 and S^j. Moreover, the probability of the event $\widehat{R}^i = \widehat{R}^j$ comes out to be at most $2/N$ due to the randomness of $\widehat{R}^i$. However, the number of choices of indices (i, j, l) is at most q^3 and the number of choices for k is at most q_5. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 2c] \leq \frac{2q^3 q_5}{N^3}. \tag{16}$$

Adding the probabilities of the above three cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll} - 2] \leq \frac{q^2 q_5}{N^2} + \frac{2q^4}{N^3} + \frac{2q^3 q_5}{N^3}. \tag{17}$$

By combining Eqs. (13) and (17), we have

$$\Pr[\mathsf{bad}\gamma - \mathsf{coll}] \leq \frac{q^2(q_1 + q_5)}{N^2} + \frac{4q^4}{N^3} + \frac{2q^3(q_1 + q_5)}{N^3}. \tag{18}$$

4.4 Bounding badγ-$\widehat{Y}$

Proposition 3 *Having defined the bad event* badγ-$\widehat{Y}$ *in Fig. 6, we have*

$$\Pr[bad\gamma - \widehat{Y}] \leq \frac{4q^2(q_1+q_5)}{N^2} + \frac{4q^3}{N^2}.$$

As before, to bound badγ-$\widehat{Y}$, we further split it into the following two cases:

- badγ-$\widehat{Y}$-1. $\exists i \in \mathcal{I}_*^c$, $j \in [q]$ and $i \neq j$ such that $R^i = R^j$ and $\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j$.
- badγ-$\widehat{Y}$-2. $\exists i \in \mathcal{I}_*^c$, $j \in [q]$ and $i \neq j$ such that $S^i = S^j$ and $\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j$.

4.4.1 Bounding badγ-$\widehat{Y}$-1

As before, we split the event into the following sub-cases and bound the probabilities of each of them.

- badγ-$\widehat{Y}$-1a $\exists i \in \mathcal{I}_R$, $j \in [q]$ and $i \neq j$ such that $R^i = R^j$ and $\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j$.
  In other words, $\exists i \in \mathcal{I}_R$, $j \in [q]$, with $i \neq j$ and $k \in [q_1]$ such that
  $$R^i + K_1 = U_1^k, R^i = R^j, \hat{S}^i + \hat{S}^j = L^i + T^i + L^j + T^j.$$
  Let's first fix the values for the indices i, j and k. The probability of the first event comes from the n-bit randomness over K_1 and the probability of the last event comes from the randomness over $\hat{S}^i$. Hence, the joint probability comes out to be at most $(2/N^2)$. However, the number of choices of indices i and j is at most $\binom{q}{2}$ and the number of choices for k is at most q_1. By using the union bound over all those possible choices to obtain
  $$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 1a] \leq \frac{q^2 q_1}{N^2}. \tag{19}$$
- badγ-$\widehat{Y}$-1b. $\exists i \in \mathcal{I}_S$, $j \in [q]$ and $i \neq j$ such that $R^i = R^j$ and $\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j$.
  In other words, $\exists i \in \mathcal{I}_S$, $j \in [q]$, with $i \neq j$ and $k \in [q_5]$ such that
  $$S^i + K_5 = U_5^k, R^i = R^j, \hat{S}^i + \hat{S}^j = L^i + T^i + L^j + T^j.$$
  Now, we consider that $j \in \mathcal{I}_S$, as the analysis of this case is the involved one. Therefore, we have
  $$S^i + K_5 = U_5^k, S^j + K_5 = U_5^l, R^i = R^j, V_5^k + V_5^l = L^i + T^i + L^j + T^j, \tag{20}$$
  for some $l \in [q_5]$ and we equivalently write Eq. (20) as
  $$S^i + K_5 = U_5^k, S^i + S^j = U_5^k + U_5^l, R^i = R^j, V_5^k + V_5^l = L^i + T^i + L^j + T^j. \tag{21}$$
  Now, we analyze this case in separate subcases:
  Case (a): We first assume the construction queries appear after the primitive queries and let $i < j$ and let j be an encryption query index (analysis for j to be a decryption query will be similar). Then from the first equation we use the randomness of K_5 and from the second equation, we use the randomness of S^j which allows us to bound the

probability of the event for a fixed choice of indices, to at most $2/N^2$. Moreover, the number of tuples (i, j, k, l) such that Eq. (21) holds is at most $\binom{q}{2}$ for choices of i and j and the number of choices for k is at most q_5 which leaves a unique choice for l such that $V_5^k + V_5^l = L^i + T^i + L^j + T^j$ holds. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_5/N^2$.

Case (b): Now, we consider the case where the primitive queries appear after the construction queries and let $k < l$ and let l be a forward query index. Then from the first equation we use the randomness of K_5 and from the fourth equation, we use the randomness of V_5^l which allows us to bound the probability of the event for a fixed choice of indices, to at most $2/N^2$. Moreover, the number of tuples (i, j, k, l) such that Eq. (21) holds is at most $\binom{q}{2}$ for choices of i and j and the number of choices for k is at most q_5 which leaves a unique choice for l such that $S^i + S^j = U_5^k + U_5^l$ holds. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_5/N^2$.

Case (c): Similarly, if l is an inverse query index. Then from the first equation we use the randomness of K_5 and from the second equation, we use the randomness of U_5^l which allows us to bound the probability of the event for a fixed choice of indices, to at most $2/N^2$. Moreover, the number of tuples (i, j, k, l) such that Eq. (21) holds is at most $\binom{q}{2}$ for choices of i and j and the number of choices for k is at most q_5 which leaves a unique choice for l such that $V_5^k + V_5^l = L^i + T^i + L^j + T^j$ holds. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_5/N^2$.

By taking the union of all the above cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 1b] \leq \frac{3q^2 q_5}{N^2}. \tag{22}$$

– $\mathsf{bad}\gamma$-$\widehat{Y}$-1c. $\exists i \in \mathcal{I}_{RR}$, $j \in [q]$ and $i \neq j$ such that $R^i = R^j$ and $\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j$.

In other words, $\exists i \in \mathcal{I}_{RR}$, $j \in [q]$, with $i \neq j$ and $i \in \mathcal{I}_{\mathsf{dec}}$ and $k \in [i-1]$ such that

$$R^i = R^k, R^i = R^j, \hat{S}^i + \hat{S}^j = L^i + T^i + L^j + T^j.$$

Let's first fix the values for the indices i, j and k. The probability of the first event comes from the n-bit randomness over R^i and the probability of the last event comes from the randomness over $\hat{S}^i$. Hence, the joint probability comes out to be at most $(2/N^2)$. However, the number of choices of indices i and j is at most $\binom{q}{2}$ and the number of choices for k is at most q. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 1c] \leq \frac{q^3}{N^2}. \tag{23}$$

– $\mathsf{bad}\gamma$-$\widehat{Y}$-1d. $\exists i \in \mathcal{I}_{SS}$, $j \in [q]$ and $i \neq j$ such that $R^i = R^j$ and $\widehat{S}^i + \widehat{S}^j = L^i + T^i + L^j + T^j$.

