IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2022, No. 4, pp. 24–91. DOI:10.46586/tosc.v2022.i4.24-91

Generalized Feistel Structures Based on Tweakable Block Ciphers

Kazuki Nakaya and Tetsu Iwata

Nagoya University, Nagoya, Japan
nakaya.kazuki.p6@s.mail.nagoya-u.ac.jp,tetsu.iwata@nagoya-u.jp

Abstract. A generalized Feistel structure (GFS) is a classical approach to construct a block cipher from pseudorandom functions (PRFs). Coron et al. at TCC 2010 instantiated a Feistel structure with a tweakable block cipher (TBC), and presented its provable security treatment. GFSs can naturally be instantiated with TBCs, and among several types of GFSs, the provable security result of TBC-based unbalanced GFSs was presented. TBC-based counterparts of the most basic types of GFSs, namely, type-1, type-2, and type-3 GFSs, can naturally be formalized, and the provable security result of these structures is open. In this paper, we present such formalization and show their provable security treatment. We use a TBC of n-bit blocks and n-bit tweaks, and we identify the number of rounds needed to achieve birthday-bound security and beyond-birthday-bound security (with respect to n). The n-bit security can be achieved with a finite number of rounds, in contrast to the case of classical PRF-based GFSs. Our proofs use Patarin's coefficient-H technique, and it turns out deriving a collision probability of various internal variables is non-trivial. In order to complete the proof, we introduce an approach to first compute a collision probability of *one specific* plaintext difference (or a ciphertext difference), and then *prove* that the case gives the maximum collision probability. We fully verify the correctness of our security bounds for a class of parameters by experimentally deriving upper bounds on the collision probability of internal variables. We also analyse the optimality of our results with respect to the number of rounds and the attack complexity.

Keywords: Generalized Feistel structure · Tweakable block cipher · Block cipher · Coefficient-H technique · Provable security

1 Introduction

Feistel Structure and Generalized Feistel Structure. There are various approaches for designing a secure block cipher, and the provable security treatment initiated by Luby and Rackoff [LR88] focuses on the structural soundness of the design. They considered a Feistel structure that uses a pseudorandom function (PRF) as a round function. They showed that with 3 rounds, it is a pseudorandom permutation (PRP), a block cipher that is indistinguishable from a random permutation against adversaries with chosen-plaintext attacks (CPAs), and with 4 rounds, it gives a strong PRP (SPRP), a block cipher that is secure against adversaries with chosen-plaintext-ciphertext attacks (CPCAs). The result has been extended and generalized in various ways. For instance, one obtains a better security bound by increasing the number of rounds [Pat98, Vau03, MP03, Pat03, Pat04], or one obtains a block cipher with a larger block length with a universal hash function [NR99] or with a generalized Feistel structure (GFS) [ZMI89].

To construct a block cipher of a certain block length, GFSs require a smaller PRF than a Feistel structure, since GFSs break the input block into smaller pieces. There are various

Received: 2022-06-01 Revised: 2022-09-01 Accepted: 2022-11-01 Published: 2022-12-07

types of GFSs, including unbalanced GFS [SK96], type-1, type-2, and type-3 GFSs [ZMI89], alternating GFS [AB96, Luc96], and Nyberg's GFS [Nyb96]. See Fig. 1 illustrating type-1, type-2, and type-3 GFSs. GFSs have been adopted in various practical designs. They are used, e.g., in hash functions SHA-1 and SHA-2 [NIS05], block ciphers [SSA+07, RRSY98], and cryptographic permutations [GM16]. The provable security treatment of type-1, type-2, and type-3 GFSs is presented in [ZMI89], followed by refined treatments in [HR10a]. The work by Shen, Guo, and Wang covers a wide range of GFSs [SGW20], and they further improved the results in [HR10a].

Tweakable Block Cipher Counterparts. A tweakable block cipher (TBC), formalized by Liskov et al. [LRW02, LRW11], generalizes a classical block cipher to take an additional input called a tweak. A TBC is a family of permutations indexed by a tweak and a key. Initially, TBCs have been constructed as a mode of operation of block ciphers [LRW02, LRW11]. The other direction to construct a block cipher with a large block length from TBCs was initiated by Minematsu [Min09]. Rich designs of practical TBCs as a primitive [JNP14, BJK+16, JNPS21] can be used to construct a block cipher with a large block length. Coron et al. [CDMS10] instantiated a Feistel structure with a TBC with n-bit blocks and n-bit tweaks to obtain a block cipher with $2n$-bit blocks, and showed that with 2 rounds, the construction gives an SPRP with the security bound of the form $O(q^2/2^n)$, i.e., birthday-bound security, where q is the number of queries. They also showed that with 3 rounds, it gives an SPRP with the security bound of the form $O(q^2/2^{2n})$, beyond-birthday-bound security (BBB security).

Following [Min15], Nakamichi and Iwata [NI19] analysed the TBC-based counterpart of the unbalanced GFS, where a contracting function is used as the round function. They showed the number of rounds to achieve birthday-bound security and BBB security.

Our Contributions. The TBC-based counterparts of the most basic types of GFSs, namely, type-1, type-2, and type-3 GFSs, can naturally be defined. In this paper, we formalize the structures and consider a question of analysing the provable security of these counterparts. See Fig. 2 for the structures analysed in this paper. We use a TBC of n-bit blocks and n-bit tweaks, and we identify the number of rounds needed to achieve birthday-bound security and BBB security (with respect to n). Concretely, we show the following results:

- For TBC-based type-1 GFSs with dn-bit blocks and r rounds, where $d \geq 3$, we consider PRP and SPRP security separately, as this construction has different security characteristics depending on the direction of the operation. For PRP security, it has birthday-bound security $O(q^2/2^n)$ with $r = 2d - 2$ rounds, and by adding d more rounds, i.e., with $r = 3d - 2$ rounds, the bound improves to BBB security $O(q^2/2^{2n})$. For SPRP security, we show that it has birthday-bound security $O(q^2/2^n)$ with $r = d^2 - 2d + 2$ rounds, and BBB security $O(q^2/2^{2n})$ with $r = d^2 - d + 2$ rounds.
- For TBC-based type-2 GFSs with dn-bit blocks and r rounds, where $d \geq 4$ is even, we consider SPRP security to show that it has birthday-bound security $O(q^2/2^n)$ with $r = d$ rounds, and BBB security $O(q^2/2^{2n})$ with $r = d + 2$ rounds.
- For TBC-based type-3 GFSs with dn-bit blocks and r rounds, where $d \geq 3$, we consider SPRP security and point out the correspondence to the result of TBC-based type-1 GFSs. It has birthday-bound security $O(q^2/2^n)$ with $r = d$ rounds, and BBB security $O(q^2/2^{2n})$ with $r = d + 1$ rounds.

Our proofs use Patarin's coefficient-H technique [Pat08] refined in [CS14]. In the proof, collision probabilities of various internal variables have to be evaluated. For a dn-bit block cipher we consider, a collision probability of internal variables depends on whether each n-bit block in a plaintext difference (or a ciphertext difference) has a non-zero value or

not. There are $(2^d - 1)$ cases to evaluate, and it turns out that theoretically deriving the collision probabilities while treating d as a parameter is non-trivial, as TBCs behave differently depending on whether it has a non-zero difference in inputs, tweaks, or outputs, and this makes it different from the analyses of PRF-based GFSs.

In order to complete the proof, we introduce an approach to first compute a collision probability of *one specific* plaintext difference (or a ciphertext difference) among the (2^d-1) possibilities, and we then *prove* that the case gives the maximum collision probability, by following the computation to show that any other plaintext difference does not have a larger collision probability.

In order to verify the correctness of our security bounds, we developed a program that exhaustively computes the collision probability for all the $(2^d - 1)$ possibilities. We executed the program in the range of $d \leq 16$, and we experimentally verified the correctness of our security bounds for parameters within the range.

We also analyse the optimality of our results with respect to the number of rounds and the attack complexity. Let r_{bb} be the number of rounds for birthday-bound security, and r_{bbb} be the number of rounds for BBB security. We present attacks against TBC-based type-1, type-2, and type-3 GFSs that use $q = 2^{n/2}$ queries when the number of rounds r satisfies $r_{\mathrm{bb}} \leq r < r_{\mathrm{bbb}}$, implying that r_{bbb} is the optimal number of rounds for BBB security. We also point out that if the number of rounds satisfies $r < r_{\mathrm{bb}}$, then there is an efficient attack with $q = 2$ queries, implying that r_{bb} is the optimal number of rounds for birthday-bound security.

Table 1 shows the summary of previous results and our results. Given that TBC-based GFSs use a stronger primitive than PRF-based GFSs, a fair comparison is not possible. Nevertheless, we make the following observations from the table:

- We observe that the n-bit security can be achieved with a finite number of rounds with TBC-based GFSs, in contrast to the cases of classical PRF-based GFSs.
- With respect to SPRP security, the number of rounds needed to achieve BBB security with TBC-based GFSs is lower than or equals the number of rounds needed to achieve birthday-bound security with PRF-based GFSs, although the results in [SGW20] are not optimized for the number of rounds (see the discussion below).

The results on PRF-based GFSs and TBC-based Feistel in [SGW20] make use of the coupling technique [MPR07], and motivated by the observation in [LL18], the result regarding TBC-based Feistel shows that it remains secure provided that $q \ll 2^{2nt/(t+1)}$, where $t \geq 1$ is a parameter that specifies the number of rounds, i.e., for TBC-based Feistel, the number of rounds is $4t + 2$ (see Table 1). The value of q can be larger than 2^n, while our results do not cover the case of q beyond 2^n. The proof technique is useful to obtain a strong security bound at the cost of non-tightness in the number of rounds. That is, TBC-based Feistel has the security bound of $O(q^2/2^{2n})$ with 3 rounds [CDMS10], which corresponds to the security bound of $t = 1$ in [SGW20], i.e., $6 = 4t+2$ rounds from Table 1. The same argument applies to the results of PRF-based GFSs in [SGW20]. This paper focuses on deriving the tight bound with respect to the number of rounds, and we leave the analysis with the coupling technique as an interesting future work.

Related Works. We list related works other than the works mentioned above. There are various constructions of (tweakable) enciphering schemes from TBCs, which can seen as a (tweakable) variable-input-length block cipher. See, e.g., [MI11, ST13, CLMP17, CMN18, BLN18, DN18]. These results generalize the results of [CDMS10] to handle variable length input, to optimize the efficiency (the number of TBC calls), and/or to maintain the provable security bound. We also note that there are various constructions of (tweakable) enciphering schemes from block ciphers, including [NR99, HR03, HR04, Hal04, WFW05, CS06a, CS06b, Sar07, MF07, Sar09, BN15, CDK+18, CEL+21].

Table 1: Summary of previous results and our results. "Model" shows the attack model and "Prim." shows the underlying primitive. "Construction" is a block cipher with dn-bit blocks, except for PRF-based Feistel and TBC-based Feistel which are $2n$-bit block ciphers. In the table, q denotes the number of queries, and in the results of [SGW20], $t \geq 1$ is a parameter that specifies the number of rounds. Only the leading terms are listed and constants are neglected in our security bounds.

Model	Prim.	Construction	Security bound	# of rounds	Reference
PRP	PRF	Type-1 GFS	$O(dq^2/2^n)$	$2d-1$	[ZMI89]
		Type-2 GFS	$O(d^2q^2/2^n)$	$d+1$	
		Type-3 GFS	$O(d^2q^2/2^n)$	$d+1$	
SPRP	PRF	Type-2 GFS	birthday	$d+2$	
SPRP	PRF	Type-1 GFS	$\frac{2q}{t+1}\left(\frac{2d^2q}{2^n}\right)^t$	$(d^2+d-2)t+1$	[SGW20]
		Type-2 GFS	$\frac{2q}{t+1}\left(\frac{2d^2q}{2^n}\right)^t$	$2dt+1$	
		Type-3 GFS	$\frac{2q}{t+1}\left(\frac{4d^2q}{2^n}\right)^t$	$(d+2)t+1$	
SPRP	PRF	Feistel	$O(q^2/2^n)$	4	[LR88]
	TBC	Feistel	$O(q^2/2^{2n})$	3	[CDMS10]
			$2\left(\frac{2q}{t+1}\left(\frac{30q}{2^{2n}}\right)^t\right)^{1/2}$	$4t+2$	[SGW20]
PRP	TBC	Type-1 GFS	$dq^2/2^n$ $d^2q^2/2^{2n}$	$2d-2$ $3d-2$	Theorem 1
SPRP	TBC	Type-1 GFS	$d^2q^2/2^n$ $d^3q^2/2^{2n}$	d^2-2d+2 d^2-d+2	Theorem 2
		Type-2 GFS	$d^2q^2/2^n$ $d^3q^2/2^{2n}$	d $d+2$	Theorem 3
		Type-3 GFS	$d^2q^2/2^n$ $d^3q^2/2^{2n}$	d $d+1$	Corollary 1

The constructions we consider in this paper have iterative structures, are not flexible in terms of the input length, are not optimized in terms of the number of TBC calls, and do not take a tweak as input. Our focus is to show the soundness of the structures that are naturally formalized from well known PRF-based GFSs, rather than proposing dedicated designs, and the constructions in this paper could be instantiated with existing TBCs or could be a starting point of designing a block cipher with a large block length as a primitive.

2 Preliminaries

2.1 Notation

For a finite set $\mathcal{S}$, $s \xleftarrow{\$} \mathcal{S}$ denotes the procedure of selecting an element from $\mathcal{S}$ uniformly at random, and assigning it to s. The set of all the bit strings of n bits is written as $\{0,1\}^n$, and for a bit string X, $|X|$ denotes its length in bits. The difference $X_i \oplus X_j$ of two bit strings X_i and X_j with $|X_i| = |X_j|$ is written as $\Delta X_{i,j}$, where $\oplus$ is the XOR operation.

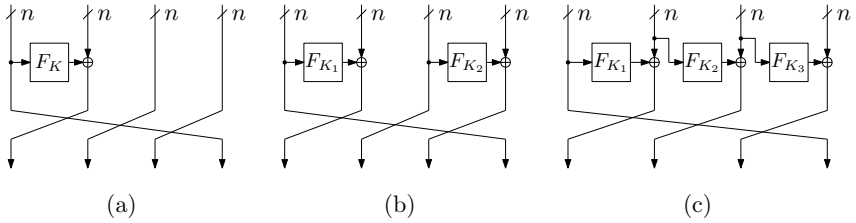

Figure 1: Round functions of classical PRF-based GFSs. (a) Type-1 (b) Type-2 (c) Type-3

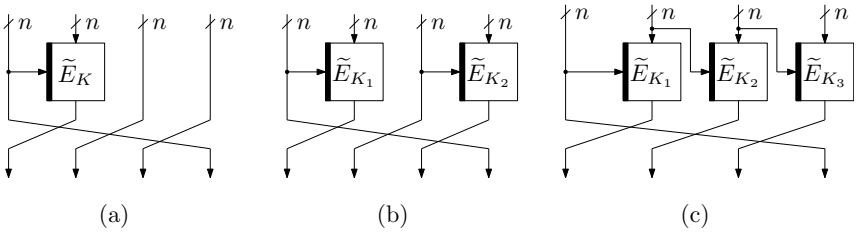

Figure 2: Round functions of TBC-based GFSs. (a) Type-1 (b) Type-2 (c) Type-3

We write the concatenation of bit strings X and Y as $X \| Y$.

For integers a, b, c with $a \le b$ and $c \ge 1$, we let $[a..b : c] = \{a + \ell c \mid a \le a + \ell c \le b \wedge \ell = 0, 1, \ldots\}$, e.g., $[3..10 : 2] = \{3, 5, 7, 9\}$. We use the convention that $[a..b : c] = \emptyset$ if $a > b$. If $c = 1$, we simply write $[a..b] = \{a, a+1, \ldots, b\}$ for $[a..b : c]$. For bit strings $X^a, X^{a+1}, \ldots, X^b$ with $X^i \in \{0,1\}^n$, if $[a..b : c] \neq \emptyset$, then the concatenation of all X^i with $i \in [a..b : c]$ is written as $X^{[a..b:c]}$. That is, we have $X^{[a..b:c]} = X^a \| X^{a+c} \| X^{a+2c} \| \cdots \| X^{a+\lfloor \frac{b-a}{c} \rfloor c}$ and $X^{[a..b]} = X^a \| X^{a+1} \| \cdots \| X^b$. We write the concatenation of X^a and X^b as $X^a \| X^b$ or $X^{[a,b]}$. For example, for $X^{[1..12]} = X^1 \| X^2 \| \cdots \| X^{12}$, we have $X^{[3..10:2]} = X^3 \| X^5 \| X^7 \| X^9$, $X^{[3..10]} = X^3 \| X^4 \| \cdots \| X^{10}$, and $X^{[3,10]} = X^3 \| X^{10}$.

For a keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, where $\mathcal{K}$ is the key space, $\mathcal{X}$ is the input space, and $\mathcal{Y}$ is the output space, the output $Y \in \mathcal{Y}$ for a key $K \in \mathcal{K}$ and an input $X \in \mathcal{X}$ is written as $Y = F_K(X)$ or $Y = F[K](X)$. For a key $K \in \mathcal{K}$, if $F_K(\cdot)$ is a permutation over $\mathcal{X}$, its inverse permutation is written as $F_K^{-1}(\cdot)$ or $F^{-1}[K](\cdot)$.

2.2 Block Ciphers and Tweakable Block Ciphers

A block cipher (BC) is a keyed permutation $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, where for any key $K \in \mathcal{K}$, $E_K(\cdot)$ is a permutation over $\{0,1\}^n$. Here, $\mathcal{K}$ is the key space and n is the block length. If $C \in \{0,1\}^n$ is a ciphertext for a key $K \in \mathcal{K}$ and a plaintext $M \in \{0,1\}^n$, we have $C = E_K(M)$ in encryption and $M = E_K^{-1}(C)$ in decryption. In what follows, we write n-BC for a block cipher with the block length of n bits.

