PAPER

Feistel Ciphers Based on a Single Primitive*

Kento TSUJI[†a)], ***Student Member and*** **Tetsu IWATA**[†b)], ***Member***

SUMMARY We consider Feistel ciphers instantiated with tweakable block ciphers (TBCs) and ideal ciphers (ICs). The indistinguishability security of the TBC-based Feistel cipher is known, and the indifferentiability security of the IC-based Feistel cipher is also known, where independently keyed TBCs and independent ICs are assumed. In this paper, we analyze the security of a single-keyed TBC-based Feistel cipher and a single IC-based Feistel cipher. We characterize the security depending on the number of rounds. More precisely, we cover the case of contracting Feistel ciphers that have $d \geq 2$ lines, and the results on Feistel ciphers are obtained as a special case by setting $d = 2$. Our indistinguishability security analysis shows that it is provably secure with $d + 1$ rounds. Our indifferentiability result shows that, regardless of the number of rounds, it cannot be secure. Our attacks are a type of a slide attack, and we consider a structure that uses a round constant, which is a well-known countermeasure against slide attacks. We show an indifferentiability attack for the case $d = 2$ and 3 rounds.

key words: *feistel cipher, tweakable block cipher, ideal cipher, provable security*

1. Introduction

(1) Background.

A Feistel structure is one of the widely used structures of a block cipher, and its security proof was given by Luby and Rackoff [2]. It is shown that the 3-round Feistel structure instantiated with 3 independent pseudorandom functions (PRFs), which we call the Feistel cipher, is a pseudorandom permutation (PRP), a block cipher that is indistinguishable from a random permutation against adversaries in a chosen plaintext attack (CPA) setting. Similarly, the 4-round Feistel cipher is a strong PRP (SPRP), where the adversary is in a chosen ciphertext attack (CCA) setting.

A question of whether one can securely reduce the number of independent PRFs has been studied, as reducing the number of PRFs implies the reduction of the key length, and hence it reduces the cost of maintaining, exchanging, and updating the secret key. Let $\Phi[F_1, F_2, \ldots, F_r]$ be the r-round Feistel cipher, where the PRF F_i is used in the i-th round. The structure that simply replaces all the PRFs with a single-keyed PRF F, i.e., $\Phi[F, F, \ldots, F]$, is easily distinguishable from a random permutation regardless of the number of rounds [3]. Pieprzyk showed that $\Phi[F_1, F_1, F_1, F_2]$ and $\Phi[F_1, F_1, F_1, F_1 \circ F_1]$ are PRPs [4]. Patarin showed that $\Phi[F_1, F_2, F_1, F_2]$ is an SPRP [5]. Additionally, Patarin pointed out that $\Phi[F, F, F, F \circ \zeta \circ F]$ is an SPRP, where it uses 1-bit cyclic rotation ζ. Nandi proved that $\Phi[\zeta \circ F, F, F, F]$ is an SPRP and has the optimal number of PRF calls [6]. See also [7] for a related result that uses a mask.

A tweakable block cipher (TBC), formalized by Liskov et al. [8], is the generalization of a block cipher to take an additional input called a tweak. Minematsu pointed out that TBCs can be used as a primitive for constructing block ciphers, and instantiated a concrete structure by combining TBCs and universal hash functions [9]. By replacing the PRFs and XORs in the Feistel cipher with TBCs, Coron et al. formalized a TBC-based Feistel cipher and proved its indistinguishability security [10].

Indifferentiability, formalized by Maurer et al. [11], is one of the security definitions for cryptographic permutations, a key-less permutation. This definition captures the hardness to distinguish a cryptographic permutation from a random permutations, where the cryptographic permutation makes oracle calls to an ideal primitive. Some instances of random oracle (RO) based Feistel ciphers are analyzed with the indifferentiability notion. See [12]–[14] for the results on this line of research. The TBC-based Feistel cipher [10] can be seen as a cryptographic permutation by regarding the TBC as the ideal cipher (IC), which models an ideally secure block cipher, and its indifferentiability analysis is presented in [10], where independent ICs are used in the construction. Bhaumik et al. later improved the security bound [15].

Contracting Feistel structures are derivations of the Feistel structure, and we consider the TBC-based counterpart [16]. These structures have d lines, where $d \geq 2$, and $d - 1$ lines are used as the tweak of the TBC to update the remaining line. See Fig. 1 for the structure. The security of the structure is known in the indistinguishability notion [16], [17], and in the indifferentiability notion [18], [19], where we consider the IC with key length of $d - 1$ lines instead of a TBC.

(2) Our Contributions.

The indistinguishability results on the TBC-based Feistel ciphers [10] and on the TBC-based contracting Feistel ciphers [16], [17] assume independent TBCs, and the indifferentiability results on the IC-based Feistel ciphers [10], [15] and on the IC-based contracting Feistel ciphers [18], [19] assume independent ICs. In this paper, we investigate the security of the single primitive-based counter parts, which

Manuscript received January 16, 2024.
Manuscript publicized March 29, 2024.

[†] Dept. of Information and Communication Engineering, Nagoya University, Nagoya-shi, 464-8603 Japan.

[*] A preliminary version of this paper was presented at IMACC 2023 [1]. Sect. 6 was improved to cover general cases.

a) E-mail: tsuji.kento.y1@s.mail.nagoya-u.ac.jp
b) E-mail: tetsu.iwata@nagoya-u.jp

DOI: 10.1587/transfun.2024EAP1006

Table 1 Summary of previous results and our results ($d = 2$) on Feistel ciphers.

(a) Results based on indistinguishability. “Model” shows the model of the adversary. “Key” indicates the relation between the keys for each round. In the results of [4]–[6], the number of PRF calls is additionally noted, and ϕ means that an additional function (e.g., a 1-bit rotation) is required for the structure.

Primitive	Key	Model	# of rounds	Security	Reference
PRF	independent	PRP	3	$O(q^2/2^n)$	[2]
		SPRP	4	$O(q^2/2^n)$	
	single	PRP	any	$O(1)$ attack	[3]
			4 (5 calls)	$O(q^2/2^n)$	[4]
		SPRP	4 (5 calls + ϕ)	$O(q^2/2^n)$	[5]
			4 (4 calls + ϕ)	$O(q^2/2^n)$	[6]
TBC	independent	SPRP	2	$O(q^2/2^n)$	[10]
			3	$O(q^2/2^{2n})$	
	single	SPRP	2	$O(1)$ attack	Theorem 1
			3	$O(q^2/2^n)$	Theorem 2
			≥ 3	$O(2^{n/2})$ attack	Theorem 3

(b) Results based on indifferentiability. “Instance” indicates the relation between the ROs/ICs for each round.

Primitive	Instance	# of rounds	Security	Reference
RO	independent	5	$O(1)$ attack	[12]
		8	$O(q^8/2^n)$	[14]
		10	$O(q^{12}/2^n)$	[13]
		14	$O(q^{16}/2^{2n})$	[12]
IC	independent	2	$O(1)$ attack	[10]
		3	$O(q^2/2^n)$	
			$O(n^2q/2^n)$	[15]
	single	any	$O(1)$ attack	Theorem 4
IC + constants	single	3	$O(1)$ attack	Theorem 5

replace the TBCs or the ICs with a single primitive, i.e., a single-keyed TBC or a single IC. Our target is the n-bit block and $(d-1)n$-bit tweak single-keyed TBC-based Feistel cipher for indistinguishability, and the n-bit block, $(d-1)n$-bit key single IC-based Feistel cipher for indifferentiability. We remark that by setting $d = 2$, our results cover the case of regular Feistel ciphers of 2 lines. We present the following results:

(3) Indistinguishability Results.

Let Φ_r be the r-round single-keyed TBC-based Feistel cipher with d lines. We show that for any $r \leq d$, Φ_r can be distinguished from a random permutation with $O(1)$ queries. We then show that Φ_{d+1} is secure in the indistinguishability notion, where the security bound is $O(q^2/2^n)$ for adversaries making q queries. This makes a sharp difference to the PRF-based Feistel cipher, which is insecure regardless of the number of rounds. Next, for any $r \geq d+1$, we show that Φ_r can be distinguished from a random permutation with $O(2^{n/2})$ queries, with a type of slide attack [20]. On one hand, this shows the tightness of the security bound of the case $r = d+1$, i.e., it is impossible to show a better security bound for this case. This also shows that, even if we increase the number of rounds beyond $d+1$ rounds, the security of Φ_r does not improve, showing an impossibility of improving the security by increasing the number of rounds.

These results show that the $(d+1)$-round structure can be practically used in applications that are sufficient with $O(2^{n/2})$ security, however, it cannot be used if higher security is needed, regardless of the number of rounds.

(4) Indifferentiability Results.

Let $\widehat{\Phi}_r$ be the r-round single IC-based Feistel cipher with d lines. We show that for any r, $\widehat{\Phi}_r$ is not secure in the indifferentiability notion. The attack is the straightforward application of the attacks against Φ_r, and they work with $O(1)$ queries. The attack can be seen as a type of slide attack [20]. Using a round constant is a well-known countermeasure, and one may hope that a round constant can prevent the attack. We consider a variant of $\widehat{\Phi}_r$ that uses a round constant, and demonstrate that the round constant cannot prevent the indifferentiability attack for the case $r = 2d-1$.

These results show that single IC based structures should not be used in practice.