Analysis of this case is identical to the analysis of $\mathsf{bad}\gamma$-$\widehat{Y}$-1c., where we use the randomness of S^i as $i \in \mathcal{I}_{\mathsf{enc}}$. Hence, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 1d] \leq \frac{q^3}{N^2}. \tag{24}$$

Adding the probabilities of the above four cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 1] \leq \frac{q^2(q_1 + 3q_5)}{N^2} + \frac{2q^3}{N^2}. \tag{25}$$

4.4.2 Bounding badγ-$\widehat{Y}$-2

As before, we split the event into the following sub-cases and bound the probabilities of each of them.

– badγ-$\widehat{Y}$-2a. $\exists i \in \mathcal{I}_R$, $j \in [q]$ and $i \neq j$ such that $S^i = S^j$ and $\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j$.
In other words, $\exists i \in \mathcal{I}_R$, $j \in [q]$, with $i \neq j$ and $k \in [q_1]$ such that

$$R^i + K_1 = U_1^k, S^i = S^j, \widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j.$$

Now, we consider that $j \in \mathcal{I}_R$ as this the analysis of this case is the involved one. Therefore, we have

$$R^i + K_1 = U_1^k, R^j + K_1 = U_1^l, S^i = S^j, V_1^k + V_1^l = L^i + T^i + L^j + T^j, \quad (26)$$

for some $l \in [q_1]$ and we equivalently write Eq. (26) as

$$R^i + K_1 = U_1^k, R^i + R^j = U_1^k + U_1^l, S^i = S^j, V_1^k + V_1^l = L^i + T^i + L^j + T^j. \quad (27)$$

Now, we analyze this case in separate subcases:
Case (a) As before, we assume the construction queries appear after the primitive queries and let $i < j$ and let j be an encryption query index (analysis for j to be a decryption query will be similar). Then from the first equation we use the randomness of K_1 and from the third equation, we use the randomness of S^j which allows us to bound the probability of the event for a fixed choice of indices, to at most $2/N^2$. Moreover, the number of tuples (i, j, k, l) such that Eq. (27) holds is at most $\binom{q}{2}$ for choices of i and j and the number of choices for k is at most q_1 which leaves a unique choice for l such that $V_1^k + V_1^l = L^i + T^i + L^j + T^j$ holds. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_1/N^2$.
Case (b) Analysis for this case is exactly identical to the case (b) of bounding badγ-$\widehat{Y}$-1c. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_1/N^2$.
Case (c) Analysis for this case is exactly identical to the case (c) of bounding badγ-$\widehat{Y}$-1c. Therefore, by varying all possible choices of indices, we bound the probability to at most $q^2 q_1/N^2$.
By taking the union of all the above cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 2a] \leq \frac{3q^2 q_1}{N^2}. \quad (28)$$

– badγ-$\widehat{Y}$-2b. $\exists i \in \mathcal{I}_S$, $j \in [q]$ and $i \neq j$ such that $S^i = S^j$ and $\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j$.
In other words, $\exists i \in \mathcal{I}_S$, $j \in [q]$, with $i \neq j$ and $k \in [q_5]$ such that

$$S^i + K_5 = U_5^k, R^i = R^j, \widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j.$$

Let's first fix the values for the indices i, j and k. The probability of the first event comes from the n-bit randomness over K_5 and the probability of the last event comes from the randomness over $\widehat{R}^i$. Hence, the joint probability comes out to be at most $(2/N^2)$. However, the number of choices of indices i and j is at most $\binom{q}{2}$ and the number of choices for k is at most q_5. By using the union bound over all those possible choices to

obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 2b] \leq \frac{q^2 q_5}{N^2}\,. \tag{29}$$

– $\mathsf{bad}\gamma$-$\widehat{Y}$-2c. $\exists i \in \mathcal{I}_{RR}$, $j \in [q]$ and $i \neq j$ such that $S^i = S^j$ and $\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j$.
In other words, $\exists i \in \mathcal{I}_{RR}$, $j \in [q]$, with $i \neq j$ and $i \in \mathcal{I}_{\mathsf{dec}}$ and $k \in [i-1]$ such that

$$R^i = R^k, S^i = S^j, \hat{R}^i + \hat{R}^j = L^i + T^i + L^j + T^j.$$

Let's first fix the values for the indices i, j and k. The probability of the first event comes from the n-bit randomness over R^i and the probability of the last event comes from the randomness over $\hat{R}^i$. Hence, the joint probability comes out to be at most $(2/N^2)$. However, the number of choices of indices i and j is at most $\binom{q}{2}$ and the number of choices for k is at most q. By using the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 2c] \leq \frac{q^3}{N^2}\,. \tag{30}$$

– $\mathsf{bad}\gamma$-$\widehat{Y}$-2d. $\exists i \in \mathcal{I}_{SS}$, $j \in [q]$ and $i \neq j$ such that $S^i = S^j$ and $\widehat{R}^i + \widehat{R}^j = L^i + T^i + L^j + T^j$.
Analysis of this case is identical to the analysis of $\mathsf{bad}\gamma$-$\widehat{Y}$-2c., where we use the randomness of S^i as $i \in \mathcal{I}_{\mathsf{enc}}$. Hence, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 2d] \leq \frac{q^3}{N^2}\,. \tag{31}$$

Adding the probabilities of the above four cases, we obtain

$$\Pr[\mathsf{bad}\gamma - \widehat{Y} - 2] \leq \frac{q^2(3q_1 + q_5)}{N^2} + \frac{2q^3}{N^2}\,. \tag{32}$$

By combining Eqs. (25) and (32), we have

$$\Pr[\mathsf{bad}\gamma - \widehat{Y}] \leq \frac{4q^2(q_1 + q_5)}{N^2} + \frac{4q^3}{N^2}. \tag{33}$$

5 Bounding the ratio of good probabilities

Lemma 2 *Let $\eta = (\rho, \tau, \mathbf{K}, \gamma, \mu, \lambda)$ be any attainable transcript such that $\eta \in \Theta_{\mathrm{g}}$. Let X_{re} and X_{id} be defined as above. Suppose $q_1 + 2(\sqrt{q}+1) \leq q_2 + q_3 + q_4$, $q_5 + 2(\sqrt{q}+1) \leq q_2 + q_3 + q_4$ and $q + (q_1 + q_2 + \cdots + q_5) \leq N/2$. Then, we have*

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}} = \eta]}{\Pr[\mathsf{X}_{\mathrm{id}} = \eta]} \geq 1 - \left(\frac{6q^3 + 4q^2(q_2+q_3+q_4) + 2qq_2q_3 + 2qq_2q_4 + 2qq_3q_4}{N^2} + \frac{8q^{3/2}}{N}\right).$$

Proof Let $\eta = (\rho, \tau, \mathbf{K}, \gamma, \mu, \lambda)$ be a good transcript. We'll calculate the exact probability of obtaining η in the real world, and an upper bound on its probability in the ideal world. □

5.1 Real world

In the real world, there are N^5 choices for $\mathbf{K}$. Let Q_j denote the number of distinct queries to P_j for each $j \in [5]$. We first set aside the q_j primitive queries to P_j for each j, and hereafter count the additional distinct queries to each P_j that comes from the construction queries.