A tweakable block cipher (TBC) [LRW02, LRW11] is a keyed permutation $\widetilde{E} : \mathcal{K} \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ that has an additional input called a tweak. For any key $K \in \mathcal{K}$ and any tweak $T \in \{0,1\}^t$, $\widetilde{E}_K(T, \cdot)$ is a permutation over $\{0,1\}^n$. Here, $\mathcal{K}$ is the key space, t is the tweak length, and n is the block length. If $C \in \{0,1\}^n$ is a ciphertext for a key $K \in \mathcal{K}$, a tweak $T \in \{0,1\}^t$, and a plaintext $M \in \{0,1\}^n$, then we have $C = \widetilde{E}_K(T, M)$ in encryption and $M = \widetilde{E}_K^{-1}(T, C)$ in decryption. We write (t, n)-TBC for a TBC with the tweak length of t bits and the block length of n bits.

We write $\mathrm{Perm}(n)$ for the set of all the permutations over $\{0,1\}^n$. A random permutation π is a permutation that is chosen uniformly at random from $\mathrm{Perm}(n)$, i.e., $\pi \xleftarrow{\$} \mathrm{Perm}(n)$. We write $\widetilde{\mathrm{Perm}}(t, n)$ for the set of all the functions $\widetilde{P} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ such that, for any tweak $T \in \{0,1\}^t$, $\widetilde{P}(T, \cdot) \in \mathrm{Perm}(n)$. A (t, n)-tweakable random permu-

tation ((t,n)-TRP) $\widetilde{P}$ is a function that is chosen uniformly at random from $\widetilde{\mathrm{Perm}}(t,n)$, i.e., $\widetilde{P}$ is a (t,n)-TRP if $\widetilde{P} \xleftarrow{\$} \widetilde{\mathrm{Perm}}(t,n)$. For a (t,n)-TRP $\widetilde{P}$, for any tweak $T \in \{0,1\}^t$, $\widetilde{P}(T,\cdot)$ is a random permutation over $\{0,1\}^n$, and we write $\widetilde{P}^{-1}(T,\cdot)$ for its inverse permutation.

2.3 Security Definitions and Coefficient-H Technique

In this paper, we consider the security of a block cipher E as a pseudorandom permutation (PRP) and a strong PRP (SPRP) [LR88]. A PRP-adversary $\mathcal{A}$ is given oracle access to an encryption oracle $E_K(\cdot)$ in the real world, and it is given oracle access to a random permutation $\pi(\cdot)$ in the ideal world. An SPRP-adversary $\mathcal{A}$ is given oracle access to $E_K(\cdot)$ and $E_K^{-1}(\cdot)$ in the real world, and it is given oracle access to $\pi(\cdot)$ and $\pi^{-1}(\cdot)$ in the ideal world. We define PRP-advantage and SPRP-advantage as follows [LR88]:

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

The probabilities are taken over the randomness of $\mathcal{A}$, K, and π. An adversary $\mathcal{A}$ in the PRP notion is in a chosen-plaintext-attack (CPA) setting, and we may call it a CPA-adversary or a PRP-adversary. An adversary $\mathcal{A}$ in the SPRP notion is in a chosen-plaintext-ciphertext-attack (CPCA) setting, and we may call it a CPCA-adversary or an SPRP-adversary. We also consider a CCA-adversary that has oracle access to decryption ($E_K^{-1}(\cdot)$ or $\pi^{-1}(\cdot)$) only.

In our security proofs, we heavily make use of Coefficient-H technique [Pat08, CS14]. Let $\mathcal{R}$ be the real world oracle defined by a block cipher E, and let $\mathcal{I}$ be the ideal world oracle defined by a random permutation π. For an adversary $\mathcal{A}$ that makes at most q queries, a transcript θ records the interaction between $\mathcal{A}$ and the oracle(s), i.e., it contains all the queries of $\mathcal{A}$ and responses from the oracle(s). Let $\Theta_{\mathcal{R}}$ be the probability distribution of transcript θ when $\mathcal{A}$ interacts with $\mathcal{R}$ (and $\mathcal{R}^{-1}$) in the real world, and $\Theta_{\mathcal{I}}$ be the probability distribution of θ when $\mathcal{A}$ interacts with $\mathcal{I}$ (and $\mathcal{I}^{-1}$) in the ideal world. An attainable transcript is a transcript θ that satisfies $\Pr[\Theta_{\mathcal{I}} = \theta] > 0$, i.e., it has a non-zero probability in the ideal world. Let $\mathsf{T}_{\mathrm{all}}$ be the set of all the attainable transcripts.

With the notation above, Coefficient-H Technique is the following lemma.

Lemma 1 (Coefficient-H Technique [Pat08, CS14])**.** *Consider a deterministic adversary $\mathcal{A}$. Let $\mathsf{T}_{\mathrm{bad}}$ be a subset of $\mathsf{T}_{\mathrm{all}}$ that contains all the "bad" transcripts, and let $\mathsf{T}_{\mathrm{good}} = \mathsf{T}_{\mathrm{all}} \backslash \mathsf{T}_{\mathrm{bad}}$. Assume that there exists $0 \le \epsilon \le 1$ such that*

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \ge 1 - \epsilon$$

holds for all $\theta \in \mathsf{T}_{\mathrm{good}}$. Then, one has $\mathbf{Adv}_E^{(\mathrm{model})}(\mathcal{A}) \le \epsilon + \Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}]$, where $(\mathrm{model}) \in \{\mathrm{prp}, \mathrm{sprp}\}$ depending on the queries $\mathcal{A}$ makes.

3 Definition of TBC-based GFSs

In this section, we formalize TBC-based type-1, type-2, and type-3 GFSs. They are naturally obtained from classical PRF-based type-1, type-2, and type-3 GFSs by using an (n,n)-TBC to define a round function. By iterating the round function for r times, we obtain a dn-BC, where r is the number of rounds and d is the number of input/output blocks. For $\tau \in \{1,2,3\}$, the encryption round function, the decryption round function, the r-round encryption function, and the r-round decryption function of TBC-based type-τ GFS is written as $\Phi_{\tau,d}$, $\Phi_{\tau,d}^{-1}$, $\mathcal{E}_{\tau,d,r}$, and $\mathcal{E}_{\tau,d,r}^{-1}$, respectively, which are defined as follows.

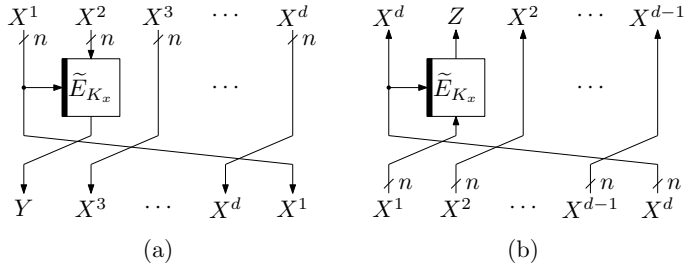

Figure 3: (a) $\Phi_{1,d}[\widetilde{E}_{K_x}](X^1 \,\|\, \cdots \,\|\, X^d) = (Y \,\|\, X^3 \,\|\, \cdots \,\|\, X^d \,\|\, X^1)$, where $Y = \widetilde{E}_{K_x}(X^1, X^2)$. (b) $\Phi^{-1}_{1,d}[\widetilde{E}_{K_x}](X^1 \,\|\, \cdots \,\|\, X^d) = (X^d \,\|\, Z \,\|\, X^2 \,\|\, \cdots \,\|\, X^{d-1})$, where $Z = \widetilde{E}^{-1}_{K_x}(X^d, X^1)$.

TBC-based Type-1 GFS. Let $d \geq 3$, $r \geq 1$, $\widetilde{E}$ be an (n,n)-TBC, and $K_1, \ldots, K_r$ be r independent keys of $\widetilde{E}$. We first define the encryption round function $\Phi_{1,d}$ of a TBC-based type-1 GFS. It is a permutation over $\{0,1\}^{dn}$ that takes $(X^1 \,\|\, \cdots \,\|\, X^d) \in \{0,1\}^{dn}$ as input. It internally makes use of a single call of $\widetilde{E}_{K_x}$, where $x \in \{1, \ldots, r\}$. Now $\Phi_{1,d}$ is defined as

$$\Phi_{1,d}[\widetilde{E}_{K_x}](X^1 \,\|\, \cdots \,\|\, X^d) = (\widetilde{E}_{K_x}(X^1, X^2) \,\|\, X^3 \,\|\, \cdots \,\|\, X^d \,\|\, X^1)\,.$$

The decryption round function $\Phi^{-1}_{1,d}$ is similarly defined by using the decryption function $\widetilde{E}^{-1}_{K_x}$ of $\widetilde{E}_{K_x}$ as

$$\Phi^{-1}_{1,d}[\widetilde{E}_{K_x}](X^1 \,\|\, \cdots \,\|\, X^d) = (X^d \,\|\, \widetilde{E}^{-1}_{K_x}(X^d, X^1) \,\|\, X^2 \,\|\, \cdots \,\|\, X^{d-1})\,.$$

See Fig. 3 for illustrations.

We next define the r-round encryption function $\mathcal{E}_{1,d,r}$ of a TBC-based type-1 GFS. It takes $M \in \{0,1\}^{dn}$ as input, and applies the encryption round function $\Phi_{1,d}[\widetilde{E}_{K_x}]$ with $x = 1, 2, \ldots, r$ in this order. That is, $\mathcal{E}_{1,d,r}$ is defined as

$$\mathcal{E}_{1,d,r}[\widetilde{E}_{K_1}, \ldots, \widetilde{E}_{K_r}](M) = \Phi_{1,d}[\widetilde{E}_{K_r}] \circ \Phi_{1,d}[\widetilde{E}_{K_{r-1}}] \circ \cdots \circ \Phi_{1,d}[\widetilde{E}_{K_1}](M)\,.$$

The r-round decryption function $\mathcal{E}^{-1}_{1,d,r}$ takes $C \in \{0,1\}^{dn}$ as input and applies $\Phi^{-1}_{1,d}[\widetilde{E}_{K_x}]$ with $x = r, r-1, \ldots, 1$. Formally, $\mathcal{E}^{-1}_{1,d,r}$ is defined as

$$\mathcal{E}^{-1}_{1,d,r}[\widetilde{E}_{K_1}, \ldots, \widetilde{E}_{K_r}](C) = \Phi^{-1}_{1,d}[\widetilde{E}_{K_1}] \circ \Phi^{-1}_{1,d}[\widetilde{E}_{K_2}] \circ \cdots \circ \Phi^{-1}_{1,d}[\widetilde{E}_{K_r}](C)\,.$$

In the proof of security presented in Sect. 4 and Sect. 5, we consider $\mathcal{E}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$ and $\mathcal{E}^{-1}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$ that are obtained by replacing each (n,n)-TBC $\widetilde{E}_{K_x}$ with an (n,n)-TRP $\widetilde{P}_x$, where $\widetilde{P}_1, \ldots, \widetilde{P}_r$ are r independent (n,n)-TRPs. In what follows, if it is clear from the context, we write $\mathcal{E}_{1,d,r}$ for $\mathcal{E}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$ and $\mathcal{E}^{-1}_{1,d,r}$ for $\mathcal{E}^{-1}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$.

TBC-based Type-2 GFS. Let $d \geq 4$ and $r \geq 1$, where d is even. We let $K_{1,1}, \ldots, K_{r,d/2}$ be $rd/2$ independent keys for (n,n)-TBC $\widetilde{E}$ used in the construction. The encryption round function $\Phi_{2,d}$ of a TBC-based type-2 GFS is a permutation over $\{0,1\}^{dn}$ that takes $(X^1 \,\|\, \cdots \,\|\, X^d) \in \{0,1\}^{dn}$ as input. Internally, $\Phi_{2,d}$ uses $d/2$ TBCs $\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}$, where $x \in \{1, \ldots, r\}$, and is defined as

$$\begin{aligned}&\Phi_{2,d}[\widetilde{E}_{K_{x,1}}, \widetilde{E}_{K_{x,2}}, \ldots, \widetilde{E}_{K_{x,d/2}}](X^1 \,\|\, \cdots \,\|\, X^d)\\ &\quad = (\widetilde{E}_{K_{x,1}}(X^1, X^2) \,\|\, X^3 \,\|\, \widetilde{E}_{K_{x,2}}(X^3, X^4) \,\|\, X^5 \,\|\, \cdots \,\|\, \widetilde{E}_{K_{x,d/2}}(X^{d-1}, X^d) \,\|\, X^1)\,.\end{aligned}$$

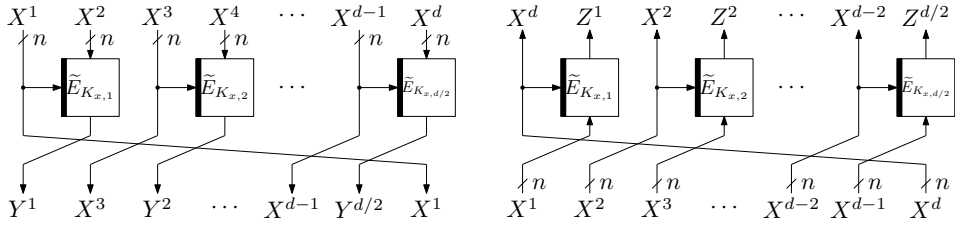

Figure 4: (a) $\Phi_{2,d}[\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}](X^1 \| \cdots \| X^d) = (Y^1 \| X^3 \| Y^2 \| \cdots \| X^{d-1} \| Y^{d/2} \| X^1)$, where $Y^\ell = \widetilde{E}_{K_{x,\ell}}(X^{2\ell-1}, X^{2\ell})$. (b) $\Phi_{2,d}^{-1}[\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}](X^1 \,\|\, \cdots \,\|\, X^d) = (X^d \,\|\, Z^1 \,\|\, X^2 \,\|\, Z^2 \,\|\, \cdots \,\|\, X^{d-2} \,\|\, Z^{d/2})$, where $Z^1 = \widetilde{E}_{K_{x,1}}^{-1}(X^d, X^1)$ and $Z^\ell = \widetilde{E}_{K_{x,\ell}}^{-1}(X^{2(\ell-1)}, X^{2\ell-1})$ for $\ell \in \{2, \ldots, d/2\}$.

The decryption round function $\Phi_{2,d}^{-1}$ uses decryption $\widetilde{E}_{K_{x,1}}^{-1}, \ldots, \widetilde{E}_{K_{x,d/2}}^{-1}$ of $\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}$ and is defined as

$$\begin{aligned}&\Phi_{2,d}^{-1}[\widetilde{E}_{K_{x,1}}, \widetilde{E}_{K_{x,2}}, \ldots, \widetilde{E}_{K_{x,d/2}}](X^1 \,\|\, \cdots \,\|\, X^d)\\ &\quad = (X^d \,\|\, \widetilde{E}_{K_{x,1}}^{-1}(X^d, X^1) \,\|\, X^2 \,\|\, \widetilde{E}_{K_{x,2}}^{-1}(X^2, X^3) \,\|\, \cdots \,\|\, X^{d-2} \,\|\, \widetilde{E}_{K_{x,d/2}}^{-1}(X^{d-2}, X^{d-1}))\,.\end{aligned}$$

See Fig. 4.

The r-round encryption function $\mathcal{E}_{2,d,r}$ of a TBC-based type-2 GFS is a dn-BC that takes $M \in \{0,1\}^{dn}$ as input. It uses r encryption round functions $\Phi_{2,d}[\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}]$ for $x = 1, 2, \ldots, r$, and is defined as

$$\begin{aligned}&\mathcal{E}_{2,d,r}[\widetilde{E}_{K_{1,1}}, \ldots, \widetilde{E}_{K_{r,d/2}}](M)\\ &= \Phi_{2,d}[\widetilde{E}_{K_{r,1}}, \ldots, \widetilde{E}_{K_{r,d/2}}] \circ \Phi_{2,d}[\widetilde{E}_{K_{r-1,1}}, \ldots, \widetilde{E}_{K_{r-1,d/2}}] \circ \cdots \circ \Phi_{2,d}[\widetilde{E}_{K_{1,1}}, \ldots, \widetilde{E}_{K_{1,d/2}}](M)\,.\end{aligned}$$

The r-round decryption function $\mathcal{E}_{2,d,r}^{-1}$ is defined in an obvious way by using r decryption round functions $\Phi_{2,d}^{-1}[\widetilde{E}_{K_{x,1}}, \ldots, \widetilde{E}_{K_{x,d/2}}]$ for $x = r, r-1, \ldots, 1$ as

$$\begin{aligned}&\mathcal{E}_{2,d,r}^{-1}[\widetilde{E}_{K_{1,1}}, \ldots, \widetilde{E}_{K_{r,d/2}}](C)\\ &= \Phi_{2,d}^{-1}[\widetilde{E}_{K_{1,1}}, \ldots, \widetilde{E}_{K_{1,d/2}}] \circ \Phi_{2,d}^{-1}[\widetilde{E}_{K_{2,1}}, \ldots, \widetilde{E}_{K_{2,d/2}}] \circ \cdots \circ \Phi_{2,d}^{-1}[\widetilde{E}_{K_{r,1}}, \ldots, \widetilde{E}_{K_{r,d/2}}](C)\,,\end{aligned}$$

where $C \in \{0,1\}^{dn}$ is the input.

In Sect. 6, we prove the security of $\mathcal{E}_{2,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}]$, where $\widetilde{P}_{x,y}$ is used as a TBC $\widetilde{E}_{K_{x,y}}$ and $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}$ are $rd/2$ independent (n,n)-TRPs. We write $\mathcal{E}_{2,d,r}$ for $\mathcal{E}_{2,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}]$ and $\mathcal{E}_{2,d,r}^{-1}$ for $\mathcal{E}_{2,d,r}^{-1}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}]$.