Table 1 and Table 2 summarize the previous results and our results. Table 1 shows the results for $d = 2$ and Table 2 shows the results for $d \geq 2$.

Table 2 Summary of previous results and our results on contracting Feistel ciphers. d denotes the number of lines, l is a constant value s.t. $1 \leq l \leq d-1$. In "Security", the maximum number of queries is additionally noted if exists.

(a) Results based on indistinguishability.

Primitive	Key	Model	# of rounds	Security	Reference
TBC	independent	SPRP	$3d$	$O(q^2/2^{dn})$	[16]
			$3d-2$	$O(q^2/2^{dn})$	[17]
			$d+l$	$O(q^2/2^{(1+l)n})$ $(q \leq 2^n)$	
			d	$O(q^2/2^n)$	
	single	SPRP	$\leq d$	$O(1)$ attack	Theorem 1
			$d+1$	$O(q^2/2^n)$	Theorem 2
			$\geq d+1$	$O(2^{n/2})$ attack	Theorem 3

(b) Results based on indifferentiability. In [18], $d > 2$.

Primitive	Instance	# of rounds	Security	Reference
IC	independent	$\leq 2d-2$	$O(1)$ attack	[18] $(d > 2)$
		$2d-1$	$O(q^2/2^n)$	
		$2d+1$	$O(q^2/2^{2n})$	[19]
		$2d+2l-1$	$O(q^2/2^{(1+l)n})$ $(q \leq 2^n)$	
	single	any	$O(1)$ attack	Theorem 4
IC + constants	single	$2d-1$	$O(1)$ attack	Theorem 5

(5) Further Related Works.

A problem of whether one can securely reduce the number of independent keys/primitives has been studied in various other constructions. See, e.g., [21]–[26]. With respect to slide attacks, key-reduced Feistel ciphers have been actively analyzed. See, e.g., [27]–[31]. Compared to these results, our attacks follow a fundamentally similar approach, while our targets employ stronger primitives, TBCs/ICs, instead of PRFs/ROs.

2. Preliminaries

2.1 Notation

For a positive integer n, let $\{0,1\}^n$ be the set of all n-bit strings. For two strings X and Y, let $X \parallel Y$ denote their concatenation. For d string $X^1, X^2, \ldots, X^d$, we denote their concatenation $X^1 \parallel X^2 \parallel \cdots \parallel X^d$ by $X^{[1..d]}$. For a finite set S, $s \xleftarrow{\$} S$ is the operation of uniformly sampling an element from S and assigning it to s.

2.2 (Tweakable) Block Cipher

A block cipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is a keyed permutation. For key $K \in \mathcal{K}$, plaintext $M \in \mathcal{M}$, and ciphertext $C \in \mathcal{M}$, we write the encryption as $C = E_K(M)$ and the decryption as $M = E_K^{-1}(C)$. If $\mathcal{M} = \{0,1\}^n$, we say that it is an n-bit block cipher. Let $\mathrm{Perm}(n)$ be the set of all n-bit permutations, and a random permutation is an element selected from $\mathrm{Perm}(n)$ uniformly at random.

A tweakable block cipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ is a keyed permutation that takes an additional input called a tweak [8]. For key $K \in \mathcal{K}$, tweak $T \in \mathcal{T}$, plaintext $M \in \mathcal{M}$, and ciphertext $C \in \mathcal{M}$, we write the encryption as $C = \widetilde{E}_K(T, M)$ and the decryption as $M = \widetilde{E}_K^{-1}(T, C)$. If $\mathcal{T} = \{0,1\}^t$ and $\mathcal{M} = \{0,1\}^n$, we say that it is an (t,n)-bit TBC. Let $\widetilde{\mathrm{Perm}}(t,n)$ be the set of all the functions $\widetilde{P} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ s.t. for any $T \in \{0,1\}^t$, $\widetilde{P}(T,\cdot) \in \mathrm{Perm}(n)$, and a tweakable random permutation (TRP) is an element selected from $\widetilde{\mathrm{Perm}}(t,n)$ uniformly at random, which we call an (t,n)-bit TRP.

The ideal cipher $\widehat{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is the set of random permutations that idealizes a block cipher. For each K, $\widehat{E}(K,\cdot)$ is a random permutation over $\mathcal{M}$. For key $K \in \mathcal{K}$, plaintext $M \in \mathcal{M}$, and ciphertext $C \in \mathcal{M}$, we write the encryption as $C = \widehat{E}(K, M)$ and the decryption as $M = \widehat{E}^{-1}(K, C)$. If $\mathcal{K} = \{0,1\}^k$ and $\mathcal{M} = \{0,1\}^n$, we say that it is an (k,n)-bit IC.

2.3 Security Definitions

We consider the security of block cipher E as a keyed primitive and as a cryptographic permutation. As a keyed primitive, we consider the indistinguishability notion [2], i.e., the notion of a pseudorandom permutation (PRP) and a strong pseudorandom permutation (SPRP). A PRP-adversary has oracle access to a cryptographic permutation oracle E_K in the real world, and random permutation π in the ideal world. For an adversary $\mathcal{A}$ that makes a maximum of q oracle queries, we define the PRP-advantage and SPRP-advantage as follows:

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) = |\Pr[\mathcal{A}^{E_K(\cdot)} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi(\cdot)} \Rightarrow 1]|$$

$$\mathbf{Adv}^{\mathrm{sprp}}_{E}(\mathcal{A}) = |\Pr[\mathcal{A}^{E_K(\cdot),E_K^{-1}(\cdot)} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi(\cdot),\pi^{-1}(\cdot)} \Rightarrow 1]|$$

Next, as a cryptographic permutation, we consider the indifferentiability notion [11]. Let C be a cryptographic permutation that is built on the ideal cipher $\widehat{E}$, i.e., C makes oracle calls to $\widehat{E}$ to compute its output, and we write $C^{\widehat{E}}$ for this. In the real world, an adversary $\mathcal{A}$ has oracle access to $\widehat{E}$ and $C^{\widehat{E}}$. In the ideal world, $\mathcal{A}$ makes queries to a random permutation π and a simulator Sim^{π}, where the simulator Sim has oracle access to π. We call a query to $C^{\widehat{E}}$ or π as a construction query, and a query to E or Sim^{π} as a primitive query. For an adversary $\mathcal{A}$ that makes a maximum of q oracle queries in total, we define the advantage as follows:

$$\mathbf{Adv}^{\mathrm{indiff}}_{C,\mathrm{Sim}}(\mathcal{A}) = |\Pr[\mathcal{A}^{C^{\widehat{E}}(\cdot),\widehat{E}(\cdot)} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi(\cdot),\mathrm{Sim}^{\pi}(\cdot)} \Rightarrow 1]|$$

2.4 Coefficient-H Technique [32], [33]

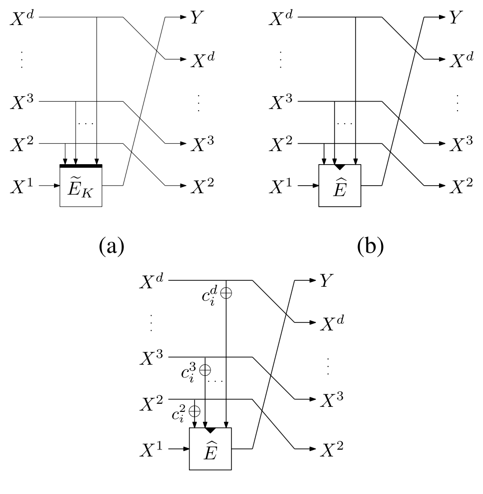
Our security proof is based on the coefficient-H technique. Let $\mathcal{R}$ and $\mathcal{R}^{-1}$ be the real world oracles that internally call a block cipher E_K and its inverse E_K^{-1}. Similarly, let $\mathcal{I}$ and $\mathcal{I}^{-1}$ be the ideal world oracles that internally call a random permutation π and its inverse π^{-1}. For an adversary $\mathcal{A}$ that makes a maximum of q oracle queries, a transcript θ denotes a tuple that records all the interactions between $\mathcal{A}$ and the oracles. Let $\Theta_{\mathcal{R}}$ be the random variable of θ when $\mathcal{A}$ interacts with $\mathcal{R}$ and $\mathcal{R}^{-1}$, and $\Theta_{\mathcal{I}}$ be the random variable of θ when $\mathcal{A}$ interacts with $\mathcal{I}$ and $\mathcal{I}^{-1}$. An attainable transcript is a transcript θ such that $\Pr[\Theta_{\mathcal{I}} = \theta] > 0$. Then, the coefficient-H technique states the following result:

Lemma 1: Consider a deterministic adversary $\mathcal{A}$. Partition all the attainable transcripts into two disjoint sets $\mathcal{T}_{\mathrm{good}}$ and $\mathcal{T}_{\mathrm{bad}}$. Suppose that there exists ϵ_1 such that $\Pr[\Theta_{\mathcal{I}} \in \mathcal{T}_{\mathrm{bad}}] \le \epsilon_1$, and there exists ϵ_2 such that, for all $\theta \in \mathcal{T}_{\mathrm{good}}$, $\Pr[\Theta_{\mathcal{R}} = \theta]/\Pr[\Theta_{\mathcal{I}} = \theta] \ge 1-\epsilon_2$. Then we have $\mathbf{Adv}^{\mathrm{sprp}}_{E}(\mathcal{A}) \le \epsilon_1+\epsilon_2$.