P_1 gets q_{R*} distinct queries in $\mathcal{I}_*$, and $q_R^{\mathcal{I}_{S*}}$ distinct queries in $\mathcal{I}_S$; and P_5 gets q_{S*} distinct queries in $\mathcal{I}_*$, and $q_S^{\mathcal{I}_{R*}}$ distinct queries in $\mathcal{I}_R$. Thus we have

$$Q_1 = q_1 + q_{R*} + q_R^{\mathcal{I}_{S*}}, \tag{34}$$

$$Q_5 = q_5 + q_{S*} + q_S^{\mathcal{I}_{R*}}. \tag{35}$$

For P_2, there are $q_X^{\mathcal{I}_R} + |\mathcal{I}_S|$ distinct queries in $\mathcal{I}_{\text{outer}}$, $|\mathcal{I}_{XX}|/2$ distinct queries in $\mathcal{I}_{XX}$, and $q_* - |\mathcal{I}_X| - |\mathcal{I}_{XX}|$ distinct queries in $\mathcal{I}_* \setminus (\mathcal{I}_X \cup \mathcal{I}_{XX})$, bringing the total to

$$\begin{aligned} &q_X^{\mathcal{I}_R} + |\mathcal{I}_S| + |\mathcal{I}_{XX}|/2 + q_* - |\mathcal{I}_X| - |\mathcal{I}_{XX}| \\ &= q_X^{\mathcal{I}_R} + |\mathcal{I}_S| + q - |\mathcal{I}_R| - |\mathcal{I}_S| - |\mathcal{I}_X| - |\mathcal{I}_{XX}|/2 \\ &= q - |\mathcal{I}_X| - |\mathcal{I}_{XX}|/2 - |\mathcal{I}_R| + q_X^{\mathcal{I}_R}. \end{aligned}$$

By a similar argument, we have $q - |\mathcal{I}_Z| - |\mathcal{I}_{ZZ}|/2 - |\mathcal{I}_S| + q_Z^{\mathcal{I}_S}$ distinct queries to P_4 in the construction queries. This gives us

$$Q_2 = q_2 + q - |\mathcal{I}_X| - |\mathcal{I}_{XX}|/2 - |\mathcal{I}_R| + q_X^{\mathcal{I}_R}, \tag{36}$$

$$Q_4 = q_4 + q - |\mathcal{I}_Z| - |\mathcal{I}_{ZZ}|/2 - |\mathcal{I}_S| + q_Z^{\mathcal{I}_S}. \tag{37}$$

Finally we note that all queries to P_3 outside $\mathcal{I}_{\widehat{Y}} \cup \mathcal{I}_{\widehat{Y}\widehat{Y}}$ are distinct, and in addition there are $|\mathcal{I}_{\widehat{Y}\widehat{Y}}|/2$ distinct queries in $\mathcal{I}_{\widehat{Y}\widehat{Y}}$. This gives us

$$Q_3 = q_3 + q - |\mathcal{I}_{\widehat{Y}}| - |\mathcal{I}_{\widehat{Y}\widehat{Y}}|/2. \tag{38}$$

We have

$$\Pr[\mathsf{X}_{\text{re}} = \eta] = \frac{1}{N^5} \cdot \frac{1}{(N)_{Q_1}} \cdot \frac{1}{(N)_{Q_2}} \cdot \frac{1}{(N)_{Q_3}} \cdot \frac{1}{(N)_{Q_4}} \cdot \frac{1}{(N)_{Q_5}}, \tag{39}$$

with $Q_1, \ldots, Q_5$ as in Eqs. (34)–(38). (We'll substitute the expressions later in Eq. (39) when cancelling out the terms.)

5.2 Ideal world

In the ideal world, we first observe that ρ, τ, $\mathbf{K}$ are sampled independently of everything else, γ is sampled conditioned on $(\rho, \tau, \mathbf{K})$, and λ is sampled conditioned on $(\rho, \tau, \mathbf{K}, \gamma)$. This gives

$$\Pr[\mathsf{X}_{\text{id}} = \eta] = \Pr_{\mathcal{O}_{\text{id}}}[\rho] \cdot \Pr_{\mathcal{O}_{\text{id}}}[\tau] \cdot \Pr_{\mathcal{O}_{\text{id}}}[\mathbf{K}] \cdot \Pr_{\mathcal{O}_{\text{id}}}[\gamma \mid \rho, \tau, \mathbf{K}] \cdot \Pr_{\mathcal{O}_{\text{id}}}[\lambda \mid \rho, \tau, \mathbf{K}, \gamma, \mu]. \tag{40}$$

Primitive queries are answered honestly, giving

$$\Pr_{\mathcal{O}_{\text{id}}}[\rho] = \frac{1}{(N)_{q_1}} \cdot \frac{1}{(N)_{q_2}} \cdot \frac{1}{(N)_{q_3}} \cdot \frac{1}{(N)_{q_4}} \cdot \frac{1}{(N)_{q_5}}. \tag{41}$$

Next, from Step-τa and Step-τb of the sampling, we get

$$\Pr_{\mathcal{O}_{\mathrm{id}}}[\tau] = \frac{1}{N^{2q}}, \tag{42}$$

and from Step-K, we get

$$\Pr_{\mathcal{O}_{\mathrm{id}}}[\mathbf{K}] = \frac{1}{N^5}. \tag{43}$$

5.2.1 A bound for γ

We recall that the tricky part of sampling γ is how we sample it over $\mathcal{I}_*$. For each $d \in [q_*]$ we try to find an upper bound for the probability of sampling γ_*^d given $\gamma_*^{[d-1]}$ has already been sampled. We define

$$a_d := \min_{\gamma_*^{[d-1]}} \left| \Gamma_*^d \left[\gamma_*^{[d-1]} \right] \right|. \tag{44}$$

Then Step-γa gives

$$\Pr_{\mathcal{O}_{\mathrm{id}}} \left[\gamma_*^d \mid \rho, \tau, \mathbf{K}, \gamma_*^{[d-1]} \right] \leq \frac{1}{a_d}. \tag{45}$$

Substituting Eq. (44) in Eq. (45) and taking the product over $d \in [q_*]$ gives

$$\Pr_{\mathcal{O}_{\mathrm{id}}} \left[\gamma^{\mathcal{I}_*} \mid \rho, \tau, \mathbf{K} \right] = \Pr_{\mathcal{O}_{\mathrm{id}}} \left[\gamma_*^{[q_*]} \mid \rho, \tau, \mathbf{K} \right] \leq \prod_{d=1}^{q_*} \frac{1}{a_d}. \tag{46}$$

This takes care of $\gamma^{\mathcal{I}_*}$. In $\mathcal{I}_{\mathrm{outer}}$, Step-$\gamma$b and Step-$\gamma$c involve taking uniform samples of size $q_S^{\mathcal{I}_{R*}}$ and $q_R^{\mathcal{I}_{S*}}$, so we have

$$\Pr_{\mathcal{O}_{\mathrm{id}}} \left[\gamma^{\mathcal{I}_{R*} \sqcup \mathcal{I}_{S*}} \mid \rho, \tau, \mathbf{K} \right] = \frac{1}{N^{q_S^{\mathcal{I}_{R*}} + q_R^{\mathcal{I}_{S*}}}}. \tag{47}$$