TBC-based Type-3 GFS. Let $d \geq 3$, $r \geq 1$, $\widetilde{E}$ be an (n,n)-TBC, and $K_{1,1}, \ldots, K_{r,d-1}$ be $r(d-1)$ independent keys of $\widetilde{E}$. The encryption round function $\Phi_{3,d}$ of a TBC-based type-3 GFS is a permutation over $\{0,1\}^{dn}$, internally uses $d-1$ independent (n,n)-TBCs $\widetilde{E}_{K_{x,1}}$, $\ldots, \widetilde{E}_{K_{x,d-1}}$ for some $x \in \{1, \ldots, r\}$, and takes $(X^1 \,\|\, \cdots \,\|\, X^d) \in \{0,1\}^{dn}$ as input. It is defined as

$$\begin{aligned}&\Phi_{3,d}[\widetilde{E}_{K_{x,1}}, \widetilde{E}_{K_{x,2}}, \ldots, \widetilde{E}_{K_{x,d-1}}](X^1 \,\|\, \cdots \,\|\, X^d)\\ &\quad = (\widetilde{E}_{K_{x,1}}(X^1, X^2) \,\|\, \widetilde{E}_{K_{x,2}}(X^2, X^3) \,\|\, \cdots \,\|\, \widetilde{E}_{K_{x,d-1}}(X^{d-1}, X^d) \,\|\, X^1)\,.\end{aligned}$$

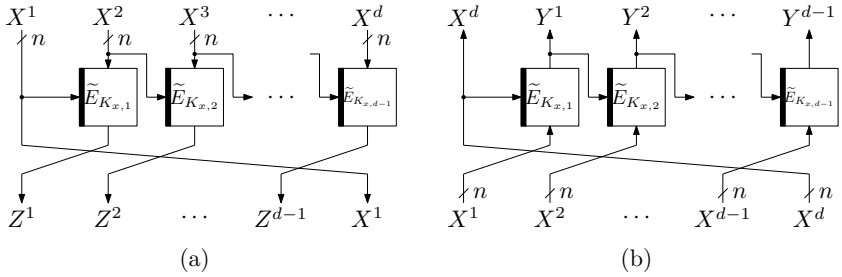

Figure 5: (a) $\Phi_{3,d}[\widetilde{E}_{K_{x,1}},\ldots,\widetilde{E}_{K_{x,d-1}}](X^1\|\cdots\|X^d) = (Z^1\|Z^2\|\cdots\|Z^{d-1}\|X^1)$, where $Z^\ell = \widetilde{E}_{K_{x,\ell}}(X^\ell, X^{\ell+1})$. (b) $\Phi^{-1}_{3,d}[\widetilde{E}_{K_{x,1}},\ldots,\widetilde{E}_{K_{x,d-1}}](X^1\,\|\cdots\|\,X^d) = (X^d\,\|\,Y^1\,\|\,Y^2\,\|\cdots\|\,Y^{d-1})$.

The decryption round function $\Phi^{-1}_{3,d}$ uses decryption $\widetilde{E}^{-1}_{K_{x,1}},\ldots,\widetilde{E}^{-1}_{K_{x,d-1}}$ of $\widetilde{E}_{K_{x,1}},\ldots,\widetilde{E}_{K_{x,d-1}}$ and is defined as

$$\Phi^{-1}_{3,d}[\widetilde{E}_{K_{x,1}},\widetilde{E}_{K_{x,2}},\ldots,\widetilde{E}_{K_{x,d-1}}](X^1\,\|\cdots\|\,X^d) = (X^d\,\|\,Y^1\,\|\,Y^2\,\|\cdots\|\,Y^{d-1})\,,$$

where $Y^1 = \widetilde{E}^{-1}_{K_{x,1}}(X^d, X^1)$ and $Y^\ell = \widetilde{E}^{-1}_{K_{x,\ell}}(Y^{\ell-1}, X^\ell)$ for $\ell \in \{2,\ldots,d-1\}$. See Fig. 5.

The r-round encryption function $\mathcal{E}_{3,d,r}$ of a TBC-based type-3 GFS is a dn-BC that takes $M \in \{0,1\}^{dn}$ as input, uses r encryption round functions $\Phi_{3,d}[\widetilde{E}_{K_{x,1}},\ldots,\widetilde{E}_{K_{x,d-1}}]$ for $x = 1,2,\ldots,r$, and is defined as

$$\begin{aligned}&\mathcal{E}_{3,d,r}[\widetilde{E}_{K_{1,1}},\ldots,\widetilde{E}_{K_{r,d-1}}](M)\\ &= \Phi_{3,d}[\widetilde{E}_{K_{r,1}},\ldots,\widetilde{E}_{K_{r,d-1}}]\circ\Phi_{3,d}[\widetilde{E}_{K_{r-1,1}},\ldots,\widetilde{E}_{K_{r-1,d-1}}]\circ\cdots\circ\Phi_{3,d}[\widetilde{E}_{K_{1,1}},\ldots,\widetilde{E}_{K_{1,d-1}}](M)\,.\end{aligned}$$

The r-round decryption function $\mathcal{E}^{-1}_{3,d,r}$ of TBC-based type-3 GFS takes $C \in \{0,1\}^{dn}$ as input, uses r decryption round functions $\Phi^{-1}_{3,d}[\widetilde{E}_{K_{x,1}},\ldots,\widetilde{E}_{K_{x,d-1}}]$ for $x = r, r-1,\ldots,1$, and is defined as

$$\begin{aligned}&\mathcal{E}^{-1}_{3,d,r}[\widetilde{E}_{K_{1,1}},\ldots,\widetilde{E}_{K_{r,d-1}}](C)\\ &= \Phi^{-1}_{3,d}[\widetilde{E}_{K_{1,1}},\ldots,\widetilde{E}_{K_{1,d-1}}]\circ\Phi^{-1}_{3,d}[\widetilde{E}_{K_{2,1}},\ldots,\widetilde{E}_{K_{2,d-1}}]\circ\cdots\circ\Phi^{-1}_{3,d}[\widetilde{E}_{K_{r,1}},\ldots,\widetilde{E}_{K_{r,d-1}}](C)\,.\end{aligned}$$

We prove the security of $\mathcal{E}_{3,d,r}[\widetilde{P}_{1,1},\ldots,\widetilde{P}_{r,d-1}]$ in Sect. 7, where we use $\widetilde{P}_{x,y}$ instead of $\widetilde{E}_{K_{x,y}}$ and $\widetilde{P}_{1,1},\ldots,\widetilde{P}_{r,d-1}$ are $r(d-1)$ independent (n,n)-TRPs. We write $\mathcal{E}_{3,d,r}$ for $\mathcal{E}_{3,d,r}[\widetilde{P}_{1,1},\ldots,\widetilde{P}_{r,d-1}]$ and $\mathcal{E}^{-1}_{3,d,r}$ for $\mathcal{E}^{-1}_{3,d,r}[\widetilde{P}_{1,1},\ldots,\widetilde{P}_{r,d-1}]$.

4 PRP Security of TBC-based Type-1 GFS

In this section, we prove PRP security of $\mathcal{E}_{1,d,r}$, TBC-based type-1 GFS, where we use r independent (n,n)-TRPs.

Theorem 1 (TBC-based type-1 GFS, PRP security)**.** *Fix $d \geq 3$, and let $\widetilde{P}_1,\ldots,\widetilde{P}_r$ be r independent (n,n)-TRPs and $E = \mathcal{E}_{1,d,r}[\widetilde{P}_1,\ldots,\widetilde{P}_r]$ be the TBC-based type-1 GFS. Then for any PRP-adversary $\mathcal{A}$ that makes q queries, if $r = 2d-2$ rounds, we have*

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \leq \frac{(d-1)q^2}{2^n} + \frac{0.5(d-1)q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,, \tag{1}$$

and if $r = 3d-2$ rounds, we have

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \leq \frac{0.25(3d^2-d-4)q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,. \tag{2}$$

In Theorem 1, Eq. (1) shows birthday-bound security and Eq. (2) shows BBB security. The birthday-bound security is obtained from Lemma 3, Lemma 6, and the Coefficient-H technique (Lemma 1), and the BBB security is obtained from Lemma 5, Lemma 6, and the Coefficient-H technique (Lemma 1).

Below, we present the proof of Theorem 1. Both Eq. (1) and Eq. (2) consider CPA security, with the difference being in the number of rounds. They share the same definition of the oracles (Sect. 4.1) and the interpolation probability (Sect. 4.3), while the computation of the probability of bad events (Sect. 4.2) requires different treatments, which are presented in Sect. 4.2.1 for $r = 2d - 2$ and in Sect. 4.2.2 for $r = 3d - 2$.

We consider a CPA-adversary $\mathcal{A}$ that interacts with the real world oracle $\mathcal{R}$, or with the ideal world oracle $\mathcal{I}$. Without loss of generality, $\mathcal{A}$ is assumed to be deterministic, makes exactly q queries, and does not repeat the same query.

4.1 Definition of the Oracles

The real world oracle $\mathcal{R}$ is defined as $\mathcal{E}_{1,d,r}$ that uses r independent TRPs $\widetilde{P}_1, \ldots, \widetilde{P}_r$. In $\mathcal{R}$, for the i-th query, we compute the internal states $S_i^1, \ldots, S_i^{r-d}$ with $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$, and the ciphertext with $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$. For each query $\mathcal{A}$ makes, we record the internal states $S_i^1, \ldots, S_i^{r-d}$ in S, and the entire history of the internal states S is given to $\mathcal{A}$ after it makes q queries and before it outputs its decision bit. This only benefits $\mathcal{A}$ to increase its advantage, and we show Eq. (1) and Eq. (2) with this $\mathcal{A}$ that has the extra information of S. The real world oracle $\mathcal{R}$ is presented in Algorithm 1 in Fig. 6. See Fig. 7 for an example and the labeling convention.

The ideal world oracle $\mathcal{I}$ is defined as the dn-bit random permutation π. In $\mathcal{I}$, for the i-th query, we use $r - d$ dummy TRPs $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$ to compute dummy internal states $S_i^1, \ldots, S_i^{r-d}$, and record them into S. The dummy internal states have the same probability distribution as in the real world oracle, and S is given to $\mathcal{A}$ after it makes q queries. The ideal world oracle $\mathcal{I}$ is given in Algorithm 2 in Fig. 6.

4.2 Bad Transcript and Bad Probability

The adversary $\mathcal{A}$ is given all the internal states after it makes q queries. The interaction between the oracle and $\mathcal{A}$ can be summarized as a transcript θ as

$$\theta = \left((M_1^{[1..d]}, C_1^{[1..d]}, S_1^{[1..r-d]}), \ldots, (M_q^{[1..d]}, C_q^{[1..d]}, S_q^{[1..r-d]})\right) .$$

Since we assume that $\mathcal{A}$ does not repeat a query, for any $1 \le j < i \le q$, we have $(M_i^1, \ldots, M_i^d) \neq (M_j^1, \ldots, M_j^d)$ and $(C_i^1, \ldots, C_i^d) \neq (C_j^1, \ldots, C_j^d)$.

In the real world, let us focus on $\widetilde{P}_x$ for some $x \in [1..r]$, and let X_i, T_i, and Y_i be the input, tweak, and output of the i-th query, respectively. We observe that in the i-th and j-th queries, if $X_i = X_j$ and $T_i = T_j$ hold, then we must have $Y_i = Y_j$, and similarly, if we have $Y_i = Y_j$ and $T_i = T_j$, then $X_i = X_j$ holds.

In the ideal world, for $\widetilde{P}_x$ with $x \in [1..r - d]$, i.e., for TPRs that are used in the simulation, it has the same input-tweak-output relation as in the real world. However, for $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$ that are not used in the simulation, this may not be the case. That is, the output can be different even though it takes the same input and tweak, or the input can be different when it takes the same output and tweak. In other words, in the ideal world, TRPs $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$ are not used in the simulation, and there are conditions on these TRPs that can hold only in the ideal world. Our definition of the set of bad transcripts, $\mathsf{T}_{\mathrm{bad}}$, consists of all such transcripts θ.

Algorithm 1: Procedure of $\mathcal{R}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $(S_i^{-d+1}, S_i^{-d+2}, \ldots, S_i^{-1}, S_i^0) \leftarrow (M_i^2, M_i^3, \ldots, M_i^d, M_i^1)$
2. **for** $x = 1, 2, \ldots, r$ **do**
   $S_i^x \leftarrow \widetilde{P}_x(S_i^{x-1}, S_i^{x-d})$
3. $(C_i^1, C_i^2, \ldots, C_i^d) \leftarrow (S_i^r, S_i^{r-d+1}, S_i^{r-d+2}, \ldots, S_i^{r-1})$
4. **return** $C_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Algorithm 2: Procedure of $\mathcal{I}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $C_i^{[1..d]} \leftarrow \pi(M_i^{[1..d]})$
2. $(S_i^{-d+1}, S_i^{-d+2}, \ldots, S_i^{-1}, S_i^0) \leftarrow (M_i^2, M_i^3, \ldots, M_i^d, M_i^1)$
3. **for** $x = 1, 2, \ldots, r-d$ **do**
   $S_i^x \leftarrow \widetilde{P}_x(S_i^{x-1}, S_i^{x-d})$
4. **return** $C_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Figure 6: Definition of $\mathcal{R}$ and $\mathcal{I}$ for the PRP proof of $\mathcal{E}_{1,d,r}$. Initially, S is empty, and S is given to $\mathcal{A}$ after it makes all the q queries.

To define the set of bad transcripts, we let $x \in [2..d]$, and we consider the following bad conditions[1]:

$$\begin{aligned}
\text{Bad at } \widetilde{P}_{r-d+1}: \ & (S_i^{r-2d+1}, S_i^{r-d}) = (S_j^{r-2d+1}, S_j^{r-d}) \wedge C_i^2 \neq C_j^2 \\
& \text{or } (S_i^{r-d}, C_i^2) = (S_j^{r-d}, C_j^2) \wedge S_i^{r-2d+1} \neq S_j^{r-2d+1} \\
\text{Bad at } \widetilde{P}_{r-d+x}: \ & (S_i^{r-2d+x}, C_i^x) = (S_j^{r-2d+x}, C_j^x) \wedge C_i^{x+1} \neq C_j^{x+1} \\
& \text{or } (C_i^x, C_i^{x+1}) = (C_j^x, C_j^{x+1}) \wedge S_i^{r-2d+x} \neq S_j^{r-2d+x}
\end{aligned}$$

Here, when $x = d$, we let $C^{d+1} = C^1$. If $r < 2d$, then a plaintext block (instead of a block of internal state) is involved in the condition, and we let $S^0 = M^1$ and $S^{-1} = M^d$.

Example 1. If $d = 4$ and $r = 2d - 2 = 6$, we have the following bad conditions:

$$\begin{aligned}
\text{Bad at } \widetilde{P}_3: \ & (M_i^4, S_i^2) = (M_j^4, S_j^2) \wedge C_i^2 \neq C_j^2 \quad \text{or} \quad (S_i^2, C_i^2) = (S_j^2, C_j^2) \wedge M_i^4 \neq M_j^4 \\
\text{Bad at } \widetilde{P}_4: \ & (M_i^1, C_i^2) = (M_j^1, C_j^2) \wedge C_i^3 \neq C_j^3 \quad \text{or} \quad (C_i^2, C_i^3) = (C_j^2, C_j^3) \wedge M_i^1 \neq M_j^1 \\
\text{Bad at } \widetilde{P}_5: \ & (S_i^1, C_i^3) = (S_j^1, C_j^3) \wedge C_i^4 \neq C_j^4 \quad \text{or} \quad (C_i^3, C_i^4) = (C_j^3, C_j^4) \wedge S_i^1 \neq S_j^1 \\
\text{Bad at } \widetilde{P}_6: \ & (S_i^2, C_i^4) = (S_j^2, C_j^4) \wedge C_i^1 \neq C_j^1 \quad \text{or} \quad (C_i^1, C_i^4) = (C_j^1, C_j^4) \wedge S_i^2 \neq S_j^2
\end{aligned}$$

These conditions can hold only in the ideal world, and they are impossible in the real world, implying that the interpolation probability of such a transcript in the real world is

[1]We follow the order of (tweak, input) or (tweak, output) to describe two n-bit blocks as an argument of a TBC. To describe bad events, we list them following the order of a plaintext, an internal state, and a ciphertext, with smaller indices come first.

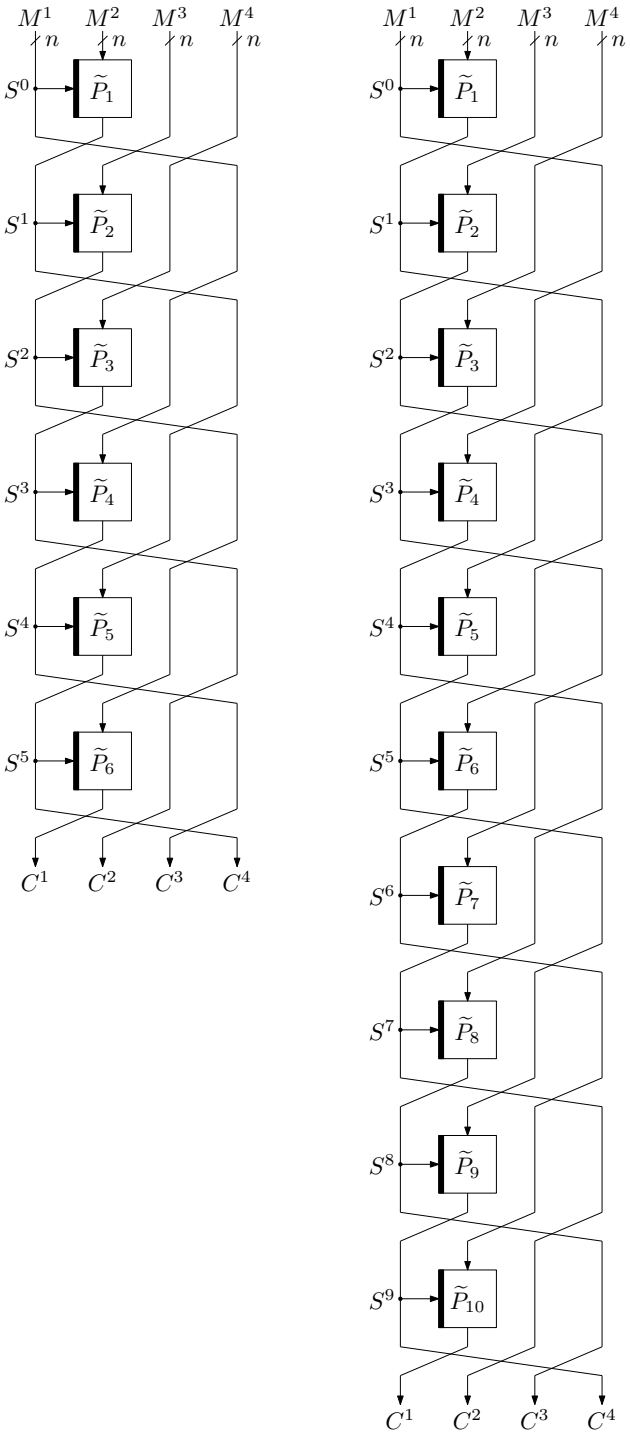

Figure 7: Left: $\mathcal{E}_{1,d,r}(M^1 \parallel \cdots \parallel M^4) = (C^1 \parallel \cdots \parallel C^4)$ for the case $d = 4$ and $r = 6$, where $(M^1 \parallel \cdots \parallel M^4) = (S^0 \parallel S^{-3} \parallel S^{-2} \parallel S^{-1})$ and $(C^1 \parallel \cdots \parallel C^4) = (S^6 \parallel S^3 \parallel S^4 \parallel S^5)$. Right: $\mathcal{E}_{1,d,r}(M^1 \parallel \cdots \parallel M^4) = (C^1 \parallel \cdots \parallel C^4)$ for the case $d = 4$ and $r = 10$, where $(M^1 \parallel \cdots \parallel M^4) = (S^0 \parallel S^{-3} \parallel S^{-2} \parallel S^{-1})$ and $(C^1 \parallel \cdots \parallel C^4) = (S^{10} \parallel S^7 \parallel S^8 \parallel S^9)$.

zero. We define $\mathsf{Bad}^1_{\mathrm{enc}}$ as the set of all these conditions. Here, $1 \le j < i \le q$, and since we have $\binom{q}{2}$ possible combinations of i and j, $\mathsf{Bad}^1_{\mathrm{enc}}$ consists of:

- $1 \times \binom{q}{2}$ conditions of a $2n$-bit collision between two internal state blocks (e.g., $(S_i^{r-2d+1}, S_i^{r-d}) = (S_j^{r-2d+1}, S_j^{r-d})$), which we write $\mathsf{coll}_{\mathrm{s,s}}$,
- $d \times \binom{q}{2}$ conditions of a $2n$-bit collision between one internal state block and one ciphertext block (e.g., $(S_i^{r-d}, C_i^2) = (S_j^{r-d}, C_j^2)$), which we write $\mathsf{coll}_{\mathrm{s,c}}$, and
- $(d-1) \times \binom{q}{2}$ conditions of a $2n$-bit collision between two ciphertext blocks (e.g., $(C_i^x, C_i^{x+1}) = (C_j^x, C_j^{x+1})$), which we write $\mathsf{coll}_{\mathrm{c,c}}$.