We remark that although Lemma 1 is modified specifically for an SPRP adversary, the coefficient-H technique can be applied to general security definitions. See e.g., [32], [33].

3. Constructions

3.1 Block Ciphers



(a) (b)

(c)

Fig. 1 (a) $\phi[\widetilde{E}_K](X^{[1..d]}) = X^{[2..d]} \parallel Y$, where $Y = \widetilde{E}_K(X^{[2..d]}, X^1)$, (b) $\phi[\widehat{E}](X^{[1..d]}) = X^{[2..d]} \parallel Y$, where $Y = \widehat{E}(X^{[2..d]}, X^1)$, and (c) $\phi_i[\widehat{E}](X^{[1..d]}) = X^{[2..d]} \parallel Y$, where $Y = \widehat{E}(X^{[2..d]} \oplus c_i^{[2..d]}, X^1)$.

Fix $d \ge 2$. Let $\widetilde{E}$ be a $((d-1)n, n)$-bit TBC and K be a key of $\widetilde{E}$. First, we define an encryption round function ϕ as

$$\phi[\widetilde{E}_K](X^{[1..d]}) = X^{[2..d]} \parallel \widetilde{E}_K(X^{[2..d]}, X^1),$$

where $X^{[1..d]} \in \{0,1\}^{dn}$ is the input. See Fig. 1(a). Then, the r-round single-keyed TBC-based Feistel cipher Φ_r is defined by iterating the round function ϕ for r times as follows:

$$\Phi_r[\widetilde{E}_K](M^{[1..d]}) = \underbrace{\phi[\widetilde{E}_K] \circ \phi[\widetilde{E}_K] \circ \cdots \circ \phi[\widetilde{E}_K]}_{r \text{ times}}(M^{[1..d]})$$

It takes $M^{[1..d]} \in \{0,1\}^{dn}$ as input.

Likewise, we define a decryption round function ϕ^{-1} as

$$\phi^{-1}[\widetilde{E}_K](X^{[1..d]}) = \widetilde{E}_K^{-1}(X^{[1..d-1]}, X^d) \parallel X^{[1..d-1]},$$

where $X^{[1..d]} \in \{0,1\}^{dn}$ is the input. Next, the decryption of Φ_r, which we write Φ_r^{-1}, is defined by repeating ϕ^{-1} for r times as follows:

$$\Phi_r^{-1}[\widetilde{E}_K](C^{[1..d]}) = \underbrace{\phi^{-1}[\widetilde{E}_K] \circ \phi^{-1}[\widetilde{E}_K] \circ \cdots \circ \phi^{-1}[\widetilde{E}_K]}_{r \text{ times}}(C^{[1..d]})$$

It takes $C^{[1..d]} \in \{0,1\}^{dn}$ as input.

3.2 Cryptographic Permutations

Let $\widehat{E}$ be a $((d-1)n, n)$-bit IC. Cryptographic permutations can be defined from an ideal cipher similarly to block ciphers.

With round functions $\phi[\widehat{E}]$ and $\phi^{-1}[\widehat{E}]$ shown in Fig. 1(b), where the key of $\widehat{E}$ is regarded as a tweak of $\widetilde{E}_K$ in $\phi[\widetilde{E}_K]$, the r-round single IC-based Feistel cipher, which we write $\widehat{\Phi}_r$, is defined as follows:

$$\widehat{\Phi}_r[\widehat{E}](M^{[1..d]}) = \underbrace{\phi[\widehat{E}] \circ \phi[\widehat{E}] \circ \cdots \circ \phi[\widehat{E}]}_{r \text{ times}}(M^{[1..d]})$$

$$\widehat{\Phi}_r^{-1}[\widehat{E}](C^{[1..d]})$$

$$= \underbrace{\phi^{-1}[\widehat{E}] \circ \phi^{-1}[\widehat{E}] \circ \cdots \circ \phi^{-1}[\widehat{E}]}_{r \text{ times}}(C^{[1..d]})$$

Cryptographic permutations with round constants are defined by introducing round constants to the key of ϕ. We define an encryption round function ϕ_i and a decryption round function ϕ_i^{-1} as follows:

$$\begin{aligned}&\phi_i[\widehat{E}](X^{[1..d]}) = X^{[2..d]} \parallel \widehat{E}(X^{[2..d]} \oplus c_i^{[2..d]}, X^1)\\ &\phi_i^{-1}[\widehat{E}](X^{[1..d]})\\ &= \widehat{E}^{-1}(X^{[1..d-1]} \oplus c_i^{[2..d]}, X^d) \parallel X^{[1..d-1]},\end{aligned}$$

where $c_i^2, \ldots, c_i^d$ is an n-bit constant. See Fig. 1(c). Then the r-round single IC-based Feistel cipher with round constants $\widehat{\Phi}'_r$ is defined as follows:

$$\begin{aligned}&\widehat{\Phi}'_r[\widehat{E}](M^{[1..d]})\\ &= \phi_r[\widehat{E}] \circ \phi_{r-1}[\widehat{E}] \circ \cdots \circ \phi_1[\widehat{E}](M^{[1..d]})\\ &\widehat{\Phi}'^{-1}_r[\widehat{E}](C^{[1..d]})\\ &= \phi_1^{-1}[\widehat{E}] \circ \phi_2^{-1}[\widehat{E}] \circ \cdots \circ \phi_r^{-1}[\widehat{E}](C^{[1..d]})\end{aligned}$$

4. Security of Φ_r

We present three results on Φ_r. In Theorem 1, we first show an efficient distinguisher on Φ_r with $r \le d$. Next, with an additional round, in Theorem 2, we prove that Φ_r with $r = d$ is provably secure up to $O(2^{n/2})$ queries. Finally, in Theorem 3, we present a distinguisher that makes $O(2^{n/2})$ queries against Φ_r for any $r \ge d+1$. This shows the tightness of Theorem 2, and this also shows that increasing the number of rounds beyond $r = d + 1$ does not increase the security.

We remark that we use a TRP $\widetilde{E}$ as the underlying TBC, and we thus omit writing the key K, while $\widetilde{E}$ and $\Phi_r = \Phi_r[\widetilde{E}]$ are still keyed primitives.

4.1 Attack on Φ_r for $r \le d$

We have the following theorem for Φ_r for $r \le d$.

Theorem 1: Fix $d \ge 2$. Let $\widetilde{E}$ be the $((d-1)n, n)$-bit TRP, and $\Phi_r = \Phi_r[\widetilde{E}]$ be the r-round single-keyed TBC-based Feistel cipher. Then there exists an adversary $\mathcal{A}$ against Φ_r with $r \le d$ such that $\mathbf{Adv}^{\mathrm{prp}}_{\Phi_r}(\mathcal{A}) = O(1)$, where $\mathcal{A}$ makes $O(1)$ queries.

Proof : Let O be the oracle, which is either the block cipher Φ_r or the random permutation π.

(1) The Attack on Φ_r for $r \le d-1$.

We first introduce $\mathcal{A}$ on Φ_r for $r \le d-1$.

$\mathcal{A}$ makes an encryption query using an arbitrary message $M^{[1..d]} \in \{0,1\}^{dn}$ to obtain the corresponding ciphertext $C^{[1..d]} \in \{0,1\}^{dn}$, and returns 1 iff $C^{d-r} = M^d$. In Φ_r, M^d never goes through $\widetilde{E}$, and it directly appears as C^{d-r}. In π, C^{d-r} is a part of a uniformly random output of π, thus $\mathcal{A}$ outputs 0 except for a negligible probability of an n-bit collision. Therefore $\mathcal{A}$ can distinguish Φ_r from π with 1 query.

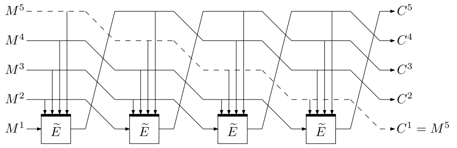


Fig. 2 Structure of Φ_4 for $d = 5$. M^5 directly appears as C^1.

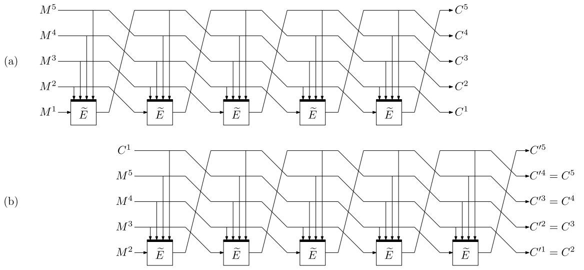


Fig. 3 Structure of Φ_5 for $d = 5$. (a) step 1, (b) step 2.

An example of Φ_4 with $d = 5$ is shown in Fig. 2.

(2) The Attack on Φ_d.

We introduce our adversary $\mathcal{A}$ on Φ_d.

$\mathcal{A}$ first makes an encryption query M to obtain C, and then makes an encryption query M' to obtain C', where $M' = M^{[1..d-1]} \parallel C'^1$. Then $\mathcal{A}$ outputs 1 iff $C^{[2..d]} = C'^{[1..d-1]}$. In Φ_d, the first round of the second query reproduces the second round of the first query. This state collision continues in the subsequent rounds, and eventually, $C^{[2..d]} = C'^{[1..d-1]}$ always holds. In π, $C^{[2..d]}$ and $C'^{[1..d-1]}$ are the outputs of random permutation π, and hence $\mathcal{A}$ outputs 0 except for a negligible probability of a $(d-1)n$-bit collision. Therefore, $\mathcal{A}$ can distinguish Φ_d from π with $O(1)$ queries.