From Eqs. (46) and (47) we get

$$\Pr_{\mathcal{O}_{\mathrm{id}}}[\gamma \mid \rho, \tau, \mathbf{K}] \leq \left(\prod_{d=1}^{q_*} \frac{1}{a_d} \right) \cdot \frac{1}{N^{q_S^{\mathcal{I}_{R*}} + q_R^{\mathcal{I}_{S*}}}}. \tag{48}$$

5.2.2 A bound for λ

Again we recall that the tricky part of sampling λ is over $\mathcal{I}_{**}$. For each $h \in [q_{**}]$ we try to find an upper bound for the probability of sampling λ_{**}^h given $\lambda_{**}^{[h-1]}$ has already been sampled. We define

$$b_h := \min_{\lambda_{**}^{[h-1]}} \left| \Lambda_{**}^h \left[\lambda_{**}^{[h-1]} \right] \right|. \tag{49}$$

Then Step-λa gives

$$\Pr_{\mathcal{O}_{\mathrm{id}}} \left[\lambda_{**}^h \mid \rho, \tau, \mathbf{K}, \gamma, \mu, \lambda_{**}^{[h-1]} \right] \leq \frac{1}{b_h}. \tag{50}$$

From the definition of b_h and by taking the product of Eq. (50) over $h \in [q_{**}]$ gives

$$\Pr_{\mathcal{O}_{\mathrm{id}}} \left[\lambda^{\mathcal{I}_{**}} \mid \rho, \tau, \mathbf{K}, \gamma, \mu \right] = \Pr_{\mathcal{O}_{\mathrm{id}}} \left[\lambda_{**}^{[q_{**}]} \mid \rho, \tau, \mathbf{K}, \gamma, \mu \right] \leq \prod_{h=1}^{q_{**}} \frac{1}{b_h}. \tag{51}$$

This takes care of $\lambda^{\mathcal{I}_{**}}$. On $\mathcal{I}_{\text{outer}}$ and $\mathcal{I}_{\text{inner}}$, in Step-$\lambda$b we take a uniform sample of size $|\mathcal{X}^{\mathcal{I}_R \sqcup \mathcal{I}_{XX}}| = q_X^{\mathcal{I}_R} + |\mathcal{I}_{XX}|/2$, so that

$$\Pr_{\mathcal{O}_{\text{id}}}\left[\lambda^{\mathcal{I}_R \sqcup \mathcal{I}_{XX}} \mid \rho, \tau, \mathbf{K}, \gamma, \mu\right] = \frac{1}{N^{q_X^{\mathcal{I}_R} + |\mathcal{I}_{XX}|/2}}; \tag{52}$$

similarly from Step-λc we get

$$\Pr_{\mathcal{O}_{\text{id}}}\left[\lambda^{\mathcal{I}_S \sqcup \mathcal{I}_{ZZ}} \mid \rho, \tau, \mathbf{K}, \gamma, \mu\right] = \frac{1}{N^{q_Z^{\mathcal{I}_S} + |\mathcal{I}_{ZZ}|/2}}; \tag{53}$$

and finally, Step-λd and Step-λe give

$$\Pr_{\mathcal{O}_{\text{id}}}\left[\lambda^{\mathcal{I}_{\widehat{Y}\widehat{Y}}} \mid \rho, \tau, \mathbf{K}, \gamma, \mu\right] = \frac{1}{N^{|\mathcal{I}_{RR}| + |\mathcal{I}_{SS}|}} \tag{54}$$

To keep the combined exponent of N readable, we'll use the notation

$$q^{\dagger} := q_X^{\mathcal{I}_R} + q_Z^{\mathcal{I}_S} + |\mathcal{I}_{RR}| + |\mathcal{I}_{SS}| + (|\mathcal{I}_{XX}| + |\mathcal{I}_{\widehat{Y}\widehat{Y}}| + |\mathcal{I}_{ZZ}|)/2. \tag{55}$$

Combining Eqs. (51), (52), (53), and (54) and substituting Eq. (55) yields

$$\Pr_{\mathcal{O}_{\text{id}}}[\lambda \mid \rho, \tau, \mathbf{K}, \gamma, \mu] \le \left(\prod_{h=1}^{q_{**}} \frac{1}{b_h}\right) \cdot \frac{1}{N^{q^{\dagger}}}. \tag{56}$$

5.3 Bounding the ratio

Plugging Eqs. (41), (42), (48), and (56) in Eq. (40) gives

$$\begin{aligned}\Pr_{\mathcal{O}_{\text{id}}}[\eta] \le \frac{1}{(N)_{q_1}} \cdot \frac{1}{(N)_{q_2}} \cdot \frac{1}{(N)_{q_3}} \cdot \frac{1}{(N)_{q_4}} \cdot \frac{1}{(N)_{q_5}} \cdot \frac{1}{N^5} \cdot \frac{1}{N^{2q}} \\ \cdot \left(\prod_{d=1}^{q_*} \frac{1}{a_d}\right) \cdot \frac{1}{N^{q_S^{\mathcal{I}_{R*}} + q_R^{\mathcal{I}_{S*}}}} \cdot \left(\prod_{h=1}^{q_{**}} \frac{1}{b_h}\right) \cdot \frac{1}{N^{q^{\dagger}}}.\end{aligned} \tag{57}$$

From Eqs. (39) and (57), on writing $(N)_{Q_j}/(N)_{q_j}$ as $(N-q_j)_{Q_j - q_j}$ for each $j \in [5]$ and denoting $N_j := N - q_j$ and $Q_j^{\dagger} := Q_j - q_j$, we can calculate the H-ratio of η as

$$\mathsf{H}[\eta] := \frac{\Pr[\mathsf{X}_{\text{re}} = \eta]}{\Pr[\mathsf{X}_{\text{id}} = \eta]} \ge \frac{N^{q_S^{\mathcal{I}_{R*}} + q_R^{\mathcal{I}_{S*}}} \cdot \prod_{d=1}^{q_*} a_d}{(N_1)_{Q_1^{\dagger}} (N_5)_{Q_5^{\dagger}}} \cdot \frac{N^{2q+q^{\dagger}} \cdot \prod_{h=1}^{q_{**}} b_h}{(N_2)_{Q_2^{\dagger}} (N)_{Q_3^{\dagger}} (N_4)_{Q_4^{\dagger}}}. \tag{58}$$

Note that, we have

$$\begin{aligned}Q_2 - q_2 &= q - |\mathcal{I}_X| - |\mathcal{I}_{XX}|/2 - |\mathcal{I}_R| + q_X^{\mathcal{I}_R} \\ &= q_{**} + q_X^{\mathcal{I}_R} + |\mathcal{I}_{RR}| + |\mathcal{I}_S| + |\mathcal{I}_{SS}| \\ &\quad + |\mathcal{I}_{XX}|/2 + |\mathcal{I}_{\widehat{Y}}| + |\mathcal{I}_{\widehat{Y}\widehat{Y}}| + |\mathcal{I}_Z| + |\mathcal{I}_{ZZ}|,\end{aligned} \tag{59}$$

so

$$(N_2)_{Q_2^{\dagger}} \le (N_2)_{q_{**}} N^{q_X^{\mathcal{I}_R} + |\mathcal{I}_{XX}|/2 + |\mathcal{I}_{RR}| + |\mathcal{I}_S| + |\mathcal{I}_{SS}| + |\mathcal{I}_{\widehat{Y}}| + |\mathcal{I}_{\widehat{Y}\widehat{Y}}| + |\mathcal{I}_Z| + |\mathcal{I}_{ZZ}|}. \tag{60}$$