In total, we have $2d \times \binom{q}{2}$ possible collisions of $2n$-bit variables in $\mathsf{Bad}^1_{\mathrm{enc}}$.

Example 2. When $d = 4$ and $r = 2d - 2 = 6$, we have $8 \times \binom{q}{2}$ conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$ (See Example 1). In this case, $\mathsf{Bad}^1_{\mathrm{enc}}$ consists of:

- $\mathsf{coll}_{\mathrm{s,s}}$: $1 \times \binom{q}{2}$ collisions at (M^4, S^2)
- $\mathsf{coll}_{\mathrm{s,c}}$: $4 \times \binom{q}{2}$ collisions at (S^2, C^2), (M^1, C^2), (S^1, C^3), and (S^2, C^4)
- $\mathsf{coll}_{\mathrm{c,c}}$: $3 \times \binom{q}{2}$ collisions at (C^2, C^3), (C^3, C^4), and (C^1, C^4)

Now the set of bad transcripts $\mathsf{T}_{\mathrm{bad}}$ is defined as the set of all the attainable transcripts that satisfy at least one of the conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$. Formally, we define

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \theta \text{ satisfies at least one of the conditions in } \mathsf{Bad}^1_{\mathrm{enc}}\}.$$

The set of good transcripts $\mathsf{T}_{\mathrm{good}}$ is defined as the set of all the attainable transcripts θ that are not in $\mathsf{T}_{\mathrm{bad}}$, i.e., we let $\mathsf{T}_{\mathrm{good}} = \mathsf{T}_{\mathrm{all}} \setminus \mathsf{T}_{\mathrm{bad}}$.

In what follows, we evaluate the probability to have bad transcripts. We consider the case $r = 2d - 2$ first, and then $r = 3d - 2$.

4.2.1 Bad Probability for $r = 2d - 2$

Let $r = 2d - 2$. For each of the conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$, we have the following lemma.

Lemma 2. *Let $r = 2d - 2$, and consider one of the $2d \times \binom{q}{2}$ conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$ in the ideal world. Then, the probability of the condition is at most $(d-2)/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $1/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,c}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{c,c}}$.*

Proof. We first present the analysis of $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a condition in $\mathsf{coll}_{\mathrm{s,s}}$, which corresponds to a unique $2n$-bit collision at (S^{r-2d+1}, S^{r-d}). As we are dealing with the case $r = 2d - 2$, it follows that $S^{r-2d+1} = S^{-1} = M^d$ and $S^{r-d} = S^{d-2}$. We focus on the i-th and j-th queries, with $1 \le j < i \le q$, and derive the upper bound on

$$\Pr[S_i^{[r-2d+1,r-d]} = S_j^{[r-2d+1,r-d]} \wedge C_i^2 \neq C_j^2] \le \Pr[(M_i^d, S_i^{d-2}) = (M_j^d, S_j^{d-2})]. \quad (3)$$

For $C_i^2 \neq C_j^2$, we use the trivial bound of $\Pr[C_i^2 \neq C_j^2] \le 1$, as this event does not change the coefficient of the leading term of Eq. (3), and hence we will not consider this event in the following analysis.

Now for each of the conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$, its probability depends on how the plaintexts are chosen by $\mathcal{A}$. Recall that we have $M_i^{[1..d]} \neq M_j^{[1..d]}$, and we write the plaintext difference as $\Delta M_{i,j}^{[1..d]} = M_i^{[1..d]} \oplus M_j^{[1..d]}$. To derive the upper bound on Eq. (3), we proceed as follows:

1. We compute the upper bound on Eq. (3) when the plaintext difference is $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$, and $\Delta M^2_{i,j}$ is an arbitrary difference.
2. We prove that the plaintext difference given above maximizes Eq. (3), by showing that any other plaintext difference does not have a larger upper bound.

We now compute the upper bound on Eq. (3) when $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$. Since $M^1_i \neq M^1_j$, the probability of a collision at $S^1 = \widetilde{P}_1(M^1, M^2)$ is $\Pr[S^1_i = S^1_j] = 1/2^n$, regardless of the difference $\Delta M^2_{i,j}$. Then, since $M^3_i = M^3_j$, the probability of a collision at $S^2 = \widetilde{P}_2(S^1, M^3)$ is at most

$$\begin{aligned}\Pr[S^2_i = S^2_j] &= \Pr[S^1_i = S^1_j] + \Pr[S^1_i \neq S^1_j] \cdot \Pr[S^2_i = S^2_j \mid S^1_i \neq S^1_j] \\ &\leq \Pr[S^1_i = S^1_j] + \frac{1}{2^n} = \frac{2}{2^n}\,.\end{aligned}$$

We continue a similar step relying on $M^{[4..d-1]}_i = M^{[4..d-1]}_j$ to obtain the upper bound on the probability of a collision at $S^x = \widetilde{P}_x(S^{x-1}, M^{x+1})$ for $x \in [3..d-2]$ as follows:

$$\begin{aligned}\Pr[S^3_i = S^3_j] &\leq \Pr[S^2_i = S^2_j] + \frac{1}{2^n} \leq \frac{3}{2^n} \\ \Pr[S^4_i = S^4_j] &\leq \Pr[S^3_i = S^3_j] + \frac{1}{2^n} \leq \frac{4}{2^n} \\ &\vdots \\ \Pr[S^{d-2}_i = S^{d-2}_j] &\leq \Pr[S^{d-3}_i = S^{d-3}_j] + \frac{1}{2^n} \leq \frac{d-2}{2^n}\end{aligned}$$

Therefore, we have

$$\text{Eq. (3)} = \Pr[(M^d_i, S^{d-2}_i) = (M^d_j, S^{d-2}_j)] \leq \Pr[S^{d-2}_i = S^{d-2}_j] \leq \frac{d-2}{2^n}\,,$$

and this gives us an upper bound $(d-2)/2^n$ on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$, and $\Delta M^2_{i,j}$ is an arbitrary difference.

We next prove that this is the upper bound for all other plaintext differences by showing that any plaintext difference other than $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$ does not have a larger upper bound. Observe that the event $(M^d_i, S^{d-2}_i) = (M^d_j, S^{d-2}_j)$ involves $d-2$ TRPs $\widetilde{P}_1, \ldots, \widetilde{P}_{d-2}$, and in the computation of the above, each TRP contributes to the addition of a term $1/2^n$ in the final upper bound. We analyze this in three cases: (C-1) $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} \neq 0$, (C-2) $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0$, and (C-3) $\Delta M^{[1,2]}_{i,j} = 0$. Note that we cover all the cases.

(C-1) Assume that we have $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} \neq 0$, say $\Delta M^x_{i,j} \neq 0$ for some $x \in [3..d]$. If $x = d$, then $\Pr[(M^d_i, S^{d-2}_i) = (M^d_j, S^{d-2}_j)]$ is zero. If $x \in [3..d-1]$, where there may be multiple indices of x, by following the above computation, we do not have the corresponding addition of a term $\Pr[S^{x-2}_i = S^{x-2}_j]$ to derive the upper bound on $\Pr[S^{x-1}_i = S^{x-1}_j]$. That is, we use $\Pr[S^{x-1}_i = S^{x-1}_j] \leq \Pr[S^{x-2}_i = S^{x-2}_j] + 1/2^n$ in the above computation, and the lack of $\Pr[S^{x-2}_i = S^{x-2}_j]$ makes it smaller, implying that the final upper bound would also be smaller.

(C-2) If $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0$, then $\Pr[S^1_i = S^1_j] = 0$, and hence the final bound would be smaller by following the above computation.

(C-3) If $\Delta M_{i,j}^{[1,2]} = 0$, then we must have $\Delta M_{i,j}^{[3..d]} \neq 0$, and assume that $\Delta M_{i,j}^{x} \neq 0$, where $x \in [3..d]$ is the smallest index. Now $\Delta M_{i,j}^{x} \neq 0$ comes at the leftmost position at the input of the x-th round, and we are back to the analysis of the initial case of $\Delta M_{i,j}^{1} \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ with a reduced round version, which cannot have a larger collision probability.

Therefore, the plaintext difference $\Delta M_{i,j}^{1} \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ maximizes Eq. (3), and the corresponding upper bound $(d-2)/2^n$ is the upper bound for all the cases in $\mathsf{coll}_{\mathrm{s,s}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. Next, we consider a condition in $\mathsf{coll}_{\mathrm{s,c}}$. Among the $d \times \binom{q}{2}$ conditions in $\mathsf{coll}_{\mathrm{s,c}}$ of $\mathsf{Bad}_{\mathrm{enc}}^{1}$, we focus on the analysis of (S^{r-2d+2}, C^2) that involves the internal state with the smallest index in the number of round, as other cases of $\mathsf{coll}_{\mathrm{s,c}}$ cannot have a larger upper bound. When $r = 2d-2$, we have $S^{r-2d+2} = S^0 = M^1$, and we therefore consider

$$\Pr[(S_i^{r-2d+2}, C_i^2) = (S_j^{r-2d+2}, C_j^2) \wedge C_i^3 \neq C_j^3] \leq \Pr[(M_i^1, C_i^2) = (M_j^1, C_j^2)]\,. \tag{4}$$

It is clear that Eq. (4) is maximized when $\Delta M_{i,j}^{1} = 0$. In the ideal world, a ciphertext is obtained as the output of the dn-bit random permutation π. This implies that regardless of the plaintext difference, for any $a \in [1..d]$, we have

$$\Pr[C_i^a = C_j^a] = \frac{2^{(d-1)n} - 1}{2^{dn} - 1} \leq \frac{2^{(d-1)n} - 1}{2^{dn} - 2^n} = \frac{1}{2^n}\,. \tag{5}$$

We thus have

$$\text{Eq. (4)} = \Pr[(M_i^1, C_i^2) = (M_j^1, C_j^2)] \leq \Pr[C_i^2 = C_j^2] \leq \frac{1}{2^n}\,,$$

and this gives us the upper bound $1/2^n$ for the conditions in $\mathsf{coll}_{\mathrm{s,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider $\mathsf{coll}_{\mathrm{c,c}}$. Since ciphertexts are generated with π, regardless of the plaintext difference, for any $a, b \in [1..d], a \neq b$, we have

$$\Pr[(C_i^a, C_i^b) = (C_j^a, C_j^b)] = \frac{2^{(d-2)n} - 1}{2^{dn} - 1} \leq \frac{2^{(d-2)n} - 1}{2^{dn} - 2^{2n}} = \frac{1}{2^{2n}}\,. \tag{6}$$

Therefore, $1/2^{2n}$ is the upper bound for all the conditions in $\mathsf{coll}_{\mathrm{c,c}}$, and this completes the proof of Lemma 2. □

We experimentally verified the correctness of Lemma 2 for $3 \leq d \leq 16$. Our program computes, for each of the conditions in $\mathsf{Bad}_{\mathrm{enc}}^{1}$, its probability for all the $(2^d - 1)$ non-zero plaintext differences, and outputs the maximum probability with the input difference that gives the maximum probability. The result fully confirms the correctness in this range. See Appendix A for more details.

We are now ready to present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = 2d-2$ in the following lemma.

Lemma 3. *For $r = 2d-2$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{(d-1)q^2}{2^n} + \frac{0.5(d-1)q^2}{2^{2n}}\,.$$

Proof. We compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. As mentioned, $\mathsf{Bad}^1_{\mathrm{enc}}$ contains $1 \times \binom{q}{2}$ conditions in $\mathsf{coll}_{\mathrm{s,s}}$, $d \times \binom{q}{2}$ conditions in $\mathsf{coll}_{\mathrm{s,c}}$, and $(d-1) \times \binom{q}{2}$ conditions in $\mathsf{coll}_{\mathrm{c,c}}$. From Lemma 2, we have

$$\begin{aligned}\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &\le \binom{q}{2} \cdot \left(\frac{d-2}{2^n} + \frac{1}{2^n} \cdot d + \frac{1}{2^{2n}} \cdot (d-1)\right) \\ &\le 0.5q^2 \cdot \left(\frac{2d-2}{2^n} + \frac{d-1}{2^{2n}}\right) = \frac{(d-1)q^2}{2^n} + \frac{0.5(d-1)q^2}{2^{2n}}\,,\end{aligned}$$

as claimed in Lemma 3. □

4.2.2 Bad Probability for $r = 3d - 2$

When $r = 3d-2$, for each of the conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$, we have the following lemma.

Lemma 4. *Let $r = 3d-2$, and consider one of the $2d \times \binom{q}{2}$ conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$. Then, the probability of the condition is at most $(d^2-d-2)/(2 \cdot 2^{2n})$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $(d-1)/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{s,c}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{c,c}}$.*

We proceed as in the proof of Lemma 2. We present a proof sketch below, and a full proof is presented in Appendix B.

Proof sketch. The overall structure of the proof is similar to that of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a $2n$-bit collision at (S^{r-2d+1}, S^{r-d}), which is a unique condition in $\mathsf{coll}_{\mathrm{s,s}}$. Since $S^{r-2d+1} = S^{d-1}$ and $S^{r-d} = S^{2d-2}$ hold when $r = 3d-2$, we evaluate

$$\Pr[S_i^{[r-2d+1,r-d]} = S_j^{[r-2d+1,r-d]} \wedge C_i^2 \neq C_j^2] \le \Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]}]\,.$$

We derive the upper bound $(d^2-d-2)/(2 \cdot 2^{2n})$ on $\Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]}]$ when the plaintext difference is $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$, where $\Delta M^2_{i,j}$ is any difference. Then, we show that this is the upper bound on all the possible plaintext differences by showing that other cases do not have a larger upper bound.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. For $\mathsf{coll}_{\mathrm{s,c}}$, we only consider a collision at (S^{r-2d+2}, C^2) that involves an internal state with the smallest index in the number of round. Since we have $S^{r-2d+2} = S^d$ when $r = 3d-2$, we evaluate

$$\Pr[(S_i^{r-2d+2}, C_i^2) = (S_j^{r-2d+2}, C_j^2) \wedge C_i^3 \neq C_j^3] \le \Pr[(S_i^d, C_i^2) = (S_j^d, C_j^2)]\,.$$

Then, we compute the upper bound $(d-1)/2^{2n}$ of $\Pr[(S_i^d, C_i^2) = (S_j^d, C_j^2)]$ when the plaintext difference is $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[4..d]} = 0$, where $\Delta M^3_{i,j}$ is an arbitrary difference. We can show that this upper bound covers all other cases.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{c,c}}$. The analysis is the same as in Eq. (6), and we obtain the upper bound $1/2^{2n}$ for all the conditions in $\mathsf{coll}_{\mathrm{c,c}}$. □

The correctness of Lemma 4 is also experimentally verified in the range of $3 \le d \le 16$. See Appendix A for more details.

We now present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = 3d-2$.

Lemma 5. *For $r = 3d - 2$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{0.25(3d^2 - d - 4)q^2}{2^{2n}}.$$

Proof. We compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world by taking summation of relevant bad probabilities. From Lemma 4, we have

$$\begin{aligned}\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &\leq \binom{q}{2} \cdot \left(\frac{d^2 - d - 2}{2 \cdot 2^{2n}} + \frac{d-1}{2^{2n}} \cdot d + \frac{1}{2^{2n}} \cdot (d-1)\right) \\ &\leq 0.5q^2 \cdot \frac{(d^2 - d - 2) + 2(d^2 - d) + 2(d-1)}{2 \cdot 2^{2n}} = \frac{0.25(3d^2 - d - 4)q^2}{2^{2n}},\end{aligned}$$

and this shows the bound in Lemma 5. □

4.3 Probability Ratio of Good Transcript

Here, we prove the following lemma regarding a good transcript $\theta \in \mathsf{T}_{\mathrm{good}}$.