An example of Φ_5 with $d = 5$ is shown in Fig. 3. □

4.2 Security of Φ_{d+1}

We have the following theorem for Φ_{d+1}.

Theorem 2: Fix $d \ge 2$. Let $\widetilde{E}$ be the $(n, (d-1)n)$-bit TRP, and $\Phi_{d+1} = \Phi_{d+1}[\widetilde{E}]$ be the r-round single-keyed TBC-based Feistel cipher, where $r = d + 1$. Then for any adversary $\mathcal{A}$ that makes at most q queries, we have

$$\mathbf{Adv}^{\mathrm{sprp}}_{\Phi_{d+1}}(\mathcal{A}) \le \frac{(4d+1)q^2}{2^n} + \frac{0.5q^2}{2^{dn}}.$$

We present the outline of the proof. The detailed proof is given in Appendix.

Outline of Proof : In $\Phi_{d+1} = \Phi_{d+1}[\widetilde{E}]$, we use a single TRP $\widetilde{E}$, and we write $\widetilde{E}^i$ to indicate $\widetilde{E}$ in the i-th round. Note that $\widetilde{E}^i = \widetilde{E}$ for all i.

Let $S = \widetilde{E}^1(M^{[2..d]}, M^1)$, an output of the TRP in the 1st round. We regard S as the internal state, and we see that,

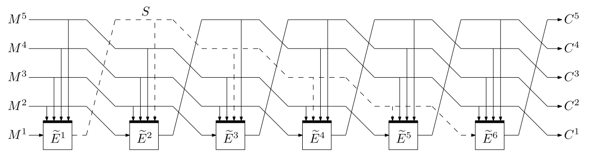


Fig. 4 Structure of Φ_6 for $d = 5$. S appears in all the tweaks from $\widetilde{E}^2$ to $\widetilde{E}^5$, and is used as an output in $\widetilde{E}^1$ and an input in $\widetilde{E}^6$.

for each of the TRP calls, S appears as the output block of the TRP (as $\widetilde{E}^1$), or as a tweak (as $\widetilde{E}^2, \ldots, \widetilde{E}^d$), or as the input block (as $\widetilde{E}^{d+1}$). See Fig. 4 for an example of Φ_6 for $d = 5$.

Our proof is based on the coefficient-H technique. Let $M_i^{[1..d]}$, S_i, and $C_i^{[1..d]}$ be the message, internal state, and the ciphertext of the i-th query, respectively. We define the bad conditions as follows:

1. $\{M_1^1, \ldots, M_1^d, \ldots, M_q^1, \ldots, M_q^d\} \cap \{S_1, \ldots, S_q\} \neq \emptyset$
2. $\{C_1^1, \ldots, C_1^d, \ldots, C_q^1, \ldots, C_q^d\} \cap \{S_1, \ldots, S_q\} \neq \emptyset$
3. $|\{S_1, \ldots, S_q\}| < q$

Namely, if any of the S_i collides with other variables, then the transcript is bad.

If S_i is a unique value, then all the tweaks of $\widetilde{E}^2, \ldots, \widetilde{E}^d$ in the i-th query are unique. For example, in $\widetilde{E}^2$ in Fig. 4, S_i appears in the 4th line of the tweak. It never appears on the same line in other TRPs. Because of this, if S_i is unique, the tweak of $\widetilde{E}^2$ never collides with other tweaks. Furthermore, an output of $\widetilde{E}^1$ and an input of $\widetilde{E}^{d+1}$ are clearly unique.

Intuitively, without the bad conditions and with an assumption that the adversary does not make redundant queries, we can show that every TRP has at least one unique element in the output block, tweak, or in the input block. This is sufficient to show that all the TRPs, which is actually a single TRP, can interpolate them with a non-zero probability.

The good probabilities are almost the same in Φ_{d+1} and π, and from the coefficient-H technique, we obtain the upper bound of the distinguishing advantage.

4.3 Attack on Φ_r for $r \geq d + 1$

We have the following theorem for Φ_r for $r \geq d + 1$.

Theorem 3: Fix $d \geq 2$. Let $\widetilde{E}$ be the $((d-1)n, n)$-bit TRP, and $\Phi_r = \Phi_r[\widetilde{E}]$ be the r-round single-keyed TBC-based Feistel cipher. Then there exists an adversary $\mathcal{A}$ against Φ_r with $r \geq d+1$ such that $\mathbf{Adv}_{\Phi_r}^{\mathrm{prp}}(\mathcal{A}) = O(1)$, where $\mathcal{A}$ makes $O(2^{n/2})$ queries.

Proof : We present our adversary $\mathcal{A}$ for $d \geq 3$ and $r \geq d+1$. We later cover the case $d = 2$.

1. Fix $M^{[2..d]} \in \{0,1\}^{(d-1)n}$ arbitrarily.
2. For $i = 1, \ldots, 2^{n/2}$, choose M_i^1 uniformly at random without overlaps, i.e., $M_i^1 \neq M_{i'}^1$ holds for any $1 \leq i < i' \leq 2^{n/2}$. Then make $2^{n/2}$ encryption queries $C_i^{[1..d]} \leftarrow O(M_i^1 \parallel M^{[2..d]})$ for $i = 1, \ldots, 2^{n/2}$.
3. For $j = 1, \ldots, 2^{n/2}$, choose S'_j uniformly at random without overlaps. Then make $2^{n/2}$ encryption queries $C'^{[1..d]}_j \leftarrow O(M^{[2..d]} \parallel S'_j)$ for $j = 1, \ldots, 2^{n/2}$.
4. If there exists (i, j) s.t. $C_i^{[2..d]} = C'^{[1..d-1]}_j$, then output 1, else output 0.

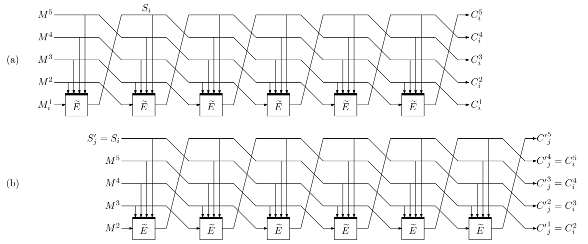


Fig. 5 Structure of Φ_6 for $d = 5$. (a): i-th query, (b) j-th query satisfying $S'_j = S_i$.

This algorithm adopts the same approach as the one for Φ_d. However, the internal states $S_i = \widetilde{E}(M^{[2..d]}, M_i)$ cannot be directly observed. We make $O(2^{n/2})$ queries so that we have the dn-bit state collision with a high probability. Let $q = 2^{n/2}$. The collision probability among the q values of S_i and q values of S'_j can be evaluated as follows:

$$\Pr[\{S_1, \ldots, S_q\} \cap \{S'_1, \ldots, S'_q\} \neq \emptyset]$$
$$\geq \left(1 - \frac{1}{e}\right) \frac{q(q-1)}{2^n} \approx 0.632$$

Here, e is the base of the natural logarithm and the last approximation follows from $q = 2^{n/2}$.

As for the random permutation, the probability of the collision among $C_i^{[2..d]}$ and $C'^{[1..d-1]}_j$ can be evaluated in a similar way by regarding them as $(d-1)n$-bit random values. We obtain

$$\Pr[\{C_1^{[2..d]}, \ldots, C_q^{[2..d]}\}$$
$$\cap \{C'^{[1..d-1]}_1, \ldots, C'^{[1..d-1]}_q\} \neq \emptyset]$$
$$\leq \frac{0.5q^2}{2^{(d-1)n}} = \frac{0.5}{2^{(d-2)n}},$$

where we used $q = 2^{n/2}$ for the last equality.

From the discussion above, we obtain the lower bound of the distinguishing advantage as

$$\mathbf{Adv}_{\Phi_r}^{\mathrm{prp}}(\mathcal{A}) \gtrapprox 0.5 \left(1 - \frac{1}{2^{(d-2)n}}\right).$$

An example of Φ_6 for $d = 5$ is shown in Fig. 5.

If $d = 2$, this algorithm does not work because in π, we have an n-bit output collision in step 4 with a high probability. To deal with this problem, we modify the algorithm as follows:

4′. If there exists no (i, j) satisfying $C_i^2 = C'^1_j$, then output 0.

5′. For (i, j) s.t. $C_i^2 = C'^1_j$, make encryption queries

$X^{[1..2]} \leftarrow O(C_i^{[1..2]})$ and $X'^{[1..2]} \leftarrow O(C_j'^{[1..2]})$.

6′. If $X^2 = X'^1$ holds, then output 1, else output 0.

Steps with a prime symbol are modified or added for $d = 2$. In both Φ_r and π, this algorithm aborts in step 4 with almost the same probability, and we see that the algorithm proceeds to steps 5′ and 6′ with a high probability.

Extra steps (steps 5′ and 6′) are based on the distinguisher on Φ_d. If $S_i = S_j'$ holds for some (i, j) in Φ_r, then we see that $C_i^{[1..2]}$ and $C_j'^{[1..2]}$ in step 5′ are the input and output of the r-th round of the encryption of (M^2, S_j'). Therefore, this algorithm outputs 1 with a high probability in Φ_r and outputs 0 in π with a similar discussion for Φ_d. □

5. Security of $\widehat{\Phi}_r$

We have the following theorem for $\widehat{\Phi}_r$.