Similarly,

$$(N_3)_{Q_3^{\dagger}} \le (N_3)_{q_{**}} N^{|\mathcal{I}_{RR}| + |\mathcal{I}_{SS}| + |\mathcal{I}_{\widehat{Y}\widehat{Y}}|/2 + |\mathcal{I}_R| + |\mathcal{I}_S| + |\mathcal{I}_X| + |\mathcal{I}_{XX}| + |\mathcal{I}_Z| + |\mathcal{I}_{ZZ}|}, \tag{61}$$

$$(N_4)_{Q_4^\dagger} \le (N_4)_{q_{**}} N^{q_Z^{\mathcal{I}_S} + |\mathcal{I}_{ZZ}|/2 + |\mathcal{I}_R| + |\mathcal{I}_{RR}| + |\mathcal{I}_{SS}| + |\mathcal{I}_Z| + |\mathcal{I}_{ZZ}| + |\mathcal{I}_{\widehat{Y}}| + |\mathcal{I}_{\widehat{Y}\widehat{Y}}|}. \tag{62}$$

We observe that the exponents of N on the right-hand-side of Eqs. (60), (61), and (62) add up to $2(q - q_{**}) + q^\dagger$. Multiplying Eqs. (60), (61), and (62) gives

$$(N_2)_{Q_2^\dagger}(N_3)_{Q_3^\dagger}(N_4)_{Q_4^\dagger} \le (N_2)_{q_{**}}(N_3)_{q_{**}}(N_4)_{q_{**}} N^{2q-2q_{**}+q^\dagger}. \tag{63}$$

It follows that

$$\frac{N^{2q+q^\dagger}}{(N_2)_{Q_2^\dagger}(N_3)_{Q_3^\dagger}(N_4)_{Q_4^\dagger}} \ge \frac{N^{2q_{**}}}{(N_2)_{q_{**}}(N_3)_{q_{**}}(N_4)_{q_{**}}}. \tag{64}$$

Since $(N_1)_{Q_1^\dagger} \le (N_1)_{q_{R*}} N^{q_R^{\mathcal{I}_{S*}}}$ and $(N_5)_{Q_5^\dagger} \le (N_5)_{q_{S*}} N^{q_S^{\mathcal{I}_{R*}}}$, we also have

$$\frac{N^{q_S^{\mathcal{I}_{R*}} + q_R^{\mathcal{I}_{S*}}}}{(N_1)_{Q_1^\dagger}(N_5)_{Q_5^\dagger}} \ge \frac{1}{(N_1)_{q_{R*}}(N_5)_{q_{S*}}}. \tag{65}$$

Substituting Eqs. (64) and (65) in Eq. (58) gives

$$\mathsf{H}[\eta] \ge \frac{N^{2q_{**}} \prod_{h=1}^{q_{**}} b_h}{(N_2)_{q_{**}}(N_3)_{q_{**}}(N_4)_{q_{**}}} \cdot \frac{\prod_{d=1}^{q_*} a_d}{(N_1)_{q_{R*}}(N_5)_{q_{S*}}}. \tag{66}$$

We count $\prod_d a_d \cdot \prod_h b_h$ on each tree in sequence. Let $q^{(j)}$ be the number of queries in the j-th tree, and define $q_{R*}^{(j)} := |\{\ell \in [q_{R*}] \mid R_\ell \text{ is on the } j\text{-th tree}\}|$, $q_{S*}^{(j)} := |\{m \mid S_m \text{ is on the } j\text{-th tree}\}|$. Also define the cumulative sums

$$q^{+(j)} := \sum_{l=1}^{j} q^{(l)}, \qquad q_{R*}^{+(j)} := \sum_{l=1}^{j} q_{R*}^{(l)}, \qquad q_{S*}^{+(j)} := \sum_{l=1}^{j} q_{S*}^{(l)}. \tag{67}$$

By our ordering, the queries in the j-th tree are precisely the ones with labels $d_1^{(j)} := q^{+(j-1)} + 1, \ldots, d_{q^{(j)}}^{(j)} := q^{+(j)}$.

5.3.1 Bounding a_d

First we consider the root node of the j-th tree. Here both R and S are fresh, so we do not have to worry about $\mathsf{bad}\gamma$-$\widehat{Y}$. We just have to exclude the ranges of P_1 and P_5 sampled in primitive queries and earlier trees, giving

$$a_{d_1^{(j)}} \ge \left(N_1 - q_{R*}^{+(j-1)}\right) \cdot \left(N_5 - q_{S*}^{+(j-1)}\right). \tag{68}$$

For a query $d_k^{(j)}$ let $t^{d_k^{(j)}}$ be the number of elder siblings of its target node, plus the number of grandparents (0 for root or second-generation nodes and 1 for all subsequent nodes). Then, for an encryption query $d_k^{(j)}$, the number of earlier nodes with the same R (which can potentially give rise to $\mathsf{bad}\gamma$-$\widehat{Y}$) is exactly $t^{d_k^{(j)}}$, and the number of distinct $\widehat{S}$ already sampled before this node is $m^{d_k^{(j)}} - 1$. Thus we have

$$a_{d_k^{(j)}} \ge N_5 - \left(m^{d_k^{(j)}} - 1\right) - t^{d_k^{(j)}}, \tag{69}$$

Reasoning similarly for a decryption query $d_k^{(j)}$ we get

$$a_{d_k^{(j)}} \geq N_1 - \left(\ell^{d_k^{(j)}} - 1\right) - t^{d_k^{(j)}}. \tag{70}$$

We note that Eqs. (69) and (70) do not depend on the tree except for the count t^d, and can simply be written as

$$a_d \geq N_5 - (m^d - 1) - t^d \tag{71}$$

and

$$a_d \geq N_1 - (\ell^d - 1) - t^d \tag{72}$$

for non-root encryption and decryption queries respectively. Similarly, Eq. (68) can be written as

$$a_d \geq \left(N_1 - (\ell^d - 1)\right)\left(N_5 - (m^d - 1)\right) \tag{73}$$

for root queries, where $t^d = 0$. Let $t(\ell)$ (resp. $t(m)$) be defined as t^d where d is the first query (in the tree ordering) where R_ℓ (resp. S_m) appears. Then

$$\prod_{d=1}^{q_*} a_d \geq \prod_{\ell=1}^{q_{R*}} [N_1 - (\ell - 1) - t(\ell)] \cdot \prod_{m=1}^{q_{S*}} [N_5 - (m - 1) - t(m)]. \tag{74}$$

5.3.2 Bounding b_h

For $h \in [q_{**}]$ let t_{**}^h be the number of elder siblings of its target node that come from $\mathcal{I}_{**}$, plus the number of grandparents that come from $\mathcal{I}_{**}$. While sampling λ_{**}^h, we need to maintain the three validity conditions on $\widehat{X}$, Y, and $\widehat{Z}$; since X, $\widehat{Y}$, and Z are all distinct on $\mathcal{I}_{**}$, we need to avoid collisions on $\widehat{X}$, Y, and $\widehat{Z}$ as well. For each of these three, in addition to the primitive queries, $h - 1$ distinct values have been sampled in the earlier nodes (in the tree-ordering), giving a total of $q_2 + q_3 + q_4 + 3(h - 1)$ candidates to avoid.