Lemma 6. *For any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have*

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq 1 - \frac{0.5q^2}{2^{dn}}.$$

Proof. In the real world, the interpolation probability $\Pr[\Theta_{\mathcal{R}} = \theta]$ of $\theta \in \mathsf{T}_{\mathrm{good}}$ is the probability that r TPRs $\widetilde{P}_1, \ldots, \widetilde{P}_r$ interpolate θ. For $x \in [1..r]$, let p^x_{all} denote the probability that $\widetilde{P}_x$ interpolates all the q input-tweak-output associated to the TRP. Then, for any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have

$$\Pr[\Theta_{\mathcal{R}} = \theta] = \prod_{x=1}^{r} p^x_{\mathrm{all}} \geq \left(\prod_{x=1}^{r-d} p^x_{\mathrm{all}}\right) \cdot \left(\prod_{x=r-d+1}^{r} \frac{1}{2^{nq}}\right) = \left(\prod_{x=1}^{r-d} p^x_{\mathrm{all}}\right) \cdot \frac{1}{2^{dnq}}.$$

In the ideal world, the interpolation probability $\Pr[\Theta_{\mathcal{I}} = \theta]$ of $\theta \in \mathsf{T}_{\mathrm{good}}$ is the probability that the dn-bit random permutation π and $r-d$ TRPs $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$ interpolate the relevant plaintext-ciphertext or input-tweak-output associated to it. Note that for $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$, they generate the internal state with the same probability distribution as in the real world, and hence they have the same interpolation probability as $p^1_{\mathrm{all}}, \ldots, p^{r-d}_{\mathrm{all}}$, respectively. Therefore, for any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \left(\prod_{x=1}^{r-d} p^x_{\mathrm{all}}\right) \cdot \left(\prod_{i=1}^{q} \frac{1}{2^{dn} - (i-1)}\right).$$

We now compute the ratio as

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq \prod_{i=1}^{q} \frac{2^{dn} - (i-1)}{2^{dn}} = \prod_{i=1}^{q} \left(1 - \frac{i-1}{2^{dn}}\right) \geq 1 - \sum_{i=2}^{q} \frac{i-1}{2^{dn}} \geq 1 - \frac{0.5q^2}{2^{dn}},$$

and we obtain Lemma 6. □

5 SPRP Security of TBC-based Type-1 GFS

In this section, we prove SPRP security of $\mathcal{E}_{1,d,r}$, TBC-based type-1 GFS, where we use r independent (n, n)-TRPs.

Theorem 2 (TBC-based type-1 GFS, SPRP-security)**.** *Fix $d \geq 3$, and let $\widetilde{P}_1, \ldots, \widetilde{P}_r$ be r independent (n,n)-TRPs and $E = \mathcal{E}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$ be the TBC-based type-1 GFS. Then for any SPRP-adversary $\mathcal{A}$ that makes q queries, if $r = d^2 - 2d + 2$ rounds, we have*

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.5(d^2-2d+2)q^2}{2^n} + \frac{0.5q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,, \tag{7}$$

and if $r = d^2 - d + 2$ rounds, we have

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.25(d^3-3d+4)q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,. \tag{8}$$

In Theorem 2, Eq. (7) shows birthday-bound security and Eq. (8) shows BBB security. The former is obtained from Lemma 8, Lemma 11, and the Coefficient-H technique (Lemma 1), and the latter is obtained from Lemma 10, Lemma 11, and the Coefficient-H technique (Lemma 1).

In the proof of Theorem 2, both Eq. (7) and Eq. (8) consider CPCA security. The difference is in the number of rounds. We use the same definition of the oracles (Sect. 5.1) and the interpolation probability (Sect. 5.3). The computation of the probability of bad events (Sect. 5.2) is different. The case $r = d^2 - 2d + 2$ is in Sect. 5.2.1, and the case $r = d^2 - d + 2$ is in Sect. 5.2.2.

We consider a CPCA-adversary $\mathcal{A}$ that interacts with the real world oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$, or with the ideal world oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$. Without loss of generality, $\mathcal{A}$ is assumed to be deterministic, makes exactly q queries, does not repeat the same query, and does not make a redundant query, i.e., if $\mathcal{A}$ makes an encryption query M to obtain C, then it does not subsequently make a decryption query C, and vice versa.

5.1 Definition of the Oracles

The real world oracle $\mathcal{R}$ is defined as $\mathcal{E}_{1,d,r}$ that uses r independent TRPs $\widetilde{P}_1, \ldots, \widetilde{P}_r$, and $\mathcal{R}^{-1}$ is defined as $\mathcal{E}_{1,d,r}^{-1}$. If the i-th query is a query for $\mathcal{R}$, then we compute the internal states $S_i^1, \ldots, S_i^{r-d}$ with $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$, and the ciphertext with $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$. If the i-th query is a query for $\mathcal{R}^{-1}$, then we compute the internal states $S_i^{r-d}, \ldots, S_i^1$ with $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_{d+1}^{-1}$, and the plaintext with $\widetilde{P}_d^{-1}, \ldots, \widetilde{P}_1^{-1}$. For each query $\mathcal{A}$ makes, we record the internal states $S_i^1, \ldots, S_i^{r-d}$ in S, and the entire history of the internal states S is given to $\mathcal{A}$ after it makes q queries and before it outputs its decision bit. This only benefits $\mathcal{A}$, and we show Eq. (7) and Eq. (8) with this $\mathcal{A}$ that has S as input. The real world oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$ are presented in Fig. 8.

The ideal world oracle $\mathcal{I}$ is defined as the dn-bit random permutation π, and $\mathcal{I}^{-1}$ is defined as π^{-1}. For the i-th query, $\mathcal{I}$ and $\mathcal{I}^{-1}$ generate dummy internal states $S_i^1, \ldots, S_i^{r-d}$, and record them into S. After $\mathcal{A}$ makes q queries, S is given to $\mathcal{A}$. In $\mathcal{I}$, we simulate $\widetilde{P}_1, \ldots, \widetilde{P}_{r-d}$ to generate the internal states that have the same probability distribution as in $\mathcal{R}$. In $\mathcal{I}^{-1}$, we simulate $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_{d+1}^{-1}$ to generate the internal states that have the same probability distribution as in $\mathcal{R}^{-1}$. The simulation uses the lazy-sampling, and the algorithms of $\mathcal{I}$ and $\mathcal{I}^{-1}$ are presented in Fig. 9.

5.2 Bad Transcript and Bad Probability

The adversary $\mathcal{A}$ is given all the internal states after it makes q queries. The interaction between the oracle and $\mathcal{A}$ can be summarized as a transcript θ as

$$\theta = \left((M_1^{[1..d]}, C_1^{[1..d]}, S_1^{[1..r-d]}), \ldots, (M_q^{[1..d]}, C_q^{[1..d]}, S_q^{[1..r-d]})\right)\,. \tag{9}$$

Algorithm 3: Procedure of $\mathcal{R}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $(S_i^{-d+1}, S_i^{-d+2}, \ldots, S_i^{-1}, S_i^0) \leftarrow (M_i^2, M_i^3, \ldots, M_i^d, M_i^1)$
2. **for** $x = 1, 2, \ldots, r$ **do**
   $S_i^x \leftarrow \widetilde{P}_x(S_i^{x-1}, S_i^{x-d})$
3. $(C_i^1, C_i^2, \ldots, C_i^d) \leftarrow (S_i^r, S_i^{r-d+1}, S_i^{r-d+2}, \ldots, S_i^{r-1})$
4. **return** $C_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Algorithm 4: Procedure of $\mathcal{R}^{-1}$ for the i-th query
Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $M_i^{[1..d]} \in \{0,1\}^{dn}$

1. $(S_i^{r-d+1}, S_i^{r-d+2}, \ldots, S_i^{r-1}, S_i^r) \leftarrow (C_i^2, C_i^3 \ldots, C_i^d, C_i^1)$
2. **for** $x = r, r-1, \ldots, 1$ **do**
   $S_i^{x-d} \leftarrow \widetilde{P}_x^{-1}(S_i^{x-1}, S_i^x)$
3. $(M_i^1, M_i^2, \ldots, M_i^d) \leftarrow (S_i^0, S_i^{-d+1}, S_i^{-d+2}, \ldots, S_i^{-1})$
4. **return** $M_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Figure 8: Definition of $\mathcal{R}$ and $\mathcal{R}^{-1}$ for the SPRP proof of $\mathcal{E}_{1,d,r}$. Initially, S is empty, and S is given to $\mathcal{A}$ after it makes all the q queries.

Since we assume that $\mathcal{A}$ does not repeat a query, for any $1 \le j < i \le q$, we have $(M_i^1, \ldots, M_i^d) \neq (M_j^1, \ldots, M_j^d)$ and $(C_i^1, \ldots, C_i^d) \neq (C_j^1, \ldots, C_j^d)$. For a transcript in Eq. (9), we define two sets of indices to specify the direction of the queries:

$$\mathcal{Q}_{\mathrm{e}} = \{i \mid \text{the } i\text{-th query is an encryption query}\}$$
$$\mathcal{Q}_{\mathrm{d}} = \{i \mid \text{the } i\text{-th query is a decryption query}\}$$

We follow a similar argument to Sect. 4.2 to define the set of bad transcripts. In the ideal world, for $\widetilde{P}_x$ with $x \in [1..r-d]$ in encryption and $\widetilde{P}_x^{-1}$ with $x \in [d+1..r]$ in decryption, i.e., for TPRs that we simulate, it has the same input-tweak-output relation as in the real world. However, for $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$ in encryption and $\widetilde{P}_d^{-1}, \ldots, \widetilde{P}_1^{-1}$ in decryption that are not simulated in the ideal world, this may not be the case. That is, the output can be different even though it takes the same input and tweak, or the input can be different when it takes the same output and tweak. In other words, in the ideal world, TRPs $\widetilde{P}_{r-d+1}, \ldots, \widetilde{P}_r$ in encryption and $\widetilde{P}_d^{-1}, \ldots, \widetilde{P}_1^{-1}$ in decryption are not simulated, and there are conditions on these TRPs that can only hold in the ideal world. Our definition of the set of bad transcripts, $\mathsf{T}_{\mathrm{bad}}$, consists of all such transcripts θ.

If the i-th query is an encryption query, the same conditions as $\mathsf{Bad}^1_{\mathrm{enc}}$ in Sect. 4.2 can only hold in the ideal world. Here, $1 \le j < i \le q$, and since we have $\sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ possible combinations of i and j, these conditions are $2d \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ possible collisions of $2n$-bit variables in $\mathsf{Bad}^1_{\mathrm{enc}}$. Note that we consider bad conditions that occur at the i-th query, and j is in the range $1 \le j < i \le q$. That is, i is in $\mathcal{Q}_{\mathrm{e}}$, while j can be in $\mathcal{Q}_{\mathrm{e}}$ or $\mathcal{Q}_{\mathrm{d}}$.

If the i-th query is a decryption query, we let $x \in [2..d]$, and we consider the following

Algorithm 5: Procedure of $\mathcal{I}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $C_i^{[1..d]} \leftarrow \pi(M_i^{[1..d]})$
2. $(S_i^{-d+1}, S_i^{-d+2}, \ldots, S_i^{-1}, S_i^0) \leftarrow (M_i^2, M_i^3, \ldots, M_i^d, M_i^1)$
3. **for** $x = 1, 2, \ldots, r-d$ **do**
   $\mathcal{S}_i^x \leftarrow \{S_j^x \mid j < i \wedge S_i^{x-1} = S_j^{x-1}\}$
   if $\exists j < i, S_i^{[x-d,x-1]} = S_j^{[x-d,x-1]}$ **then** $S_i^x \leftarrow S_j^x$
   else $S_i^x \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{S}_i^x$
4. **return** $C_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Algorithm 6: Procedure of $\mathcal{I}^{-1}$ for the i-th query
Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $M_i^{[1..d]} \in \{0,1\}^{dn}$

1. $M_i^{[1..d]} \leftarrow \pi^{-1}(C_i^{[1..d]})$
2. $(S_i^{r-d+1}, S_i^{r-d+2}, \ldots, S_i^{r-1}, S_i^r) \leftarrow (C_i^2, C_i^3 \ldots, C_i^d, C_i^1)$
3. **for** $x = r, r-1, \ldots, d+1$ **do**
   $\mathcal{S}_i^{x-d} \leftarrow \{S_j^{x-d} \mid j < i \wedge S_i^{x-1} = S_j^{x-1}\}$
   if $\exists j < i, S_i^{[x-1,x]} = S_j^{[x-1,x]}$ **then** $S_i^{x-d} \leftarrow S_j^{x-d}$
   else $S_i^{x-d} \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{S}_i^{x-d}$
4. **return** $M_i^{[1..d]}$
5. $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{[1..r-d]}$

Figure 9: Definition of $\mathcal{I}$ and $\mathcal{I}^{-1}$ for the SPRP proof of $\mathcal{E}_{1,d,r}$. Initially, S is empty, and S is given to $\mathcal{A}$ after it makes all the q queries.

bad conditions:

$$\begin{aligned}
\text{Bad at } \widetilde{P}_1 :\ & (M_i^1, M_i^2) = (M_j^1, M_j^2) \wedge S_i^1 \neq S_j^1 \\
& \text{or } (M_i^1, S_i^1) = (M_j^1, S_j^1) \wedge M_i^2 \neq M_j^2 \\
\text{Bad at } \widetilde{P}_x :\ & (M_i^{x+1}, S_i^{x-1}) = (M_j^{x+1}, S_j^{x-1}) \wedge S_i^x \neq S_j^x \\
& \text{or } (S_i^{x-1}, S_i^x) = (S_j^{x-1}, S_j^x) \wedge M_i^{x+1} \neq M_j^{x+1}
\end{aligned}$$

Here, when $x = d$, we let $M^{d+1} = M^1$. If $r < 2d$, then a ciphertext block (instead of a block of internal state) is involved in the condition, and we let $S^{r-d+1} = C^2$.

These conditions can only hold in the ideal world, and they are impossible in the real world. We define $\mathsf{Bad}^1_{\mathrm{dec}}$ as the set of all these conditions. Here, $1 \le j < i \le q$, and since we have $\sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ possible combinations of i and j, $\mathsf{Bad}^1_{\mathrm{dec}}$ consists of:

- $(d-1) \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions of a $2n$-bit collision between two internal state blocks (e.g., $(S_i^{x-1}, S_i^x) = (S_j^{x-1}, S_j^x)$), which we write $\mathsf{coll}_{\mathrm{s,s}}$,
- $d \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions of a $2n$-bit collision between one internal state block and one plaintext block (e.g., $(M_i^{x+1}, S_i^{x-1}) = (M_j^{x+1}, S_j^{x-1})$), which we write $\mathsf{coll}_{\mathrm{s,m}}$, and

- $1 \times \sum_{i \in \mathcal{Q}_\mathrm{d}} (i-1)$ conditions of a $2n$-bit collision between two plaintext blocks (e.g., $(M_i^1, M_i^2) = (M_j^1, M_j^2)$), which we write $\mathsf{coll}_{\mathrm{m,m}}$.

In total, we have $2d \times \sum_{i \in \mathcal{Q}_\mathrm{d}} (i-1)$ possible collisions of $2n$-bit variables in $\mathsf{Bad}^1_{\mathrm{dec}}$. Note that i is in $\mathcal{Q}_\mathrm{d}$, while j can be in $\mathcal{Q}_\mathrm{e}$ or $\mathcal{Q}_\mathrm{d}$.

Now the set of bad transcripts $\mathsf{T}_{\mathrm{bad}}$ is defined as the set of all the attainable transcripts that satisfy at least one of the conditions in $\mathsf{Bad}^1_{\mathrm{enc}} \cup \mathsf{Bad}^1_{\mathrm{dec}}$. Formally, we define

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \theta \text{ satisfies at least one of the conditions in } \mathsf{Bad}^1_{\mathrm{enc}} \cup \mathsf{Bad}^1_{\mathrm{dec}}\}.$$

The set of good transcripts $\mathsf{T}_{\mathrm{good}} = \mathsf{T}_{\mathrm{all}} \setminus \mathsf{T}_{\mathrm{bad}}$ is defined as the set of all the attainable transcripts θ that are not in $\mathsf{T}_{\mathrm{bad}}$.

In what follows, we evaluate the probability to have bad transcripts. We consider the case $r = d^2 - 2d + 2$ first, and then $r = d^2 - d + 2$.

5.2.1 Bad Probability for $r = d^2 - 2d + 2$

Let $r = d^2 - 2d + 2$. For each of the conditions in $\mathsf{Bad}^1_{\mathrm{dec}}$, we have the following lemma.

Lemma 7. *Let $r = d^2 - 2d + 2$, and consider one of the $2d \times \sum_{i \in \mathcal{Q}_\mathrm{d}} (i-1)$ conditions in $\mathsf{Bad}^1_{\mathrm{dec}}$ in the ideal world. Then, the probability of the condition is at most $(d-2)/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $1/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,m}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{m,m}}$.*

Proof. In this proof, we write $\widetilde{P}'_1, \ldots, \widetilde{P}'_{r-d}$ for $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_{d+1}^{-1}$ that are simulated in $\mathcal{I}^{-1}$, i.e., for $x \in [d+1..r]$, we let $\widetilde{P}_x^{-1}(\cdot) = \widetilde{P}'_{r-x+1}(\cdot)$. Similarly, we write $T^1, \ldots, T^{r-d}$ for the internal states $S^{r-d}, \ldots, S^1$ that are computed with $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_{d+1}^{-1}$, respectively, i.e., we let $S^x = T^{r-d-x+1}$ for $x \in [1..r-d]$. That is, for $x_1 \in [2..d-1]$ and $x_2 \in [d+1..r-d]$, we write

$$\begin{array}{rl} S^{r-d} = \widetilde{P}_r^{-1}(C^d, C^1) & \\ S^{r-d-x_1+1} = \widetilde{P}_{r-x_1+1}^{-1}(C^{d-x_1+1}, C^{d-x_1+2}) & \\ S^{r-2d+1} = \widetilde{P}_{r-d+1}^{-1}(S^{r-d}, C^2) & \\ S^{r-d-x_2+1} = \widetilde{P}_{r-x_2+1}^{-1}(S^{r-x_2}, S^{r-x_2+1}) & \end{array} \mapsto \begin{array}{l} T^1 = \widetilde{P}'_1(C^d, C^1) \\ T^{x_1} = \widetilde{P}'_{x_1}(C^{d-x_1+1}, C^{d-x_1+2}) \\ T^d = \widetilde{P}'_d(T^1, C^2) \\ T^{x_2} = \widetilde{P}'_{x_2}(T^{x_2-d+1}, T^{x_2-d}) \end{array},$$

where the index x in $\widetilde{P}'_x$ indicates that the TRP $\widetilde{P}'_x$ is in the x-th round in the decryption direction. See Fig. 10 for an example of this labeling. Note that $\widetilde{P}'_{r-d+1}, \ldots, \widetilde{P}'_r$ are not used in this proof since we consider $\mathcal{I}^{-1}$ that simulates $\widetilde{P}'_1, \ldots, \widetilde{P}'_{r-d}$.