Theorem 4: Fix $d \geq 2$. Let $\widehat{E}$ be the $((d-1)n, n)$-bit IC, and $\widehat{\Phi}_r = \widehat{\Phi}_r[\widehat{E}]$ be the r-round single IC-based Feistel cipher. Then for any $r \geq 1$, $\widehat{\Phi}_r$ is not indifferentiable from a random permutation.

Proof : We first consider the case $r \leq d$. Now we see that the same adversary against Φ_r for $r \leq d$ in Sect. 4.1 works as the adversary against $\widehat{\Phi}_r$, since the adversary against Φ_r can be regarded as the adversary against $\widehat{\Phi}_r$ in the indifferentiability notion that makes only construction queries without making any primitive queries. Although the simulator can make queries to a random permutation π, the simulator cannot control π's entries at all, so that any simulator does not affect the success probability of the adversary.

Next, we consider the case $r \geq d + 1$. We take the approach of the adversary against Φ_r with $r \geq d+1$ presented in Sect. 4.3. For an arbitrary message $M^{[1..d]} \in \{0,1\}^{dn}$, $\mathcal{A}$ first obtains the output of the 1st round IC by using a primitive query $S \leftarrow \widehat{E}(M^{[2..d]}, M_1)$. Next, $\mathcal{A}$ makes two construction queries with messages $M^{[1..d]}$ and $M^{[2..d]} \parallel S$ to obtain ciphertexts $C^{[1..d]}$ and $C'^{[1..d]}$. Then $\mathcal{A}$ outputs 1 if $C^{[2..d]} = C'^{[1..d-1]}$. Otherwise, $\mathcal{A}$ outputs 0.

In $\widehat{\Phi}_r$, the ciphertexts $C^{[1..d]}$ and $C'^{[1..d]}$ always satisfy $C^{[2..d]} = C'^{[1..d-1]}$. Observe that the complexity to search for the internal state S is replaced with a primitive query, and hence $\mathcal{A}$ runs with $O(1)$ queries. On the other hand, in π, the simulator has to find S such that the last $(d-1)n$ bits of $\pi(M^{[1..d]})$ collides with the first $(d-1)n$ bits of $\pi(M^{[2..d]} \parallel S)$. However, finding such S needs approximately $O(2^{(d-1)n})$ queries, or there does not exist such S. Therefore, $\mathcal{A}$ can distinguish $\widehat{\Phi}_r$ from π with a high probability. □

6. Indifferentiability of Feistel Cipher with Constants

We have seen in the previous section that for any $r \geq 1$, $\widehat{\Phi}_r[\widehat{E}]$ cannot be secure in the indifferentiability notion. The attack can be seen as a type of slide attacks [20], and introducing a round constant is a well-known countermeasure against the attack. In this section, we consider a variant of $\widehat{\Phi}_r$ that uses a round constant. One may hope that the round constant prevents the slide attacks. However, we show that this is not the case for $r = 2d - 1$ in the indifferentiability notion.

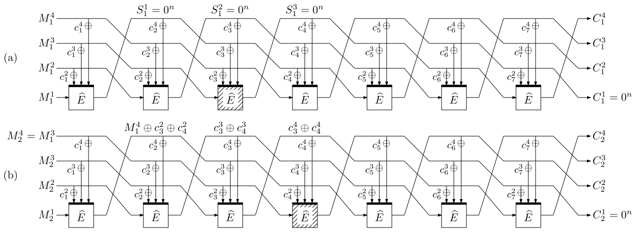


Fig. 6 Structure of $\widehat{\Phi}'_7$. Hatched ICs have the same input block, key, and output block. (a) step 6, (b) step 7.

We have the following theorem for $\widehat{\Phi}'_{2d-1}$.

Theorem 5: Fix $d \geq 2$. Let $\widehat{E}$ be the $((d-1)n, n)$-bit IC, $c_1^2, \ldots, c_1^d, \ldots, c_{2d-1}^2, \ldots, c_{2d-1}^d$ be the n-bit round constants, and $\widehat{\Phi}'_{2d-1} = \widehat{\Phi}'_{2d-1}[\widehat{E}]$ be the r-round single IC-based Feistel cipher with round constants, where $r = 2d - 1$. Then $\widehat{\Phi}_{2d-1}$ is not indifferentiable from a random permutation.

Proof : We show that $\widehat{\Phi}'_{2d-1}$ can be distinguished from π with $O(1)$ queries.

1. Fix $S_1^1 = \cdots = S_1^{d-1} = C_1^1 = 0^n$.
2. Obtain M_1^d by a primitive query of ϕ_d^{-1} with $S_1^1, \ldots, S_1^{d-1}, C_1^1$.
3. Obtain $C_1^2, \ldots, C_1^d$ by primitive queries of $\phi_{d+1}, \ldots, \phi_{2d-1}$ with $S_1^1, \ldots, S_1^{d-1}, C_1^1$.
4. Fix $S_2^1 = M_1^d \oplus c_{d-1}^2 \oplus c_d^2, S_2^2 = c_{d-1}^3 \oplus c_d^3, \ldots, S_2^{d-1} = c_{d-1}^d \oplus c_d^d$, and $C_2^1 = 0^n$.
5. Obtain $C_2^2, \ldots, C_2^d$ by primitive queries of $\phi_{d+1}, \ldots, \phi_{2d-1}$ with $S_2^1, \ldots, S_2^{d-1}, C_2^1$.
6. Make a construction query $M_1^{[1..d]} \leftarrow O^{-1}(C_1^{[1..d]})$.
7. Make a construction query $M_2^{[1..d]} \leftarrow O^{-1}(C_2^{[1..d]})$.
8. If $M_1^{d-1} = M_2^d$ holds, then output 1, else output 0.

An example of $\widehat{\Phi}'_7$ with $d = 4$ is shown in Fig. 6.

Figure 7 focuses on ϕ_{d-1} and ϕ_d of the construction. We first fix all the d-line output of ϕ_d in the 1st query to all zero. At this point, the output of IC in ϕ_{d-1} is also fixed as 0^n, which is the hatched IC in Fig. 7(a). The 2nd construction query reproduces the input and output of the hatched IC in the 1st query. Therefore, the bottommost dash-dotted line of the ϕ_d outputs in the 1st and 2nd queries collide. We observe these values as output lines of $\widehat{\Phi}'_{2d-1}$ even when $d - 1$ extra rounds are appended to an output side of ϕ_d. Furthermore, the inputs of the hatched ICs, namely, the bottommost dashed line of the ϕ_{d-1} input in the 1st query and the penultimate dashed line of the ϕ_{d-1} input in the 2nd query are equal. This collision occurs even when we append $d - 2$ additional rounds to an input side of ϕ_{d-1}.

Now we observe that n-bit simultaneous collisions on the input and output of the construction. We see that finding

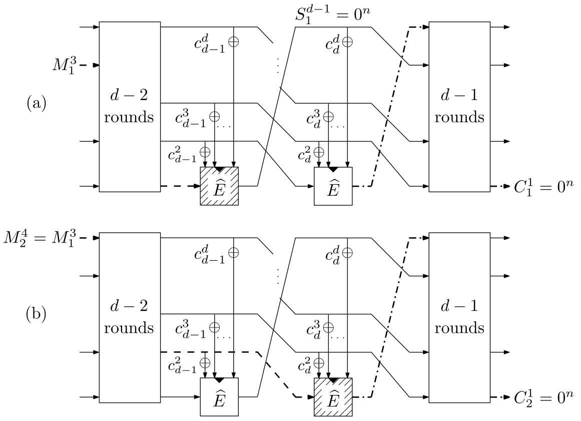


Fig. 7 ϕ_{d-1} and ϕ_d of $\widehat{\Phi}'_{2d-1}$. Hatched ICs have the same input block, key, and output block. (a) step 6, (b) step 7.

such a collision in π is not possible if we consider efficient simulators. Therefore, the probability of $M_1^{d-1} = M_2^d$ is negligible in π. □

As a remark, this algorithm never makes primitive queries once a construction query is made. This implies that $\widehat{\Phi}'_{2d-1}[\widehat{E}]$ does not achieve the sequential indifferentiability notion [34] which is a weaker notion of indifferentiability.

7. Conclusions

In this paper, we analyzed the security of the single-keyed TBC-based Feistel ciphers in the indistinguishability notion, and the single IC-based Feistel ciphers in the indifferentiability notion. We completed the security characterization depending on the number of rounds. We also considered a structure that employs a round constant, and showed that this does not work for the case $r = 2d-1$ in the indifferentiability notion.

As open problems, there have been various proposals to modify the PRF-based Feistel cipher so that the security is maintained [4]–[7], and it would be interesting to see how one can modify the single-keyed TBC-based/single IC-based Feistel ciphers to improve the security. With respect to the construction with a round constant, we have only covered the indifferentiability notion of the case $r = 2d-1$, and it would be interesting to see the security with other parameters and/or in the indistinguishability notion.

Acknowledgments

This work was supported by JSPS KAKENHI JP20K11675. The authors thank the anonymous reviewers for careful reading of the paper.