However, it turns out we can do slightly better. The key observation here is that for all earlier nodes with the same R or same S as this node, we avoid one of the three collisions for free! (For instance, $R^i = R^{i'}$ and $\widehat{X}^i \neq \widehat{X}^{i'}$ automatically imply that $Y^i = \widehat{X}^i + R^i \neq \widehat{X}^{i'} + R^{i'} = Y^{i'}$.) Thus, for the t_{**}^h earlier nodes with the same R or same S, we have one collision less to worry about. This shows that

$$b_h \geq N - (q_2 + q_3 + q_4) - 3(h - 1) + t_{**}^h. \tag{75}$$

Denote $N_{234} := N - (q_2 + q_3 + q_4)$. Taking product over $[q_{**}]$ yields

$$\prod_{h=1}^{q_{**}} b_h \geq \prod_{h=1}^{q_{**}} \left[N_{234} - 3(h - 1) + t_{**}^h\right]. \tag{76}$$

This t_{**}^h term that we save here is crucial for the proof, as we use it to cancel out the corresponding $-t_*^d$ in the bound for a_d. That leaves us with reasonably simple bounds which we can approximate using standard techniques.

However, we still need to be careful, because $\mathcal{I}_{**}$ is slightly smaller than $\mathcal{I}_*$, which means that (i) each t_{**}^h will be slightly smaller than the corresponding t_*^d, and (ii) there will be slightly fewer t_{**}^h terms than $-t_*^d$ terms, leaving a few $-t_*^d$ terms that we can cancel out. Fortunately, the restrictions we have put in the bad events will be enough to bound these corner cases. We devote the rest of the section to deriving this concrete bound.

5.3.3 Completing the proof

For $i \in \mathcal{I}_{**}$ (returning for the moment to the original query-order labelling), we look at $a_{d_i} b_{h_i}$. Suppose i is a non-root encryption query. Then from Eqs. (71) and (75) we get

$$a_{d_i} b_{h_i} \geq \left[N_5 - (m^{d_i} - 1) - t^{d_i}\right] \cdot \left[N_{234} - 3(h_i - 1) + t_{**}^{h_i}\right]. \tag{77}$$

We want to transfer the $t_{**}^{h_i}$ from the right parentheses to the left. For any N', N'', to claim $N'(N'' + t_{**}^{h_i}) \geq (N' + t_{**}^{h_i})N''$, we just need to show that $N' \geq N''$ (since $t_{**}^{h_i}$ is positive). Here we have $N' = N_5 - (m^{d_i} - 1) - t^{d_i} = N - [q_5 + (m^{d_i} - 1) + t^{d_i}]$ and $N'' = N_{234} - 3(h_i - 1) = N - [(q_2 + q_3 + q_4) + 3(h_i - 1)]$, so we just need to show that $(q_2 + q_3 + q_4) + 3(h_i - 1) \geq q_5 + (m^{d_i} - 1) + t^{d_i}$. Since $m^{d_i} \leq d_i$, and $t^{d_i} \leq d_i$, we get

$$\begin{aligned}
&q_2 + q_3 + q_4 + 3(h_i - 1) - q_5 - (m^{d_i} - 1) - t^{d_i} \\
&\quad \geq q_2 + q_3 + q_4 + 3h_i - 3 - q_5 - d_i + 1 - d_i \\
&\quad \geq q_2 + q_3 + q_4 - 2(d_i - h_i) - q_5 - 2 \\
&\quad \geq q_2 + q_3 + q_4 - 2|\mathcal{I}_{\text{inner}}| - q_5 - 2 \\
&\quad \geq q_2 + q_3 + q_4 - (2\sqrt{q} + q_5 + 2) \geq 0,
\end{aligned} \tag{78}$$

since $q_2 + q_3 + q_4 \geq 2\sqrt{q} + q_5 + 2$. This allows us to carry out the intended transfer in Eq. (77) and get

$$\begin{aligned}
a_{d_i} b_{h_i} &\geq \left[N_5 - (m^{d_i} - 1) - (t^{d_i} - t_{**}^{h_i})\right] \cdot [N_{234} - 3(h_i - 1)] \\
&\geq \left[N_5 - (m^{d_i} - 1) - |\mathcal{I}_{\text{inner}}|\right] \cdot [N_{234} - 3(h_i - 1)] \\
&\geq \left[N_5 - (m^{d_i} - 1) - \sqrt{q}\right] \cdot [N_{234} - 3(h_i - 1)]\,.
\end{aligned} \tag{79}$$

Similarly, when i is a non-root decryption query, we use the inequality $q_2 + q_3 + q_4 \geq 2\sqrt{q} + q_1 + 2$ to get

$$a_{d_i} b_{h_i} \geq \left[N_1 - (\ell^{d_i} - 1) - \sqrt{q}\right] \cdot [N_{234} - 3(h_i - 1)]\,. \tag{80}$$

Here on, we can proceed to bound the two branches separately. For the parentheses on the right of Eq. (80), taking product over $\mathcal{I}_{**}$ gives

$$\prod_{i \in \mathcal{I}_{**}} [N_{234} - 3(h_i - 1)] = \prod_{h \in [q_{**}]} [N_{234} - 3(h - 1)]\,. \tag{81}$$

We observe that

$$\begin{aligned}
&N^2(N - q_2 - q_3 - q_4 - 3(h - 1)) \\
&\quad = (N - q_2 - (h - 1))(N - q_3 - (h - 1))(N - q_4 - (h - 1)) \\
&\qquad - N\,[(q_2 + (h - 1))(q_3 + (h - 1)) + (q_2 + (h - 1))(q_4 + (h - 1)) \\
&\qquad + (q_3 + (h - 1))(q_4 + (h - 1))] + (q_2 + (h - 1))(q_3 + (h - 1))(q_4 + (h - 1)) \\
&\quad \geq (N - q_2 - (h - 1))(N - q_3 - (h - 1))(N - q_4 - (h - 1)) \\
&\qquad \cdot \left[1 - \frac{2}{N^2} \cdot \{(q_2 + (h - 1))(q_3 + (h - 1)) \right. \\
&\qquad \left. + (q_2 + (h - 1))(q_4 + (h - 1)) + (q_3 + (h - 1))(q_4 + (h - 1))\}\right].
\end{aligned} \tag{82}$$

Taking product over h gives

$$N^{2q_{**}} \cdot \prod_{h=1}^{q_{**}} (N_{234} - 3(h-1)) \geq (N_2)_{q_{**}} \cdot (N_3)_{q_{**}} \cdot (N_4)_{q_{**}} \cdot (1-\epsilon_0), \tag{83}$$

where $\epsilon_0 = 2q[(q_2+q_{**})(q_3+q_{**}) + (q_2+q_{**})(q_4+q_{**}) + (q_3+q_{**})(q_4+q_{**})]/N^2$.