We proceed as in the proof of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,m}}$ and $\mathsf{coll}_{\mathrm{m,m}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We analyze a condition in $\mathsf{coll}_{\mathrm{s,s}}$. Now $\mathsf{coll}_{\mathrm{s,s}}$ contains a collision at $(S^1, S^2), (S^2, S^3), \ldots, (S^{d-1}, S^d)$. Among these $d-1$ collisions, we focus on (S^{d-1}, S^d) that involves the internal states with the largest index in the number of round, since other collisions cannot have a larger collision probability. For instance, for $d = 4$, $\mathsf{coll}_{\mathrm{s,s}}$ contains a collision at $(S^1, S^2), (S^2, S^3)$, and (S^3, S^4), and clearly, the collision probability at (S^3, S^4) is no smaller than the collision probability at other places (See Fig. 7, right). Recall that here we are dealing with decryption queries. Since $S^{d-1} = T^{r-2d+2} = T^{d^2-4d+4}$ and $S^d = T^{d^2-4d+3}$ hold when $r = d^2 - 2d + 2$, we evaluate

$$\Pr[S_i^{[d-1,d]} = S_j^{[d-1,d]} \wedge M_i^1 \neq M_j^1] \leq \Pr[T_i^{[d^2-4d+3, d^2-4d+4]} = T_j^{[d^2-4d+3, d^2-4d+4]}]. \quad (10)$$

We first evaluate Eq. (10) when the ciphertext difference is $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^d \neq 0$, where $\Delta C_{i,j}^1$ can take any difference. We then show that this gives us the upper bound on

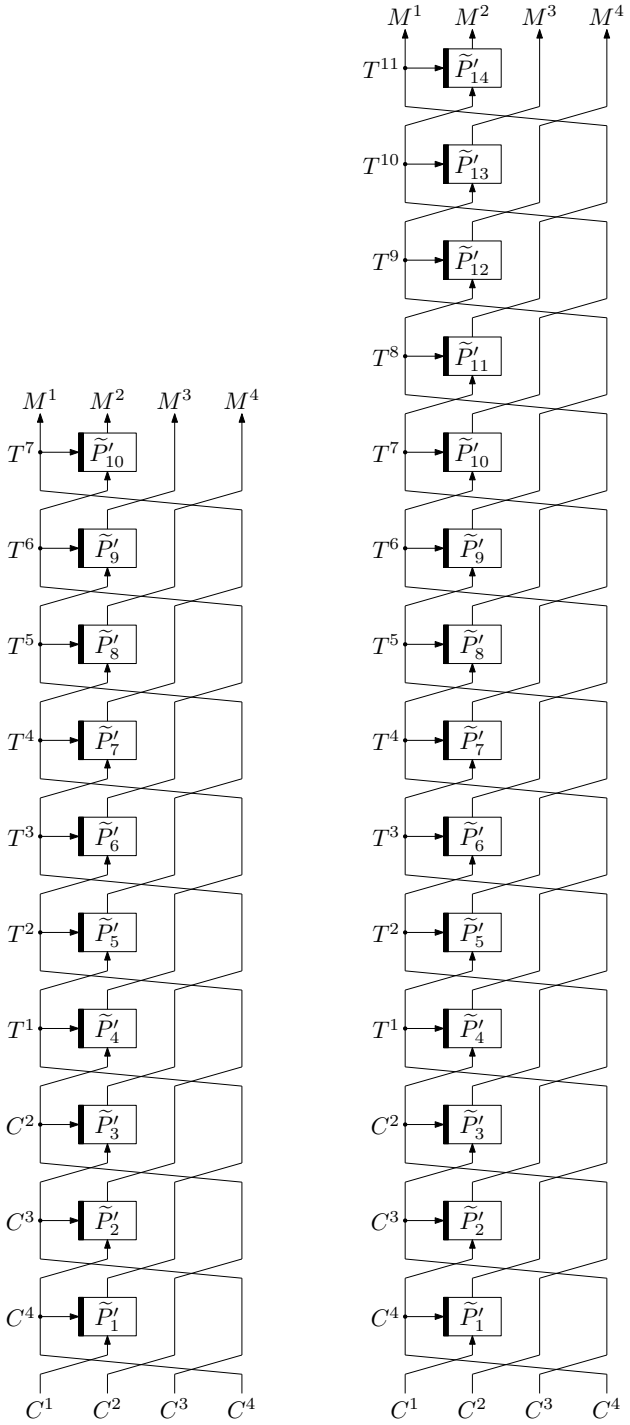

Figure 10: Examples of $\mathcal{E}_{1,d,r}^{-1}$ with $d = 4$, where the TRPs and the internal states are labeled as in the proof of Lemma 7. Left: $\mathcal{E}_{1,d,r}^{-1}(C^1 \parallel \cdots \parallel C^4) = (M^1 \parallel \cdots \parallel M^4)$ for $r = d^2 - 2d + 2 = 10$. Right: $\mathcal{E}_{1,d,r}^{-1}(C^1 \parallel \cdots \parallel C^4) = (M^1 \parallel \cdots \parallel M^4)$ for $r = d^2 - d + 2 = 14$.

all the possible ciphertext differences by showing that all other cases do not have a larger upper bound.

Now, for any $x \in [3..d-1]$, since we have $T^x = \widetilde{P}'_x(C^{d-x+1}, C^{d-x+2})$ and from $C_i^{[2..d-1]} = C_j^{[2..d-1]}$, we must have $T_i^x = T_j^x$, i.e., $T_i^{[3..d-1]} = T_j^{[3..d-1]}$. From this and $T^x = \widetilde{P}'_x(T^{x-d+1}, T^{x-d})$ for any $x \in [d+3..2d-2]$, we must have $T_i^x = T_j^x$, i.e., $T_i^{[d+3..2d-2]} = T_j^{[d+3..2d-2]}$. Furthermore, for any $x \in [2d+3..3d-3]$, we must have $T_i^x = T_j^x$ from $T^x = \widetilde{P}'_x(T^{x-d+1}, T^{x-d})$. Similarly, for integer $\ell \geq 1$ and $x \in [(\ell-1)d+3..\ell(d-1)]$, we must have collisions at $T^x = \widetilde{P}'_x(C^{d-x+1}, C^{d-x+2})$ if $\ell = 1$, and have collisions at $T^x = \widetilde{P}'_x(T^{x-d+1}, T^{x-d})$ if $\ell \geq 2$. These collisions hold up to $\ell = d-3$ which satisfies $(\ell-1)d+3 = \ell(d-1)$. In other words, we always have $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$, since we have $T_i^x = T_j^x$ for $\ell \in [1..d-3]$ and $x \in [(\ell-1)d+3..\ell(d-1)]$. Therefore, we have $\Pr[T_i^{d^2-4d+3} = T_j^{d^2-4d+3}] = 1$ from $(d-3)(d-1) = d^2-4d+3$. This probability holds in the case $d = 3$, since $T^{d^2-4d+3} = T^0$ corresponds to C^2.

Example 3. If $d = 4$ and $r = d^2 - 2d + 2 = 10$ (See Fig. 10, left), we have

$$\text{Eq. (10)} = \Pr[T_i^{[d^2-4d+3,d^2-4d+4]} = T_j^{[d^2-4d+3,d^2-4d+4]}] = \Pr[T_i^{[3,4]} = T_j^{[3,4]}]\,.$$

When $\Delta C_{i,j}^{[2,3]} = 0 \wedge \Delta C_{i,j}^4 \neq 0$, we must have $T_i^3 = T_j^3$ from $T^3 = \widetilde{P}'_3(C^2, C^3)$, i.e., $\Pr[T_i^3 = T_j^3] = 1$.

Example 4. If $d = 6$ and $r = d^2 - 2d + 2 = 26$, we have

$$\text{Eq. (10)} = \Pr[T_i^{[d^2-4d+3,d^2-4d+4]} = T_j^{[d^2-4d+3,d^2-4d+4]}] = \Pr[T_i^{[15,16]} = T_j^{[15,16]}]\,.$$

When $\Delta C_{i,j}^{[2..5]} = 0 \wedge \Delta C_{i,j}^6 \neq 0$, we must have $T_i^{[3..5]} = T_j^{[3..5]}$ from $T^3 = \widetilde{P}'_3(C^4, C^5)$, $T^4 = \widetilde{P}'_4(C^3, C^4)$, and $T^5 = \widetilde{P}'_5(C^2, C^3)$. Since $T^9 = \widetilde{P}'_9(T^4, T^3)$ and $T^{10} = \widetilde{P}'_{10}(T^5, T^4)$, we must have $T_i^{[9,10]} = T_j^{[9,10]}$. Therefore, we also have $T_i^{15} = T_j^{15}$ from $T^{15} = \widetilde{P}'_{15}(T^{10}, T^9)$, i.e., $T_i^{[5..15:5]} = T_j^{[5..15:5]}$ and $\Pr[T_i^{15} = T_j^{15}] = 1$.

Next, the probability of a collision at $T^1 = \widetilde{P}'_1(C^d, C^1)$ is $\Pr[T_i^1 = T_j^1] = 1/2^n$, since $C_i^d \neq C_j^d$. From $C_i^2 = C_j^2$, the probability of a collision at $T^d = \widetilde{P}'_d(T^1, C^2)$ is

$$\begin{aligned}\Pr[T_i^d = T_j^d] &= \Pr[T_i^1 = T_j^1] + \Pr[T_i^1 \neq T_j^1] \cdot \Pr[T_i^d = T_j^d \mid T_i^1 \neq T_j^1] \\ &\leq \Pr[T_i^1 = T_j^1] + \frac{1}{2^n} = \frac{2}{2^n}\,.\end{aligned}$$

Similarly, for any $x \in [1..d-4]$, since we have $T^{x(d-1)+d} = \widetilde{P}'_{x(d-1)+d}(T^{x(d-1)+1}, T^{x(d-1)})$ and from $T_i^{[d-1..(d-4)(d-1):d-1]} = T_j^{[d-1..(d-4)(d-1):d-1]}$, if $T_i^{x(d-1)+1} = T_j^{x(d-1)+1}$, then we must have $T_i^{x(d-1)+d} = T_j^{x(d-1)+d}$. Therefore, for each $x \in [0..d-4]$, we have

$$\begin{aligned}&\Pr[T_i^{x(d-1)+d} = T_j^{x(d-1)+d}] \\ &\quad= \Pr[T_i^{x(d-1)+1} = T_j^{x(d-1)+1}] + \Pr[T_i^{x(d-1)+1} \neq T_j^{x(d-1)+1}] \\ &\qquad\cdot \Pr[T_i^{x(d-1)+d} = T_j^{x(d-1)+d} \mid T_i^{x(d-1)+1} \neq T_j^{x(d-1)+1}] \\ &\quad\leq \Pr[T_i^{x(d-1)+1} = T_j^{x(d-1)+1}] + \frac{1}{2^n} \leq \Pr[T_i^1 = T_j^1] + \sum_{\ell=0}^{x} \frac{1}{2^n} = \frac{x+2}{2^n}\,.\end{aligned}$$

From $(d-4)(d-1)+d = d^2-4d+4$, we have $\Pr[T_i^{d^2-4d+4} = T_j^{d^2-4d+4}] \le ((d-4)+2)/2^n = (d-2)/2^n$. Therefore, from $\Pr[T_i^{d^2-4d+3} = T_j^{d^2-4d+3}] = 1$, we obtain

$$\begin{aligned}\text{Eq. (10)} &= \Pr[T_i^{[d^2-4d+3,d^2-4d+4]} = T_j^{[d^2-4d+3,d^2-4d+4]}] \\ &\le \Pr[T_i^{d^2-4d+4} = T_j^{d^2-4d+4}] \le \frac{d-2}{2^n}\,,\end{aligned}$$

and this gives us an upper bound $(d-2)/2^n$ on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^{d} \neq 0$, and $\Delta C_{i,j}^{1}$ is any difference.

Example 5. Following Example 3 with $d = 4$ and $r = 10$, if $\Delta C_{i,j}^{[2,3]} = 0 \wedge \Delta C_{i,j}^{4} \neq 0$, the probability of a collision at $T^1 = \widetilde{P}_1'(C^4, C^1)$ is $\Pr[T_i^1 = T_j^1] = 1/2^n$ from $C_i^4 \neq C_j^4$. Since $C_i^2 = C_j^2$ and $T^4 = \widetilde{P}_4'(T^1, C^2)$, we have $\Pr[T_i^4 = T_j^4] \le \Pr[T_i^1 = T_j^1] + 1/2^n = 2/2^n$. Therefore, from $\Pr[T_i^3 = T_j^3] = 1$, we obtain

$$\text{Eq. (10)} = \Pr[T_i^{[3,4]} = T_j^{[3,4]}] \le \Pr[T_i^4 = T_j^4] \le \frac{2}{2^n}\,.$$

Example 6. With $d = 6$ and $r = 26$ as in Example 4, if $\Delta C_{i,j}^{[2..5]} = 0 \wedge \Delta C_{i,j}^{6} \neq 0$, the probability of a collision at $T^1 = \widetilde{P}_1'(C^6, C^1)$ is $\Pr[T_i^1 = T_j^1] = 1/2^n$ from $C_i^6 \neq C_j^6$. Since $C_i^2 = C_j^2$ and $T^6 = \widetilde{P}_6'(T^1, C^2)$, we have $\Pr[T_i^6 = T_j^6] \le \Pr[T_i^1 = T_j^1] + 1/2^n = 2/2^n$. Similarly, from $T^{11} = \widetilde{P}_{11}'(T^6, T^5)$, $T^{16} = \widetilde{P}_{16}'(T^{11}, T^{10})$, and $T_i^{[5,10]} = T_j^{[5,10]}$, we also have $\Pr[T_i^{16} = T_j^{16}] \le \Pr[T_i^{11} = T_j^{11}] + 1/2^n \le \Pr[T_i^6 = T_j^6] + 2/2^n \le 4/2^n$. Therefore, from $\Pr[T_i^{15} = T_j^{15}] = 1$, we obtain

$$\text{Eq. (10)} = \Pr[T_i^{[15,16]} = T_j^{[15,16]}] \le \Pr[T_i^{16} = T_j^{16}] \le \frac{4}{2^n}\,.$$

We next prove that this is the upper bound for all other ciphertext differences by showing that any other ciphertext difference does not have a larger upper bound. Observe that the event $T_i^{[d^2-4d+3,d^2-4d+4]} = T_j^{[d^2-4d+3,d^2-4d+4]}$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,s}}$ in the proof of Lemma 2.

(C-4) First, let us assume that $\Delta C_{i,j}^{[2..d-1]} \neq 0 \wedge \Delta C_{i,j}^{d} \neq 0$, namely, for some $x \in [2..d-1]$, we have $\Delta C_{i,j}^{x} \neq 0$, where there may be multiple indices of x. If $x = 2$, we have $\Pr[T_i^d = T_j^d] \le 1/2^n$ from $T^d = \widetilde{P}_d'(T^1, C^2)$, and hence the probability would be smaller. If $x \in [3..d-1]$, the event $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$ would be a probabilistic event. Therefore, we have $\Pr[T_i^{d^2-4d+3} = T_j^{d^2-4d+3}] < 1$, and hence the probability would be smaller.

(C-5) Next, consider the case $\Delta C_{i,j}^{1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$. From $T^1 = \widetilde{P}_1'(C^d, C^1)$, we must have $T_i^1 \neq T_j^1$. Now if we further assume that $\Delta C_{i,j}^{[2..d-1]} = 0$, we are back to the initial case of $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^{d} \neq 0$ starting from the d-th round, and the analysis corresponds to the one with a reduced round version by $(d-1)$ rounds. Following the above computation, this would result in the reduction on the number of terms added to the upper bound. The case $\Delta C_{i,j}^{[2..d-1]} \neq 0$ would have a smaller upper bound as in the case (C-4).

(C-6) Finally, we consider the case $\Delta C_{i,j}^{[1,d]} = 0$, in which case we necessarily have $\Delta C_{i,j}^{[2..d-1]} \neq 0$. Consider the largest index $y \in [2..d-1]$ such that $\Delta C_{i,j}^{y} \neq 0$.

Then since $\Delta C_{i,j}^{[y+1..d]} = 0$, it has the same input difference as $\Delta C_{i,j}^{d} \neq 0$ at the input of the $(d-y+1)$-th round, and hence this case corresponds to the analysis of the reduced round version by $(d-y)$ rounds.

If $y = d-1$ and $\Delta C_{i,j}^{[2..d-2]} = 0$, we have $\Pr[T_i^{d^2-4d+4} = T_j^{d^2-4d+4}] = 1$, but we also have $\Pr[T_i^{d^2-4d+3} = T_j^{d^2-4d+3}] = 0$. Since this case corresponds to the analysis of the reduced round version by one round, T^x in the initial case corresponds to T^{x+1} in this case. Then, we have $T_i^x = T_j^x$ for $\ell \in [1..d-3]$ and $x \in [(\ell-1)d+4..\ell(d-1)+1]$, i.e., $T_i^{[4..(d-4)d+4:d]} = T_j^{[4..(d-4)d+4:d]}$. It follows that for any $\ell \in [0..d-4]$, we have $T_i^{\ell d+3} \neq T_j^{\ell d+3}$ since $T^3 = \widetilde{P}'_3(C^{d-2}, C^{d-1})$ and $T^{\ell d+3} = \widetilde{P}'_{\ell d+3}(T^{(\ell-1)d+4}, T^{(\ell-1)d+3})$. Therefore, $\Pr[T_i^{d^2-4d+3} = T_j^{d^2-4d+3}] = 0$ holds in this case. Note that this holds for the case $d = 3$, since $T^{d^2-4d+3} = T^0 = C^2$.

In other cases, the event $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$ would be a probabilistic event, and hence the final bound cannot be larger as in the analysis of the case (C-4).