References

[1] K. Tsuji and T. Iwata, “Feistel ciphers based on a single primitive,” Cryptography and Coding - 19th IMA International Conference, IMACC 2023, London, UK, Proceedings, E.A. Quaglia, ed., Lecture Notes in Computer Science, vol.14421, pp.57–79, Springer, 2023.

[2] M. Luby and C. Rackoff, “How to construct pseudorandom permutations from pseudorandom functions,” SIAM J. Comput., vol.17, no.2, pp.373–386, 1988.

[3] Y. Zheng, T. Matsumoto, and H. Imai, “Impossibility and optimality results on constructing pseudorandom permutations (extended abstract),” Advances in Cryptology - EUROCRYPT ’89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, Proceedings, J. Quisquater and J. Vandewalle, eds., Lecture Notes in Computer Science, vol.434, pp.412–422, Springer, 1989.

[4] J. Pieprzyk, “How to construct pseudorandom permutations from single pseudorandom functions,” Advances in Cryptology - EUROCRYPT’90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, Proceedings, I. Damgård, ed., Lecture Notes in Computer Science, vol.473, pp.140–150, Springer, 1990.

[5] J. Patarin, “How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function,” Advances in Cryptology - EUROCRYPT’92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, Proceedings, R.A. Rueppel, ed., Lecture Notes in Computer Science, vol.658, pp.256–266, Springer, 1992.

[6] M. Nandi, “The characterization of luby-rackoff and its optimum single-key variants,” Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, Proceedings, G. Gong and K.C. Gupta, eds., Lecture Notes in Computer Science, vol.6498, pp.82–97, Springer, 2010.

[7] M. Nandi, “On the optimality of non-linear computations of length-preserving encryption schemes,” Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, Proceedings, Part II, T. Iwata and J.H. Cheon, eds., Lecture Notes in Computer Science, vol.9453, pp.113–133, Springer, 2015.

[8] M.D. Liskov, R.L. Rivest, and D.A. Wagner, “Tweakable block ciphers,” J. Cryptol., vol.24, no.3, pp.588–613, 2011.

[9] K. Minematsu, “Beyond-birthday-bound security based on tweakable block cipher,” Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, Revised Selected Papers, O. Dunkelman, ed., Lecture Notes in Computer Science, vol.5665, pp.308–326, Springer, 2009.

[10] J. Coron, Y. Dodis, A. Mandal, and Y. Seurin, “A domain extender for the ideal cipher,” Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, Proceedings, D. Micciancio, ed., Lecture Notes in Computer Science, vol.5978, pp.273–289, Springer, 2010.

[11] U.M. Maurer, R. Renner, and C. Holenstein, “Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology,” Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, Proceedings, M. Naor, ed., Lecture Notes in Computer Science, vol.2951, pp.21–39, Springer, 2004.

[12] J. Coron, T. Holenstein, R. Künzler, J. Patarin, Y. Seurin, and S. Tessaro, “How to build an ideal cipher: The indifferentiability of the feistel construction,” J. Cryptol., vol.29, no.1, pp.61–114, 2016.

[13] D. Dachman-Soled, J. Katz, and A. Thiruvengadam, “10-round feistel is indifferentiable from an ideal cipher,” Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, Proceedings, Part II, M. Fischlin and J. Coron, eds., Lecture Notes in Computer Science, vol.9666, pp.649–678, Springer, 2016.

[14] Y. Dai and J.P. Steinberger, “Indifferentiability of 8-round feistel networks,” Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, Proceedings, Part I, M. Robshaw and J. Katz, eds., Lecture Notes in Computer Science, vol.9814, pp.95–120, Springer, 2016.

[15] R. Bhaumik, M. Nandi, and A. Raychaudhuri, “Improved indiffer-

entiability security proof for 3-round tweakable luby-rackoff," Des. Codes Cryptogr., vol.89, no.10, pp.2255–2281, 2021.

[16] K. Minematsu, "Building blockcipher from small-block tweakable blockcipher," Des. Codes Cryptogr., vol.74, no.3, pp.645–663, 2015.

[17] R. Nakamichi and T. Iwata, "Iterative block ciphers from tweakable block ciphers with long tweaks," IACR Trans. Symmetric Cryptol., vol.2019, no.4, pp.54–80, 2019.

[18] C. Guo and D. Lin, "Improved domain extender for the ideal cipher," Cryptogr. Commun., vol.7, no.4, pp.509–533, 2015.

[19] R. Nakamichi and T. Iwata, "Beyond-birthday-bound secure cryptographic permutations from ideal ciphers with long keys," IACR Trans. Symmetric Cryptol., vol.2020, no.2, pp.68–92, 2020.

[20] A. Biryukov and D.A. Wagner, "Slide attacks," Fast Software Encryption, 6th International Workshop, FSE'99, Rome, Italy, Proceedings, L.R. Knudsen, ed., Lecture Notes in Computer Science, vol.1636, pp.245–259, Springer, 1999.

[21] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink, and J.P. Steinberger, "On the indifferentiability of key-alternating ciphers," Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, Proceedings, Part I, R. Canetti and J.A. Garay, eds., Lecture Notes in Computer Science, vol.8042, pp.531–550, Springer, 2013.

[22] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J.P. Steinberger, "Minimizing the two-round even-mansour cipher," Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, Proceedings, Part I, J.A. Garay and R. Gennaro, eds., Lecture Notes in Computer Science, vol.8616, pp.39–56, Springer, 2014.

[23] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, "Cryptanalysis of iterated even-mansour schemes with two keys," Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., Proceedings, Part I, P. Sarkar and T. Iwata, eds., Lecture Notes in Computer Science, vol.8873, pp.439–457, Springer, 2014.

[24] B. Cogliati and Y. Seurin, "On the provable security of the iterated even-mansour cipher against related-key and chosen-key attacks," Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, Proceedings, Part I, E. Oswald and M. Fischlin, eds., Lecture Notes in Computer Science, vol.9056, pp.584–613, Springer, 2015.

[25] S. Xu, Q. Da, and C. Guo, "Minimizing even-mansour ciphers for sequential indifferentiability (without key schedules)," Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, Proceedings, T. Isobe and S. Sarkar, eds., Lecture Notes in Computer Science, vol.13774, pp.125–145, Springer, 2022.

[26] S. Xu, Q. Da, and C. Guo, "Chosen-key secure even-mansour cipher from a single permutation," IACR Trans. Symmetric Cryptol., vol.2023, no.1, pp.244–287, 2023.

[27] J. Daemen, L.R. Knudsen, and V. Rijmen, "The block cipher square," Fast Software Encryption, 4th International Workshop, FSE'97, Haifa, Israel, Proceedings, E. Biham, ed., Lecture Notes in Computer Science, vol.1267, pp.149–165, Springer, 1997.

[28] A. Biryukov and A. Shamir, "Structural cryptanalysis of SASAS," J. Cryptol., vol.23, no.4, pp.505–518, 2010.

[29] I. Dinur, O. Dunkelman, and A. Shamir, "Improved attacks on full GOST," Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, Revised Selected Papers, A. Canteaut, ed., Lecture Notes in Computer Science, vol.7549, pp.9–28, Springer, 2012.

[30] T. Isobe and K. Shibutani, "Generic key recovery attack on feistel scheme," Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, Proceedings, Part I, K. Sako and P. Sarkar, eds., Lecture Notes in Computer Science, vol.8269, pp.464–485, Springer, 2013.

[31] A. Bar-On, E. Biham, O. Dunkelman, and N. Keller, "Efficient slide attacks," J. Cryptol., vol.31, no.3, pp.641–670, 2018.

[32] J. Patarin, "The "Coefficients H" technique," Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, Revised Selected Papers, R.M. Avanzi, L. Keliher, and F. Sica, eds., Lecture Notes in Computer Science, vol.5381, pp.328–345, Springer, 2008.

[33] S. Chen and J.P. Steinberger, "Tight security bounds for key-alternating ciphers," Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, Proceedings, P.Q. Nguyen and E. Oswald, eds., Lecture Notes in Computer Science, vol.8441, pp.327–350, Springer, 2014.

[34] A. Mandal, J. Patarin, and Y. Seurin, "On the public indifferentiability and correlation intractability of the 6-round feistel construction," Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, Proceedings, R. Cramer, ed., Lecture Notes in Computer Science, vol.7194, pp.285–302, Springer, 2012.

Appendix: Security Proof of Φ_{d+1}

We show the detailed proof of Theorem 2. We recall the theorem.

Theorem 2: Fix $d \geq 2$. Let $\widetilde{E}$ be the $(n, (d-1)n)$-bit TRP, and $\Phi_{d+1} = \Phi_{d+1}[\widetilde{E}]$ be the r-round single-keyed TBC-based Feistel cipher, where $r = d + 1$. Then for any adversary $\mathcal{A}$ that makes at most q queries, we have

$$\mathbf{Adv}^{\mathrm{sprp}}_{\Phi_{d+1}}(\mathcal{A}) \leq \frac{(4d+1)q^2}{2^n} + \frac{0.5q^2}{2^{dn}}.$$

We first define the transcripts followed by two oracles, the real world oracle based on Φ_{d+1} and the ideal world oracle based on the random permutation π, and the bad conditions. Next, we compute the bad probability in Lemma 2 and the good probability ratio in Lemma 3. The security bound is obtained from these lemmas and the coefficient-H technique in Lemma 1.