This completes the bounding of the branch on the right of Eq. (80). The final task that remains is to bound the branch on the left, combined with the a_d terms in $\mathcal{I}_{\text{inner}}$ (where the t_d did not get cancelled out). For each $i \in \mathcal{I}_*$, let w^i denote $\sqrt{q}$ if $i \in \mathcal{I}_{**}$ (corresponding to the $\sqrt{q}$ in the left parentheses of Eq. (80)) and q if $i \in \mathcal{I}_{\text{inner}}$ (corresponding to the $t(\ell)$ or $t(m)$ in Eq. (74)). Let $w(\ell)$ (resp. $w(m)$) be defined as w^i where d_i is the first query where R_ℓ (resp. S_m) appears. Then

$$\begin{aligned}
&\prod_{\ell=1}^{q_{R*}} [N_1 - (\ell-1) - w(\ell)] \cdot \prod_{m=1}^{q_{S*}} [N_5 - (m-1) - w(m)] \\
&\geq (N_1)_{q_{R*}} (N_5)_{q_{S*}} \left[1 - \frac{2}{N} \cdot \left(\sum_{\ell=1}^{q_{R*}} w(\ell) + \sum_{m=1}^{q_{S*}} w(m) \right)\right] \\
&\geq (N_1)_{q_{R*}} (N_5)_{q_{S*}} \left[1 - \frac{4}{N} \cdot \left(\sqrt{q} \cdot |\mathcal{I}_{**}| + q \cdot |\mathcal{I}_{\text{inner}}| \right)\right] \\
&\geq (N_1)_{q_{R*}} (N_5)_{q_{S*}} \left(1 - \frac{8q^{3/2}}{N}\right).
\end{aligned} \tag{84}$$

From Eqs. (79), (80), (83) and (84) we have

$$\prod_{d=1}^{q_*} a_d \prod_{h=1}^{q_{**}} b_h \geq \frac{(N_2)_{q_{**}} (N_3)_{q_{**}} (N_4)_{q_{**}}}{N^{2q_{**}}} \cdot (N_1)_{q_{R*}} (N_5)_{q_{S*}} \left(1 - \epsilon_0 - \frac{8q^{3/2}}{N}\right). \tag{85}$$

Plugging in the value of ϵ_0 in Eq. (85), using the inequality $q_{**} \leq q$ and substituting Eq. (85) in Eq. (66) gives

$$\mathsf{H}[\eta] \geq 1 - \left(\frac{6q^3 + 4q^2(q_2+q_3+q_4) + 2qq_2q_3 + 2qq_2q_4 + 2qq_3q_4}{N^2} + \frac{8q^{3/2}}{N} \right), \tag{86}$$

which completes the proof.

Impact on the Security After Removing Output Masking Keys. At this point, it is natural to wonder about the impact on the security bound if we remove masking the round keys at the output of every round of the construction, i.e., each round function is $P(x+k)$ instead of $P(x+k)+K$. First of all, it is interesting to investigate the security of this modified construction. However, it seems that we may not get same level of security from this modified construction as we obtained it from the analysis of our proposed construction. This is partly because in the modified construction, the output of each round permutation is "open", in the sense that the output of those permutation can be directly controlled by the adversary through inverse permutation queries. Nonetheless, if the security goes through, we believe that the argument would be far complex and may require some combinatorial results like

Sum-Capture Lemma [11] to prove the security of the construction without the output round keys.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10623-023-01288-4.

Funding Open access funding provided by EPFL Lausanne

Data availability The authors of the manuscript declare that this manuscript does not have any associated data.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose. The authors have no conflicts of interest to declare that are relevant to the content of this article. All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Barbosa M., Farshim P.: The related-key analysis of Feistel constructions. In: Cid C., Rechberger C. (ed.) FSE 2014. Revised Selected Papers. LNCS, vol. 8540, pp. 265–284. Springer, Berlin (2014).
2. Bernstein D.J., Kölbl S., Lucks S., Massolino P.M.C., Mendel F., Nawaz K., Schneider T., Schwabe P., Standaert F.-X., Todo Y., Viguier B.: Gimli: a cross-platform permutation. In: CHES 2017, Proceedings, pp. 299–320 (2017).
3. Bertoni G., Daemen J., Peeters M., Van Assche G.: Duplexing the sponge: single-pass authenticated encryption and other applications. In: SAC 2011, Revised Selected Papers, pp. 320–337 (2011).
4. Bertoni G., Daemen J., Peeters M., Van Assche G.: Keccak. In: EUROCRYPT 2013. Proceedings, pp. 313–314 (2013).
5. Bhattacharjee A., López C.M., List E., Nandi M.: The Oribatida v1.3 family of lightweight authenticated encryption schemes. J. Math. Cryptol. **15**(1), 305–344 (2021).
6. Biham E., Shamir A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes A., Vanstone S.A. (eds.) CRYPTO '90, Proceedings. LNCS, vol. 537, pp. 2–21. Springer, Berlin (1990).
7. Bogdanov A., Knezevic M., Leander G., Toz D., Varici K., Verbauwhede I.: SPONGENT: the design space of lightweight cryptographic hashing. IEEE Trans. Comput. **62**(10), 2041–2053 (2013).
8. Chakraborti A., Datta N., Nandi M., Yasuda K.: Beetle family of lightweight and secure authenticated encryption ciphers. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2018**(2), 218–241 (2018).
9. Chakraborty B., Nandi M.: Orange. In: NIST LWC (2019).
10. Chen S., Steinberger J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen P.Q., Oswald E. (eds.) EUROCRYPT 2014. Proceedings. LNCS. vol. 8441, pp. 327–350. Springer, Berlin (2014).
11. Chen S., Lampe R., Lee J., Seurin Y., Steinberger J.P.: Minimizing the two-round even-Mansour cipher. In: Garay J.A., Gennaro R. (eds.) CRYPTO 2014, Proceedings, Part I. LNCS, vol. 8616, pp. 39–56. Springer, Berlin (2014).
12. Cogliati B., Seurin Y.: Beyond-birthday-bound security for tweakable even-Mansour ciphers with linear tweak and key mixing. In: Iwata T., Cheon J.H. (eds.) ASIACRYPT 2015, Proceedings, Part II. LNCS. vol. 9453, pp. 134–158. Springer, Berlin (2015).
13. Cogliati B., Lampe R., Seurin Y.: Tweaking even-Mansour ciphers. In: Gennaro R., Robshaw M. (eds.) CRYPTO 2015, Proceedings, Part I, LNCS. vol. 9215, pp. 189–208. Springer, Berlin (2015).