Therefore, the case $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^{d} \neq 0$, where $\Delta C_{i,j}^{1}$ is any difference, maximizes Eq. (10) and the corresponding upper bound $(d-2)/2^n$ is the upper bound for all the cases in $\mathsf{coll}_{\mathrm{s,s}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,m}}$. Next, we consider a condition in $\mathsf{coll}_{\mathrm{s,m}}$. With the same reasoning as the case of $\mathsf{coll}_{\mathrm{s,s}}$, we consider a collision at (M^1, S^{d-1}) that involves an internal state with the largest index in the number of round, as a collision at other places cannot have a larger collision probability. Since $S^{d-1} = T^{r-2d+2} = T^{d^2-4d+4}$ holds when $r = d^2-2d+2$, we evaluate

$$\Pr[(M_i^1, S_i^{d-1}) = (M_j^1, S_j^{d-1}) \wedge S_i^d \neq S_j^d] \leq \Pr[(M_i^1, T_i^{d^2-4d+4}) = (M_j^1, T_j^{d^2-4d+4})]\,. \quad (11)$$

We first compute the upper bound on Eq. (11) when the ciphertext difference is $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$. We then show that this upper bound covers all other cases.

Now from $C_i^{[1,d]} = C_j^{[1,d]}$, we have $T_i^1 = T_j^1$ since $T^1 = \widetilde{P}'_1(C^d, C^1)$. Then the input difference $C^d \parallel T^1 \parallel C^{[2..d-1]}$ of the second round becomes the same ciphertext difference $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^{d} \neq 0$ in the analysis of $\mathsf{coll}_{\mathrm{s,s}}$. By adding a round at the beginning, T^x in the analysis of $\mathsf{coll}_{\mathrm{s,s}}$ corresponds to T^{x+1} in this analysis. With the same argument, we have $\Pr[T_i^{d^2-4d+4} = T_j^{d^2-4d+4}] = 1$.

In the ideal world, plaintexts are obtained as the output of the dn-bit random permutation π^{-1}. This implies that regardless of the ciphertext difference, by following the computation in Eq. (5), we similarly have $\Pr[M_i^1 = M_j^1] \leq 1/2^n$. We thus have

$$\text{Eq. (11)} = \Pr[(M_i^1, T_i^{d^2-4d+4}) = (M_j^1, T_j^{d^2-4d+4})] \leq \Pr[M_i^1 = M_j^1] \leq \frac{1}{2^n}\,,$$

when the ciphertext difference is $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$.

Next, we show that this upper bound covers all other cases. Since $\Pr[M_i^1 = M_j^1]$ does not depend on the ciphertext difference, and we cannot have a larger probability than $\Pr[T_i^{d^2-4d+4} = T_j^{d^2-4d+4}] = 1$, the case $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$ maximizes Eq. (11) and $1/2^n$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,m}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{m,m}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{m,m}}$. From a similar analysis to Eq. (6), the probability of a condition in $\mathsf{coll}_{\mathrm{m,m}}$ is at most $1/2^{2n}$. This completes the proof of Lemma 7. □

The correctness of Lemma 7 is also experimentally verified in the range of $3 \leq d \leq 16$. See Appendix A for more details.

We are now ready to present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = d^2 - 2d + 2$.

Lemma 8. *For $r = d^2 - 2d + 2$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{0.5(d^2 - 2d + 2)q^2}{2^n} + \frac{0.5q^2}{2^{2n}}.$$

Proof. We compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. Let p_i^{enc} and p_i^{dec} be the probability that $\mathsf{Bad}_{\mathrm{enc}}^1$ and $\mathsf{Bad}_{\mathrm{dec}}^1$ occur for the first time in the i-th query, respectively. In other words, we assume that neither $\mathsf{Bad}_{\mathrm{enc}}^1$ nor $\mathsf{Bad}_{\mathrm{dec}}^1$ occurs before the i-th query, and compute p_i^{enc} and p_i^{dec}. Then, we have

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] = \sum_{i=2}^{q} (p_i^{\mathrm{enc}} + p_i^{\mathrm{dec}}) = \sum_{i \in \mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i \in \mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}}. \tag{12}$$

We note that $p_i^{\mathrm{enc}} = 0$ if $i \notin \mathcal{Q}_{\mathrm{e}}$. Similarly, $p_i^{\mathrm{dec}} = 0$ if $i \notin \mathcal{Q}_{\mathrm{d}}$.

If the i-th query is an encryption query, we consider bad conditions in $\mathsf{Bad}_{\mathrm{enc}}^1$. Since $d \geq 3$, we have $d^2 - 2d + 2 > 2d - 2$ from $(d^2 - 2d + 2) - (2d - 2) = (d - 2)^2 > 0$, i.e., $r = d^2 - 2d + 2$ is larger than $r = 2d - 2$ in Sect. 4.2.1. Therefore, for $r = d^2 - 2d + 2$, each probability of the conditions in $\mathsf{Bad}_{\mathrm{enc}}^1$ does not have a larger upper bound than the probability in Lemma 2. As mentioned, $\mathsf{Bad}_{\mathrm{enc}}^1$ contains $1 \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,s}}$, $d \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,c}}$, and $(d-1) \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{c,c}}$. From Lemma 2, we have

$$p_i^{\mathrm{enc}} \leq (i-1) \cdot \left(\frac{d-2}{2^n} + \frac{1}{2^n} \cdot d + \frac{1}{2^{2n}} \cdot (d-1) \right) = (i-1) \cdot \left(\frac{2d-2}{2^n} + \frac{d-1}{2^{2n}} \right).$$

If the i-th query is a decryption query, we consider bad conditions in $\mathsf{Bad}_{\mathrm{dec}}^1$. As mentioned, $\mathsf{Bad}_{\mathrm{dec}}^1$ contains $(d-1) \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,s}}$, $d \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,m}}$, and $1 \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{m,m}}$. From Lemma 7, we have

$$p_i^{\mathrm{dec}} \leq (i-1) \cdot \left(\frac{d-2}{2^n} \cdot (d-1) + \frac{1}{2^n} \cdot d + \frac{1}{2^{2n}} \right) = (i-1) \cdot \left(\frac{d^2 - 2d + 2}{2^n} + \frac{1}{2^{2n}} \right).$$

Therefore, p_i^{dec} in the case that the i-th query is decryption has a larger upper bound than p_i^{enc} in the case that the i-th query is encryption, and we have

$$\begin{aligned} \Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &= \sum_{i \in \mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i \in \mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}} \leq \sum_{i=2}^{q} \left((i-1) \cdot \left(\frac{d^2 - 2d + 2}{2^n} + \frac{1}{2^{2n}} \right) \right) \\ &\leq 0.5q^2 \cdot \left(\frac{d^2 - 2d + 2}{2^n} + \frac{1}{2^{2n}} \right) = \frac{0.5(d^2 - 2d + 2)q^2}{2^n} + \frac{0.5q^2}{2^{2n}}, \end{aligned}$$

as claimed in Lemma 8. □

5.2.2 Bad Probability for $r = d^2 - d + 2$

When $r = d^2 - d + 2$, for each of the conditions in $\mathsf{Bad}_{\mathrm{dec}}^1$, we have the following lemma.

Lemma 9. *Let $r = d^2 - d + 2$, and consider one of the $2d \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions in $\mathsf{Bad}_{\mathrm{dec}}^1$. Then, the probability of the condition is at most $(d^2 - d - 2)/(2 \cdot 2^{2n})$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $(d-1)/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{s,m}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{m,m}}$.*

We proceed as in the proof of Lemma 2. We present a proof sketch below, and a full proof is presented in Appendix C.

Proof sketch. The overall structure of the proof is similar to that of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,m}}$ and $\mathsf{coll}_{\mathrm{m,m}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a $2n$-bit collision at (S^{d-1}, S^d) that involves an internal state with the largest index in the number of round. We evaluate

$$\Pr[S_i^{[d-1,d]} = S_j^{[d-1,d]} \wedge M_i^1 \neq M_j^1] \leq \Pr[S_i^{[d-1,d]} = S_j^{[d-1,d]}] .$$

We derive the upper bound $(d^2 - d - 2)/(2 \cdot 2^{2n})$ on $\Pr[S_i^{[d-1,d]} = S_j^{[d-1,d]}]$ when the ciphertext difference is $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^d \neq 0$, where $\Delta C_{i,j}^1$ is any difference. Then, we show that this is the upper bound on all the possible ciphertext differences by showing that other cases do not have a larger upper bound.

Analysis of $\mathsf{coll}_{\mathrm{s,m}}$. For $\mathsf{coll}_{\mathrm{s,m}}$, we only consider a collision at (M^1, S^{d-1}) that involves an internal state with the largest index in the number of round. We evaluate

$$\Pr[(M_i^1, S_i^{d-1}) = (M_j^1, S_j^{d-1}) \wedge S_i^d \neq S_j^d] \leq \Pr[(M_i^1, S_i^{d-1}) = (M_j^1, S_j^{d-1})] .$$

Then, we compute the upper bound $(d-1)/2^{2n}$ of $\Pr[(M_i^1, S_i^{d-1}) = (M_j^1, S_j^{d-1})]$ when the ciphertext difference is $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C^d = 0$. We can show that this upper bound covers all other cases.

Analysis of $\mathsf{coll}_{\mathrm{m,m}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{m,m}}$. The analysis is similar to Eq. (6), and we obtain the upper bound $1/2^{2n}$ for all the conditions in $\mathsf{coll}_{\mathrm{m,m}}$. □

The correctness of Lemma 9 is also experimentally verified in the range of $3 \leq d \leq 16$. See Appendix A for more details.

We now present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = d^2 - d + 2$.

Lemma 10. *For $r = d^2 - d + 2$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{0.25(d^3 - 3d + 4)q^2}{2^{2n}} .$$

Proof. We follow a similar argument to the proof of Lemma 8 to compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. Let p_i^{enc} and p_i^{dec} be the probability that $\mathsf{Bad}_{\mathrm{enc}}^1$ and $\mathsf{Bad}_{\mathrm{dec}}^1$ occur for the first time in the i-th query, respectively. Then, we have the same equation as Eq. (12).

If the i-th query is encryption, we consider bad conditions in $\mathsf{Bad}_{\mathrm{enc}}^1$. Since $d \geq 3$, we have $d^2 - d + 2 > 3d - 2$ from $(d^2 - d + 2) - (3d - 2) = (d-2)^2 > 0$, i.e., $r = d^2 - d + 2$ is larger than $r = 3d - 2$ in Sect. 4.2.2. Therefore, for $r = d^2 - d + 2$, each probability of the conditions in $\mathsf{Bad}_{\mathrm{enc}}^1$ does not have a larger upper bound than the probability in Lemma 4. From Lemma 4, we have

$$\begin{aligned} p_i^{\mathrm{enc}} &\leq (i-1) \cdot \left(\frac{d^2 - d - 2}{2 \cdot 2^{2n}} + \frac{d-1}{2^{2n}} \cdot d + \frac{1}{2^{2n}} \cdot (d-1) \right) \\ &= (i-1) \cdot \frac{(d^2 - d - 2) + 2(d^2 - d) + 2(d-1)}{2 \cdot 2^{2n}} = (i-1) \cdot \frac{0.5(3d^2 - d - 4)}{2^{2n}} . \end{aligned}$$

If the i-th query is decryption, we consider bad conditions in $\mathsf{Bad}^1_{\mathrm{dec}}$. From Lemma 9, we have

$$p_i^{\mathrm{dec}} \le (i-1)\cdot\left(\frac{d^2-d-2}{2\cdot 2^{2n}}\cdot(d-1)+\frac{d-1}{2^{2n}}\cdot d+\frac{1}{2^{2n}}\right)$$
$$= (i-1)\cdot\frac{(d^3-2d^2-d+2)+2(d^2-d)+2}{2\cdot 2^{2n}} = (i-1)\cdot\frac{0.5(d^3-3d+4)}{2^{2n}}\,.$$

Here, since $d\ge 3$, we have $d^3-3d+4 > 3d^2-d-4$ from $(d^3-3d+4)-(3d^2-d-4) = (d-2)(d^2-d-4) > 0$. Therefore, p_i^{dec} in the case that i-th query is decryption has a larger upper bound than p_i^{enc} in the case that i-th query is encryption, and we have

$$\Pr[\Theta_{\mathcal{I}}\in\mathsf{T}_{\mathrm{bad}}] = \sum_{i\in\mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i\in\mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}} \le \sum_{i=2}^{q}\left((i-1)\cdot\frac{0.5(d^3-3d+4)}{2^{2n}}\right)$$
$$\le 0.5q^2\cdot\frac{0.5(d^3-3d+4)}{2^{2n}} = \frac{0.25(d^3-3d+4)q^2}{2^{2n}}\,,$$

as claimed in Lemma 10. □

5.3 Probability Ratio of Good Transcript

Here, we prove the following lemma regarding a good transcript $\theta\in\mathsf{T}_{\mathrm{good}}$.

Lemma 11. *For any $\theta\in\mathsf{T}_{\mathrm{good}}$, we have*

$$\frac{\Pr[\Theta_{\mathcal{R}}=\theta]}{\Pr[\Theta_{\mathcal{I}}=\theta]} \ge 1-\frac{0.5q^2}{2^{dn}}\,.$$

Proof. Let q_{e} and q_{d} be the number of times that the adversary $\mathcal{A}$ makes encryption and decryption queries, respectively, i.e., we have $q_{\mathrm{e}}+q_{\mathrm{d}}=q$.

In the real world, the interpolation probability $\Pr[\Theta_{\mathcal{R}}=\theta]$ of $\theta\in\mathsf{T}_{\mathrm{good}}$ is the probability that r TPRs $\widetilde{P}_1,\ldots,\widetilde{P}_r$ interpolate θ. For $x\in[1..r]$, let p^x_{all} denote the probability that $\widetilde{P}_x$ interpolates all the q input-tweak-output associated to the TRP, and let p_i^x denote the probability that $\widetilde{P}_x$ interpolates the input-tweak-output associated to the TRP in the i-th query, i.e., $p^x_{\mathrm{all}}=\prod_{i=1}^q p_i^x$. We remark that the probabilities are taken over the experiment in Fig. 8. We also let p^x_{e} (resp. p^x_{d}) denote the probability that $\widetilde{P}_x$ interpolates the q_{e} (resp. q_{d}) input-tweak-output associated to the TRP in the i-th query for any $i\in\mathcal{Q}_{\mathrm{e}}$ (resp. $i\in\mathcal{Q}_{\mathrm{d}}$). In other words, we let $p^x_{\mathrm{e}}=\prod_{i\in\mathcal{Q}_{\mathrm{e}}} p_i^x$ and $p^x_{\mathrm{d}}=\prod_{i\in\mathcal{Q}_{\mathrm{d}}} p_i^x$, and we thus have $p^x_{\mathrm{all}}=p^x_{\mathrm{e}}\cdot p^x_{\mathrm{d}}$. Therefore, for any $\theta\in\mathsf{T}_{\mathrm{good}}$, we have

$$\Pr[\Theta_{\mathcal{R}}=\theta] = \prod_{x=1}^{r} p^x_{\mathrm{all}} \ge \left(\prod_{x=1}^{r-d} p^x_{\mathrm{e}}\right)\cdot\left(\prod_{x=r-d+1}^{r}\frac{1}{2^{nq_{\mathrm{e}}}}\right)\cdot\left(\prod_{x=d+1}^{r} p^x_{\mathrm{d}}\right)\cdot\left(\prod_{x=1}^{d}\frac{1}{2^{nq_{\mathrm{d}}}}\right)$$
$$= \left(\prod_{x=1}^{r-d} p^x_{\mathrm{e}}\right)\cdot\left(\prod_{x=d+1}^{r} p^x_{\mathrm{d}}\right)\cdot\frac{1}{2^{dnq}}\,.$$

In the ideal world, the interpolation probability $\Pr[\Theta_{\mathcal{I}}=\theta]$ of $\theta\in\mathsf{T}_{\mathrm{good}}$ is the probability that the dn-bit random permutation π and simulated $r-d$ TRPs ($\widetilde{P}_1,\ldots,\widetilde{P}_{r-d}$ in encryption or $\widetilde{P}^{-1}_{d+1},\ldots,\widetilde{P}^{-1}_r$ in decryption) interpolate the relevant plaintext-ciphertext or input-tweak-output associated to it. Note that for simulated $\widetilde{P}_1,\ldots,\widetilde{P}_{r-d}$ in encryption (resp. $\widetilde{P}^{-1}_{d+1},\ldots,\widetilde{P}^{-1}_r$ in decryption), they generate the internal state with the same probability distribution as in the real world, and hence they have the same interpolation

probability as $p_{\mathrm{e}}^1, \ldots, p_{\mathrm{e}}^{r-d}$ (resp. $p_{\mathrm{d}}^{d+1}, \ldots, p_{\mathrm{d}}^r$), respectively. Therefore, for any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \left(\prod_{x=1}^{r-d} p_{\mathrm{e}}^x\right) \cdot \left(\prod_{x=d+1}^{r} p_{\mathrm{d}}^x\right) \cdot \left(\prod_{i=1}^{q} \frac{1}{2^{dn} - (i-1)}\right).$$

We now compute the ratio as

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq \prod_{i=1}^{q} \frac{2^{dn} - (i-1)}{2^{dn}} = \prod_{i=1}^{q} \left(1 - \frac{i-1}{2^{dn}}\right) \geq 1 - \sum_{i=2}^{q} \frac{i-1}{2^{dn}} \geq 1 - \frac{0.5q^2}{2^{dn}},$$

and we obtain Lemma 11. □

6 Provable Security of TBC-based Type-2 GFS

In this section, we prove SPRP security of $\mathcal{E}_{2,d,r}$, TBC-based type-2 GFS, where we use $rd/2$ independent (n,n)-TRPs.

Theorem 3 (TBC-based type-2 GFS, SPRP security)**.** *Fix $d \geq 4$, where d is even, and let $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}$ be $rd/2$ independent (n,n)-TRPs and $E = \mathcal{E}_{2,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}]$ be the TBC-based type-2 GFS. Then for any SPRP-adversary $\mathcal{A}$ that makes q queries, if $r = d$ rounds, we have*

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.25d^2q^2}{2^n} + \frac{0.25dq^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}, \tag{13}$$

and if $r = d + 2$, then we have

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.125d(d^2 + 3d - 4)q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}. \tag{14}$$

We obtain birthday-bound security of Eq. (13) from Lemma 13, Lemma 16, and the Coefficient-H technique (Lemma 1), and BBB security of Eq. (14) from Lemma 15, Lemma 16, and the Coefficient-H technique (Lemma 1).