A.1 Transcripts

The adversary $\mathcal{A}$ is given access to the encryption and decryption oracles. If the i-th query is an encryption query $M_i^{[1..d]}$, then $\mathcal{A}$ obtains the corresponding ciphertext $C_i^{[1..d]}$. If the i-th query is a decryption query $C_i^{[1..d]}$, then $\mathcal{A}$ obtains $M_i^{[1..d]}$. Without loss of generality, we assume that $\mathcal{A}$ makes exactly q queries, does not repeat a query, and does not make a redundant query, i.e., if $\mathcal{A}$ obtains $C_i^{[1..d]}$ for an encryption query $M_i^{[1..d]}$, then it does not use $C_i^{[1..d]}$ in the subsequent decryption queries, and vice versa. As we detail below, after making q queries and before returning the decision bit, $\mathcal{A}$ is given all the internal state values $S_1, \ldots, S_q$. Since it is only beneficial to $\mathcal{A}$, there is no loss of generality of giving the additional input to $\mathcal{A}$. Then the transcript is defined as follows:

$$((M_1^{[1..d]}, C_1^{[1..d]}), \ldots, (M_q^{[1..d]}, C_q^{[1..d]}), S_1, \ldots, S_q) \tag{A$\cdot$ 1}$$

Algorithm 1 Procedure of $\mathcal{R}$ for the i-th query (encryption)

```
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$
  $X_i^{[1..d]} \leftarrow M_i^{[1..d]}$
  for $j = 1$ to $d+1$ do
      $X_i^{d+j} \leftarrow \widetilde{E}(X_i^{[1+j..d-1+j]}, X_i^j)$
  $S_i \parallel C_i^{[1..d]} \leftarrow X_i^{[d+1..2d+1]}$
  return $C^{[1..d]}$
```

Algorithm 2 Procedure of $\mathcal{R}^{-1}$ for the i-th query (decryption)

```
Input: $C^{[1..d]} \in \{0,1\}^{dn}$
Output: $M^{[1..d]} \in \{0,1\}^{dn}$
  $X_i^{[d+2..2d+1]} \leftarrow C_i^{[1..d]}$
  for $j = d+1$ to $1$ do
      $X_i^j \leftarrow \widetilde{E}(X_i^{[2+j..d+j]}, X_i^{1+j})$
  $M_i^{[1..d]} \parallel S_i \leftarrow X_i^{[1..d+1]}$
  return $M^{[1..d]}$
```

Fig. A· 1 Algorithm of $\mathcal{R}$ and $\mathcal{R}^{-1}$.

Algorithm 3 Procedure of $\mathcal{I}$ for the i-th query (encryption)

```
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$
  $C_i^{[1..d]} \leftarrow \pi(M_i^{[1..d]})$
  return $C_i^{[1..d]}$
```

Algorithm 4 Procedure of $\mathcal{I}^{-1}$ for the i-th query (decryption)

```
Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $M_i^{[1..d]} \in \{0,1\}^{dn}$
  $M_i^{[1..d]} \leftarrow \pi^{-1}(C_i^{[1..d]})$
  return $M_i^{[1..d]}$
```

Algorithm 5 Generation of dummy internal states $S_1, \ldots, S_q$

```
Input: $(M_1^{[1..d]}, C_1^{[1..d]}), \ldots, (M_q^{[1..d]}, M_q^{[1..d]}) \in (\{0,1\}^{dn} \times \{0,1\}^{dn})^q$
Output: $S_1, \ldots, S_q \in (\{0,1\}^n)^q$
  for $i = 1$ to $q$ do
      if the $i$-th query is encryption then
          if $\widetilde{E}(M_i^{[2..d]}, M_i^1)$ is defined then
              $S_i \leftarrow \widetilde{E}(M_i^{[2..d]}, M_i^1)$
          else
              $S_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Ran}(M_i^{[2..d]})$
      else                                            ▷ the i-th query is decryption
          if $\widetilde{E}^{-1}(C_i^{[1..d-1]}, C_i^d)$ is defined then
              $S_i \leftarrow \widetilde{E}^{-1}(C_i^{[1..d-1]}, C_i^d)$
          else
              $S_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Dom}(C_i^{[1..d-1]})$
      $X_i^{[1..2d+1]} \leftarrow M_i^{[1..d]} \parallel S_i \parallel C_i^{[1..d]}$
      for $j = 1$ to $d+1$ do
          $\widetilde{E}(X_i^{[1+j..d-1+j]}, X_i^j) \leftarrow X_i^{d+j}$
  return $S_1, \ldots, S_q$
```

Fig. A· 2 Algorithm of $\mathcal{I}$ and $\mathcal{I}^{-1}$, where Dom(T) and Ran(T) are defined as Dom(T) $= \{x \mid \widetilde{E}(T,x) = y$ is defined for some $y\}$ and Ran(T) $= \{y \mid \widetilde{E}(T,x) = y$ is defined for some $x\}$.

A.2 Definition of the Oracles

The real world oracles $\mathcal{R}, \mathcal{R}^{-1}$ internally make use of the block cipher Φ_{d+1} and its inverse Φ_{d+1}^{-1}. After making q queries, the oracles $\mathcal{R}, \mathcal{R}^{-1}$ give $\mathcal{A}$ all the internal states $S_1, \ldots, S_q$. Fig. A· 1 shows the algorithms of $\mathcal{R}, \mathcal{R}^{-1}$.

The ideal world oracles $\mathcal{I}, \mathcal{I}^{-1}$ internally make use of the random permutation π and its inverse π^{-1}. After q queries, $\mathcal{I}, \mathcal{I}^{-1}$ generate dummy internal states $S_1, \ldots, S_q$ with the same probability distribution as TRP $\widetilde{E}$. For this, for an encryption query, the oracle simulates the 1st round TRP. For a decryption query, the oracle simulates the $(d+1)$-st round TRP. After completing the simulation, $S_1, \ldots, S_q$ are given to $\mathcal{A}$. Fig. A· 2 shows the algorithms of $\mathcal{I}, \mathcal{I}^{-1}$.

A.3 Bad Conditions

For the TRP $\widetilde{E}$ in the real world, the tweak determines the permutation between the input and output of the TRP. Accordingly, if the tweaks are the same, the TRP does not output distinct outputs from the same inputs or distinct inputs from the same outputs. By applying this to all the combinations of the TRPs in Φ_{d+1}, we obtain the bad conditions of the whole structure of Φ_{d+1} as follows:

1. $\{M_1^1, \ldots, M_1^d, \ldots, M_q^1, \ldots, M_q^d\} \cap \{S_1, \ldots, S_q\} \neq \emptyset$
2. $\{C_1^1, \ldots, C_1^d, \ldots, C_q^1, \ldots, C_q^d\} \cap \{S_1, \ldots, S_q\} \neq \emptyset$
3. $|\{S_1, \ldots, S_q\}| < q$

Recall that a transcript is defined as (A· 1), and let $\mathcal{T}_{\text{bad}}$ be the set of all the transcripts that satisfy at least one of the conditions above. Let $\mathcal{T}_{\text{good}}$ be the set of all the transcripts that does not satisfy any of the conditions above.

In what follows, we discuss the correctness of the above bad conditions, i.e., without the bad conditions, we show that the underlying TRP $\widetilde{E}$ can interpolate all the relevant inputs, tweaks, and the outputs with a non-zero probability. See Fig. 4 for an example of Φ_6.

First, observe that the absence of the above three conditions guarantees that all the tweaks in $\widetilde{E}^2, \ldots, \widetilde{E}^d$ are distinct. That is, there are q tweaks for each of $\widetilde{E}^2, \ldots, \widetilde{E}^d$, and we thus have $q(d-1)$ values of the tweak in total for $\widetilde{E}^2, \ldots, \widetilde{E}^d$. It can be verified that all these $q(d-1)$ values are distinct, and they are also different from the q tweaks of $\widetilde{E}^1$ and the q tweaks of $\widetilde{E}^{d+1}$.

Next, let $\mathcal{T}^1 = \{M_1^{[2..d]}, \ldots, M_q^{[2..d]}\}$ be the set of the q tweaks of $\widetilde{E}^1$ and $\mathcal{T}^{d+1} = \{C_1^{[1..d-1]}, \ldots, C_q^{[1..d-1]}\}$ be the set of the q tweaks of $\widetilde{E}^{d+1}$. From the discussion above, all these $2q$ tweaks are different from those of $\widetilde{E}^2, \ldots, \widetilde{E}^d$, while we may have $|\mathcal{T}^1| < q$, $\mathcal{T}^1 \cap \mathcal{T}^{d+1} \neq \emptyset$, or $|\mathcal{T}^{d+1}| < q$.