14. Daemen J., Hoffert S., Peeters M., Van Assche G., Van Keer R.: Xoodyak, a lightweight cryptographic scheme. IACR Trans. Symmetric Cryptol. **2020**(S1), 60–87 (2020).
15. Dobraunig C., Eichlseder M., Mendel F., Schläffer M.: Ascon v1.2. In: NIST LWC (2019).
16. Dobraunig C., Eichlseder M., Mangard S., Mendel F., Mennink B., Primas R., Unterluggauer T.: ISAP v2.0. IACR Trans. Symmetric Cryptol. **2020**(S1), 390–416 (2020).
17. Dutta A.: Minimizing the two-round tweakable even-Mansour cipher. In: Moriai S., Wang H. (eds.) ASIACRYPT 2020, Proceedings, Part I. LNCS. vol. 12491, pp. 601–629. Springer, Berlin (2020).
18. Even S., Mansour Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997).
19. Gentry C., Ramzan Z.: Eliminating random permutation oracles in the even-Mansour cipher. In: Lee P.J. (ed.) ASIACRYPT 2004, Proceedings. LNCS. vol. 3329, pp. 32–47. Springer, Berlin (2004).
20. Guo C., Wang L.: Revisiting key-alternating Feistel ciphers for shorter keys and multi-user security. In: Peyrin T., Galbraith S.D. (eds.) ASIACRYPT 2018, Proceedings, Part I. LNCS. vol. 11272, pp. 213–243. Springer, Berlin (2018).
21. Guo J., Peyrin T., Poschmann A.: The PHOTON family of lightweight hash functions. In: CRYPTO 2011. Proceedings, pp. 222–239 (2011).
22. Guo J., Jean J., Nikolic I., Sasaki Y.: Meet-in-the-middle attacks on generic Feistel constructions. In: Sarkar P., Iwata T. (eds.) ASIACRYPT 2014. Proceedings, Part I. LNCS. vol. 8873, pp. 458–477. Springer, Berlin (2014).
23. Hoang V.T., Rogaway P.: On generalized Feistel networks. In: Rabin T. (ed.) CRYPTO 2010. Proceedings. LNCS. vol. 6223, pp. 613–630. Springer, Berlin (2010).
24. Jean J.: TikZ for cryptographers (2016). https://www.iacr.org/authors/tikz/.
25. Krawczyk H., Bellare M., Canetti R.: HMAC: keyed-hashing for message authentication. RFC **2104**, 1–11 (1997).
26. Lampe R., Seurin Y.: Security analysis of key-alternating Feistel ciphers. In: Cid C., Rechberger C. (eds.) FSE 2014. Revised Selected Papers. LNCS, vol. 8540, pp. 243–264. Springer, Berlin (2014).
27. Luby M., Rackoff C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988).
28. Matsui M.: Linear cryptanalysis method for DES cipher. In: Helleseth T. (ed.) EUROCRYPT '93, Proceedings. LNCS, vol. 765, pp. 386–397. Springer, Berlin (1993).
29. Maurer U.M., Pietrzak K.: The security of many-round Luby-Rackoff pseudo-random permutations. In: Biham E. (ed.) EUROCRYPT 2003, Proceedings. LNCS, vol. 2656, pp. 544–561. Springer, Berlin (2003).
30. Nachef V., Patarin J., Volte E.: Feistel Ciphers—Security Proofs and Cryptanalysis. Springer, Berlin (2017).
31. Nandi M.: The characterization of Luby-Rackoff and its optimum single-key variants. In: Gong G., Gupta K.C. (eds.) INDOCRYPT 2010, Proceedings. LNCS, vol. 6498, pp. 82–97. Springer, Berlin (2010).
32. Nandi M.: On the optimality of non-linear computations of length-preserving encryption schemes. In: Iwata T., Cheon J.H. (eds.) ASIACRYPT 2015, Proceedings, Part II. LNCS, vol. 9453, pp. 113–133. Springer, Berlin (2015).
33. Naor M., Reingold O.: On the construction of pseudorandom permutations: Luby-rackoff revisited. J. Cryptol. **12**(1), 29–66 (1999).
34. Patarin J.: Pseudorandom permutations based on the DES scheme. In: Gérard D.C., Charpin P. (eds.) EUROCODE '90, Proceedings. LNCS. vol. 514, pp. 193–204. Springer, Berlin (1990).
35. Patarin J.: How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. In: Rueppel R.A. (ed.) EUROCRYPT '92, Proceedings. LNCS, vol. 658, pp. 256–266. Springer, Berlin (1992).
36. Patarin, J.: About Feistel schemes with six (or more) rounds. In: Vaudenay S. (ed.) FSE '98, Proceedings. LNCS, vol. 1372, pp. 103–121. Springer, Berlin (1998).
37. Patarin J.: Security of random Feistel schemes with 5 or more rounds. In: Franklin M.K. (ed.) CRYPTO 2004, Proceedings. LNCS, vol. 3152, pp. 106–122. Springer, Berlin (2004).
38. Patarin J.: Security of balanced and unbalanced Feistel schemes with linear non equalities. In: IACR Cryptology, p. 293 (2010).
39. Patel S., Ramzan Z., Sundaram G.S.: Towards making Luby-Rackoff ciphers optimal and practical. In: Knudsen L.R. (ed.) FSE '99, Proceedings. LNCS, vol. 1636, pp. 171–185. Springer, Berlin (1999).
40. Ramzan Z., Reyzin L.: On the round security of symmetric-key cryptographic primitives. In: Bellare M. (ed.) CRYPTO 2000, Proceedings. LNCS, vol. 1880, pp. 376–393. Springer, Berlin (2000).
41. Rogaway P., Bellare M., Black J.: Sha-3 standard. TISSEC **6**(3), 365–403 (2003).
42. Sadeghiyan B., Pieprzyk J.: A construction for super pseudorandom permutations from a single pseudorandom function. In: Rueppel R.A. (ed.) EUROCRYPT '92, Proceedings. LNCS, vol. 658, pp. 267–284. Springer, Berlin (1992).

43. Shen Y., Yan H., Wang L., Lai X.: Secure key-alternating Feistel ciphers without key schedule. Sci. China Inf. Sci. **64**, 1–3 (2021).
44. Suzaki T., Minematsu K., Morioka S., Kobayashi E.: Twine: a lightweight block cipher for multiple platforms. In: Knudsen L.R., Wu H. (eds.) SAC 2012, Revised Selected Papers. LNCS, vol. 7707, pp. 339–354. Springer, Berlin (2012).
45. Tessaro S., Zhang X.: Tight security for key-alternating ciphers with correlated sub-keys. In: Tibouchi M., Wang H. (eds.) ASIACRYPT 2021, Proceedings, Part III. LNCS, vol. 13092, pp. 435–464. Springer, Berlin (2021).
46. Wu W., Zhang L.: Lblock: a lightweight block cipher. In: López J., Tsudik G. (eds.) ACNS 2011. Proceedings. LNCS, vol. 6715, pp. 327–344 (2011).
47. Wu Y., Yu L., Cao Z., Dong X.: Tight security analysis of 3-round key-alternating cipher with a single permutation. In: Moriai S., Wang H. (eds.) ASIACRYPT 2020, Proceedings, Part I. LNCS, vol. 12491, pp. 662–693. Springer, Berlin (2020).