- If $|\mathcal{T}^1| < q$, i.e., if $M_i^{[2..d]} = M_j^{[2..d]}$ holds for some $1 \le i < j \le q$, we necessary have $M_i^1 \ne M_j^1$ since the adversary does not repeat a query, and from $S_i \ne S_j$, this case does not yield inconsistency in $\widetilde{E}$.
- If $\mathcal{T}^1 \cap \mathcal{T}^{d+1} \ne \emptyset$, there are two cases to consider.
  The first case is $M_i^{[2..d]} = C_j^{[2..d]}$ for some $1 \le i < j \le q$. In this case, $\widetilde{E}^1$ and $\widetilde{E}^{d+1}$ have to satisfy $S_i = \widetilde{E}^1(M_i^{[2..d]}, M_i^1)$ and $C_j^d = \widetilde{E}^{d+1}(C_j^{[1..d-1]}, S_j)$, which is possible since $S_i \ne C_j^d$ and $M_i^1 \ne S_j$.
  The second case is $M_i^{[2..d]} = C_i^{[2..d]}$ for some $1 \le i \le q$. In this case, $\widetilde{E}^1$ and $\widetilde{E}^{d+1}$ have to satisfy $S_i = \widetilde{E}^1(M_i^{[2..d]}, M_i^1)$ and $C_i^d = \widetilde{E}^{d+1}(C_i^{[1..d-1]}, S_i)$, which is again possible since $S_i \ne C_i^d$ and $M_i^1 \ne S_i$.
- The analysis of the case $|\mathcal{T}^{d+1}| < q$ is similar to the case $|\mathcal{T}^1| < q$.

Therefore, the absence of the bad conditions implies that the TRP $\widetilde{E}$ can interpolate all the relevant inputs, tweaks, and the outputs with a non-zero probability. We next compute the probability of the bad conditions and the ratio of the good probabilities to use the coefficient-H Technique.

A.4 Probability of the Bad Conditions

We have the following lemma.

Lemma 2: We have $\Pr[\Theta_\mathcal{I} \in \mathcal{T}_{\text{bad}}] \le \dfrac{(4d+1)q^2}{2^n}$.

Proof : We compute the probability of the bad conditions based on the randomness of $S_1, \ldots, S_q$. Assume that $\mathcal{A}$ has completed making q queries to the oracles, and hence $(M_1^{[1..d]}, C_1^{[1..d]}), \ldots, (M_q^{[1..d]}, C_q^{[1..d]})$ are fixed. We further assume that we do not have the bad conditions for $S_1, \ldots, S_{i-1}$, and we compute the probability that S_i causes one of the bad conditions, which we write "S_i is bad." We then have

$$\Pr[S_i \text{ is bad}] \le \frac{2dq + (i-1)}{2^n - 2q}.$$

The term $2q$ of the denominator indicates the maximum value of $|\mathrm{Ran}(M_i^{[2..d]})|$ or $|\mathrm{Dom}(C_i^{[1..d-1]})|$. Due to the uniqueness of $S_1, \ldots, S_{i-1}$, the tweaks of TRPs other than $\widetilde{E}^1$ and $\widetilde{E}^{d+1}$ also have unique values. Therefore, $|\mathrm{Ran}(M_i^{[2..d]})|$ or $|\mathrm{Dom}(C_i^{[1..d-1]})|$ takes the maximum value of $2q$ when $M_j^{[2..d]}$ and $C_j^{[1..d-1]}$ take the same value for all $j = 1, \ldots, i-1$. Besides, from the uniqueness of $S_1, \ldots, S_{i-1}$ and the assumption that no queries are repeated, it is guaranteed that the corresponding entry, i.e., $(M_i^{[2..d]}, M_i^1)$ for encryption or $(C_i^{[1..d-1]}, C_i^d)$ for decryption, does not exist at the generation of S_i. That is, S_i has randomness when generating it.

Now, by taking the summation of $\Pr[S_i$ is bad$]$, we have

$$\Pr[\Theta_\mathcal{I} \in \mathcal{T}_{\text{bad}}] \le \sum_{i=1}^{q} \frac{2dq + (i-1)}{2^n - 2q}$$

$$\le \frac{(2d + 0.5)q^2}{2^n - 2q}$$

$$\le \frac{(4d+1)q^2}{2^n},$$

where the third inequality follows from $2q < 2^{n-1}$.

A.5 Ratio of the Good Probabilities

We have the following lemma.

Lemma 3: For any $\theta \in \mathcal{T}_{\text{good}}$, we have $\dfrac{\Pr[\Theta_\mathcal{R} = \theta]}{\Pr[\Theta_\mathcal{I} = \theta]} \ge 1 - \dfrac{0.5q^2}{2^{dn}}$.

Proof : First, we define the following two sets:

$$Q_e = \{i \mid \text{the } i\text{-th query is encryption}\}$$
$$Q_d = \{i \mid \text{the } i\text{-th query is decryption}\}$$

In the real world, we additionally define two sets as follows:

$$\begin{aligned} S_i^{\text{enc},x} &= \{(j,k) \\ &\mid ((j < i \wedge 1 \le k \le d+1) \vee (j = i \wedge 1 \le k < x)) \\ &\wedge (\text{the } j\text{-th tweak of } \widetilde{E}^k) = (\text{the } i\text{-th tweak of } \widetilde{E}^x)\} \\ S_i^{\text{dec},x} &= \{(j,k) \\ &\mid ((j < i \wedge 1 \le k \le d+1) \vee (j = i \wedge x < k \le d+1)) \\ &\wedge (\text{the } j\text{-th tweak of } \widetilde{E}^k) = (\text{the } i\text{-th tweak of } \widetilde{E}^x)\} \end{aligned}$$

Intuitively, $S_i^{\text{enc},x}$ is the set of (j,k) that shares the same tweak as the i-th tweak of $\widetilde{E}^x$ when the i-th query is encryption, and $S_i^{\text{dec},x}$ is that when the i-th query is decryption. That is, for the i-th tweak of $\widetilde{E}^x$, these sets indicate the indices that share the same tweak in the previous TRP calls. Then, the probability can be evaluated as follows:

$$\begin{aligned} &\Pr[\Theta_\mathcal{R} = \theta] \\ &= \prod_{x=1}^{d+1} \left(\prod_{i \in Q_e} \frac{1}{2^n - |S_i^{\text{enc},x}|} \times \prod_{i \in Q_d} \frac{1}{2^n - |S_i^{\text{dec},x}|} \right) \\ &\ge \frac{1}{(2^n)^{dq}} \times \prod_{i \in Q_e} \frac{1}{2^n - |S_i^{\text{enc},1}|} \times \prod_{i \in Q_d} \frac{1}{2^n - |S_i^{\text{dec},d+1}|}. \end{aligned}$$

The last inequality is obtained by assuming $|S_i^{\text{enc},x}| = |S_i^{\text{dec},x}| = 0$ except for $|S_i^{\text{enc},1}|$ and $|S_i^{\text{dec},d+1}|$.

In the ideal world, as with the real world, we define two sets as follows:

$$\begin{aligned} T_i^{\text{enc},x} &= \{(j,k) \\ &\mid ((j < i \wedge 1 \le k \le d+1) \vee (j = i \wedge 1 \le k < x)) \\ &\wedge (\text{the } j\text{-th tweak of } \widetilde{E}^k) = (\text{the } i\text{-th tweak of } \widetilde{E}^x)\} \\ T_i^{\text{dec},x} &= \{(j,k) \end{aligned}$$

$$\begin{aligned}&\mid ((j < i \land 1 \le k \le d+1) \lor (j = i \land x < k \le d+1))\\ &\land (\text{the } j\text{-th tweak of } \widetilde{E}^k) = (\text{the } i\text{-th tweak of } \widetilde{E}^x)\} \,.\end{aligned}$$

Here, in the definitions above, we abuse the notation to write $\widetilde{E}^k$ for the TRP $\widetilde{E}$ used in the k-th round in Algorithm 5. Then, the probability can be evaluated as follows:

$$\begin{aligned}&\Pr[\Theta_{\mathcal{I}} = \theta]\\ &= \frac{1}{(2^{dn})_q} \times \prod_{i \in Q_e} \frac{1}{2^n - |T_i^{\mathrm{enc},1}|} \times \prod_{i \in Q_d} \frac{1}{2^n - |T_i^{\mathrm{dec},d+1}|} \,.\end{aligned}$$

Finally, we compute the ratio of the two possibilities. We have

$$\begin{aligned}&\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]}\\ &\ge \frac{(2^{dn})_q}{(2^n)^{dq}} \times \prod_{i \in Q_e} \frac{2^n - |S_i^{\mathrm{enc},1}|}{2^n - |T_i^{\mathrm{enc},1}|} \times \prod_{i \in Q_d} \frac{2^n - |S_i^{\mathrm{dec},d+1}|}{2^n - |T_i^{\mathrm{dec},d+1}|}\\ &\ge 1 - \frac{0.5q^2}{2^{dn}} \,,\end{aligned}$$

where the last inequality follows since $S_i^{\mathrm{enc},x} = T_i^{\mathrm{enc},x}$ and $S_i^{\mathrm{dec},x} = T_i^{\mathrm{dec},x}$ are always satisfied from the definitions of the oracles.

From Lemma 2, Lemma 3, and the coefficient-H technique, we obtain Theorem 2.

Kento Tsuji received the B.E. degree from Nagoya University, Japan in 2022. Since 2022, he has been enrolled in the master's program in department of information and communication engineering, Nagoya University.

Tetsu Iwata received his B.E., M.E., and Dr.E. degrees in electrical and electronic engineering from Tokyo Institute of Technology in 1997, 1999, and 2002, respectively. He is currently a Professor in the Department of Information and Communication Engineering at Nagoya University. He was the general co-chair of FSE 2017, and the program co-chairs of FSE 2010, ASIACRYPT 2014, and ASIACRYPT 2015. He received the FSE 2015 best paper award, the CRYPTO 2019 best paper award, the FSE 2021 Test of Time award, and the FSE 2022 Test of Time award. His research interests include information security and cryptography.