We present the definition of the oracles in Sect. 6.1, the analysis of bad probabilities in Sect. 6.2, and the analysis of the interpolation probability in Sect. 6.3. The analysis of bad probabilities is divided into the analysis of case $r = d$ in Sect. 6.2.1 and case $r = d + 2$ in Sect. 6.2.2.

We consider real world oracles $\mathcal{R}, \mathcal{R}^{-1}$ and ideal world oracles $\mathcal{I}, \mathcal{I}^{-1}$. The adversary $\mathcal{A}$ is assumed to be deterministic, makes exactly q queries, does not repeat the same query, and does not make a redundant query.

6.1 Definition of the Oracles

The encryption oracle $\mathcal{R}$ in the real world is $\mathcal{E}_{2,d,r}$ that uses $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}$, and the decryption oracle $\mathcal{R}^{-1}$ is $\mathcal{E}_{2,d,r}^{-1}$. If the i-th query is a query for $\mathcal{R}$, then we generate internal states $S_i^{1,1}, \ldots, S_i^{r-2,d/2}$ with $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r-2,d/2}$, and ciphertexts with $\widetilde{P}_{r-1,1}, \ldots, \widetilde{P}_{r,d/2}$. If the i-th query is a query for $\mathcal{R}^{-1}$, then we generate internal states $S_i^{r-2,d/2}, \ldots, S_i^{1,1}$ with $\widetilde{P}_{r,d/2}^{-1}, \ldots, \widetilde{P}_{3,1}^{-1}$, and plaintexts with $\widetilde{P}_{2,d/2}^{-1}, \ldots, \widetilde{P}_{1,1}^{-1}$. Here, for each query $\mathcal{A}$ makes, we record $S_i^{1,1}, \ldots, S_i^{r-2,d/2}$ into S, and we give $\mathcal{A}$ the entire internal states S after it makes q queries. The algorithms of $\mathcal{R}$ and $\mathcal{R}^{-1}$ are presented in Fig. 11. See Fig. 13 for an example and the labeling convention.

Algorithm 7: Procedure of $\mathcal{R}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $(S_i^{-1,1}, S_i^{-1,2}, \ldots, S_i^{-1,d/2}) \leftarrow (M_i^d, M_i^2, M_i^4, \ldots, M_i^{d-2})$
2. $(S_i^{0,1}, S_i^{0,2}, \ldots, S_i^{0,d/2}) \leftarrow (M_i^1, M_i^3, \ldots, M_i^{d-1})$
3. **for** $x = 1, 2, \ldots, r$ **do**
   for $y = 1, 2, \ldots, d/2$ **do**
   $\ell \leftarrow (y \bmod d/2) + 1$
   $S_i^{x,y} \leftarrow \widetilde{P}_{x,y}(S_i^{x-1,y}, S_i^{x-2,\ell})$
4. $(C_i^2, C_i^4, \ldots, C_i^d) \leftarrow (S_i^{r-1,2}, S_i^{r-1,3}, \ldots, S_i^{r-1,d/2}, S_i^{r-1,1})$
5. $(C_i^1, C_i^3, \ldots, C_i^{d-1}) \leftarrow (S_i^{r,1}, S_i^{r,2}, \ldots, S_i^{r,d/2})$
6. **return** $C_i^{[1..d]}$
7. **for** $x = 1, 2, \ldots, r-2$ **do**
   $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{x,[1..d/2]}$

Algorithm 8: Procedure of $\mathcal{R}^{-1}$ for the i-th query
Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $M_i^{[1..d]} \in \{0,1\}^{dn}$

1. $(S_i^{r,1}, S_i^{r,2}, \ldots, S_i^{r,d/2}) \leftarrow (C_i^1, C_i^3, \ldots, C_i^{d-1})$
2. $(S_i^{r-1,1}, S_i^{r-1,2}, \ldots, S_i^{r-1,d/2}) \leftarrow (C_i^d, C_i^2, C_i^4, \ldots, C_i^{d-2})$
3. **for** $x = r, r-1, \ldots, 1$ **do**
   for $y = 1, 2, \ldots, d/2$ **do**
   $\ell \leftarrow (y \bmod d/2) + 1$
   $S_i^{x-2,\ell} \leftarrow \widetilde{P}_{x,y}^{-1}(S_i^{x-1,y}, S_i^{x,y})$
4. $(M_i^1, M_i^3, \ldots, M_i^{d-1}) \leftarrow (S_i^{0,1}, S_i^{0,2}, \ldots, S_i^{0,d/2})$
5. $(M_i^2, M_i^4, \ldots, M_i^d) \leftarrow (S_i^{-1,2}, S_i^{-1,3} \ldots, S_i^{-1,d/2}, S_i^{-1,1})$
6. **return** $M_i^{[1..d]}$
7. **for** $x = 1, 2, \ldots, r-2$ **do**
   $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{x,[1..d/2]}$

Figure 11: Definition of $\mathcal{R}$ and $\mathcal{R}^{-1}$ for the SPRP proof of $\mathcal{E}_{2,d,r}$. Initially, S is empty, and it is given to $\mathcal{A}$ after it makes all the q queries.

The encryption oracle $\mathcal{I}$ in the ideal world is the dn-bit random permutation π, and the decryption oracle $\mathcal{I}^{-1}$ is π^{-1}. For the i-th query, $\mathcal{I}$ and $\mathcal{I}^{-1}$ generate dummy internal states $S_i^{1,1}, \ldots, S_i^{r-2,d/2}$, and record them into S. After $\mathcal{A}$ makes q queries, S is given to $\mathcal{A}$. In $\mathcal{I}$, we simulate $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r-2,d/2}$ to generate the internal states that have the same probability distribution as in $\mathcal{R}$. In $\mathcal{I}^{-1}$, we simulate $\widetilde{P}_{r,d/2}^{-1}, \ldots, \widetilde{P}_{3,1}^{-1}$ to generate the internal states that have the same probability distribution as in $\mathcal{R}^{-1}$. The simulation uses the lazy-sampling, and the algorithms of $\mathcal{I}$ and $\mathcal{I}^{-1}$ are presented in Fig. 12.

Algorithm 9: Procedure of $\mathcal{I}$ for the i-th query
Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $C_i^{[1..d]} \in \{0,1\}^{dn}$

1. $C_i^{[1..d]} \leftarrow \pi(M_i^{[1..d]})$
2. $(S_i^{-1,1}, S_i^{-1,2}, \ldots, S_i^{-1,d/2}) \leftarrow (M_i^d, M_i^2, M_i^4, \ldots, M_i^{d-2})$
3. $(S_i^{0,1}, S_i^{0,2}, \ldots, S_i^{0,d/2}) \leftarrow (M_i^1, M_i^3, \ldots, M_i^{d-1})$
4. **for** $x = 1, 2, \ldots, r-2$ **do**
   for $y = 1, 2, \ldots, d/2$ **do**
   $\ell \leftarrow (y \bmod d/2) + 1$
   $\mathcal{S}_i^{x,y} \leftarrow \{S_j^{x,y} \mid j < i \wedge S_i^{x-1,y} = S_j^{x-1,y}\}$
   if $\exists j < i, (S_i^{x-2,\ell}, S_i^{x-1,y}) = (S_j^{x-2,\ell}, S_j^{x-1,y})$ **then** $S_i^{x,y} \leftarrow S_j^{x,y}$
   else $S_i^{x,y} \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{S}_i^{x,y}$
5. **return** $C_i^{[1..d]}$
6. **for** $x = 1, 2, \ldots, r-2$ **do**
   $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{x,[1..d/2]}$

Algorithm 10: Procedure of $\mathcal{I}^{-1}$ for the i-th query
Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $M_i^{[1..d]} \in \{0,1\}^{dn}$

1. $M_i^{[1..d]} \leftarrow \pi^{-1}(C_i^{[1..d]})$
2. $(S_i^{r,1}, S_i^{r,2}, \ldots, S_i^{r,d/2}) \leftarrow (C_i^1, C_i^3, \ldots, C_i^{d-1})$
3. $(S_i^{r-1,1}, S_i^{r-1,2}, \ldots, S_i^{r-1,d/2}) \leftarrow (C_i^d, C_i^2, C_i^4, \ldots, C_i^{d-2})$
4. **for** $x = r, r-1, \ldots, 3$ **do**
   for $y = 1, 2, \ldots, d/2$ **do**
   $\ell \leftarrow (y \bmod d/2) + 1$
   $\mathcal{S}_i^{x-2,\ell} \leftarrow \{S_j^{x-2,\ell} \mid j < i \wedge S_i^{x-1,y} = S_j^{x-1,y}\}$
   if $\exists j < i, (S_i^{x-1,y}, S_i^{x,y}) = (S_j^{x-1,y}, S_j^{x,y})$ **then** $S_i^{x-2,\ell} \leftarrow S_j^{x-2,\ell}$
   else $S_i^{x-2,\ell} \xleftarrow{\$} \{0,1\}^n \setminus \mathcal{S}_i^{x-2,\ell}$
5. **return** $M_i^{[1..d]}$
6. **for** $x = 1, 2, \ldots, r-2$ **do**
   $\mathsf{S} \leftarrow \mathsf{S} \parallel S_i^{x,[1..d/2]}$

Figure 12: Definition of $\mathcal{I}$ and $\mathcal{I}^{-1}$ for the SPRP proof of $\mathcal{E}_{2,d,r}$. Initially, S is empty, and it is given to $\mathcal{A}$ after it makes all the q queries.

6.2 Bad Transcript and Bad Probability

The adversary $\mathcal{A}$ receives all the internal states after making q queries, and the interaction between $\mathcal{A}$ and oracles can be summarized as the following transcript θ:

$$\theta = \left((M_1^{[1..d]}, C_1^{[1..d]}, S_1^{1,1}, \ldots, S_1^{r-2,d/2}), \ldots, (M_q^{[1..d]}, C_q^{[1..d]}, S_q^{1,1}, \ldots, S_q^{r-2,d/2})\right). \quad (15)$$

The adversary does not repeat a query, so we have $(M_i^1, \ldots, M_i^d) \neq (M_j^1, \ldots, M_j^d)$ and $(C_i^1, \ldots, C_i^d) \neq (C_j^1, \ldots, C_j^d)$ for any $1 \leq j < i \leq q$. For a transcript in Eq. (15), we define

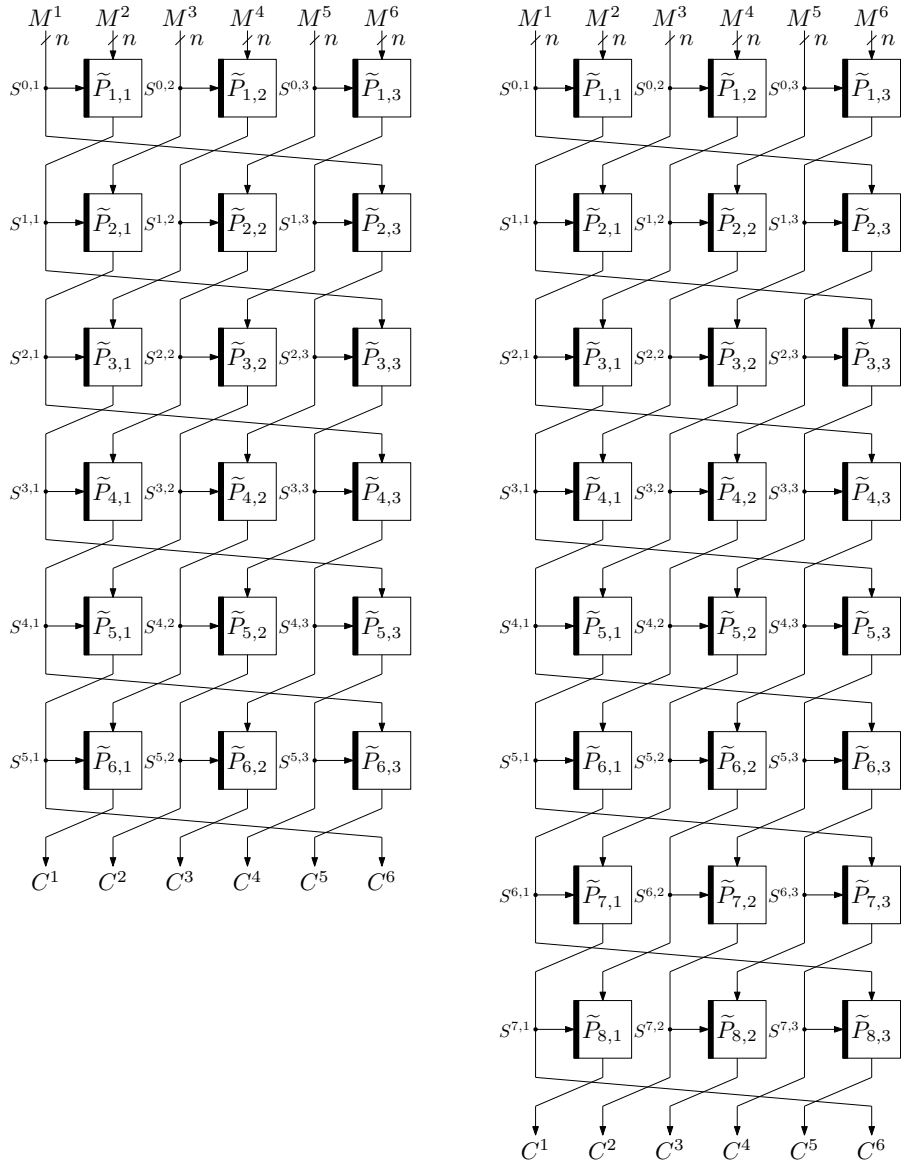

Figure 13: Left: $\mathcal{E}_{2,d,r}(M^1 \,\|\, \cdots \,\|\, M^6) = (C^1 \,\|\, \cdots \,\|\, C^6)$ for the case $d = 6$ and $r = 6$, where $(M^1 \,\|\, \cdots \,\|\, M^6) = (S^{0,1} \,\|\, S^{-1,2} \,\|\, S^{0,2} \,\|\, S^{-1,3} \,\|\, S^{0,3} \,\|\, S^{-1,1})$ and $(C^1 \,\|\, \cdots \,\|\, C^6) = (S^{6,1} \,\|\, S^{5,2} \,\|\, S^{6,2} \,\|\, S^{5,3} \,\|\, S^{6,3} \,\|\, S^{5,1})$. Right: $\mathcal{E}_{2,d,r}(M^1 \,\|\, \cdots \,\|\, M^6) = (C^1 \,\|\, \cdots \,\|\, C^6)$ for the case $d = 6$ and $r = 8$, where $(M^1 \,\|\, \cdots \,\|\, M^6) = (S^{0,1} \,\|\, S^{-1,2} \,\|\, S^{0,2} \,\|\, S^{-1,3} \,\|\, S^{0,3} \,\|\, S^{-1,1})$ and $(C^1 \,\|\, \cdots \,\|\, C^6) = (S^{8,1} \,\|\, S^{7,2} \,\|\, S^{8,2} \,\|\, S^{7,3} \,\|\, S^{8,3} \,\|\, S^{7,1})$.

two sets of indices to specify the direction of the queries:

$$\mathcal{Q}_{\mathrm{e}} = \{i \mid \text{the } i\text{-th query is an encryption query}\}$$
$$\mathcal{Q}_{\mathrm{d}} = \{i \mid \text{the } i\text{-th query is a decryption query}\}$$

We define bad transcripts following Sect. 4.2 and Sect. 5.2. In the ideal world, TRPs $\widetilde{P}_{x,y}$ that we simulate have the same input-tweak-output relation as in $\widetilde{P}_{x,y}$ in the real world. For an encryption query, for TRPs $\widetilde{P}_{r-1,1}, \ldots, \widetilde{P}_{r,d/2}$ that are not simulated in $\mathcal{I}$, there are conditions that hold only in the ideal world. Similarly, for a decryption query, for TRPs $\widetilde{P}^{-1}_{1,1}, \ldots, \widetilde{P}^{-1}_{2,d/2}$ that are not simulated in $\mathcal{I}^{-1}$, there are conditions that hold only in the ideal world. We use these conditions to define $\mathsf{T}_{\mathrm{bad}}$, the set of bad transcripts.

If the i-th query is an encryption query, for $y \in [1..d/2]$, we define the following bad conditions:

$$\begin{aligned}
\text{Bad at } \widetilde{P}_{r-1,y}: \ & (S_i^{r-3,y+1}, S_i^{r-2,y}) = (S_j^{r-3,y+1}, S_j^{r-2,y}) \wedge C_i^{2y-2} \neq C_j^{2y-2} \\
& \text{or } (S_i^{r-2,y}, C_i^{2y-2}) = (S_j^{r-2,y}, C_j^{2y-2}) \wedge S_i^{r-3,y+1} \neq S_j^{r-3,y+1} \\
\text{Bad at } \widetilde{P}_{r,y}: \ & (S_i^{r-2,y+1}, C_i^{2y-2}) = (S_j^{r-2,y+1}, C_j^{2y-2}) \wedge C_i^{2y-1} \neq C_j^{2y-1} \\
& \text{or } (C_i^{2y-2}, C_i^{2y-1}) = (C_j^{2y-2}, C_j^{2y-1}) \wedge S_i^{r-2,y+1} \neq S_j^{r-2,y+1}
\end{aligned}$$

Here, $C^0 = C^d$ for $y = 1$, and $S^{x,d/2+1} = S^{x,1}$ for $y = d/2$. These conditions can hold only in the ideal world, and in the real world, the probability of the corresponding transcript is zero. We let $\mathsf{Bad}^2_{\mathrm{enc}}$ be the set of all these conditions. Since $1 \leq j < i \leq q$, we have $\sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ possible combinations of i and j, and hence $\mathsf{Bad}^2_{\mathrm{enc}}$ includes:

- $d/2 \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions of a $2n$-bit collision between two internal state blocks, which we write $\mathsf{coll}_{\mathrm{s,s}}$,
- $d \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions of a $2n$-bit collision between one internal state block and one ciphertext block, which we write $\mathsf{coll}_{\mathrm{s,c}}$, and
- $d/2 \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions of a $2n$-bit collision between two ciphertext blocks, which we write $\mathsf{coll}_{\mathrm{c,c}}$.

In total, we have $2d \times \sum_{i \in \mathcal{Q}_{\mathrm{e}}}(i-1)$ possible conditions of $2n$-bit variables in $\mathsf{Bad}^2_{\mathrm{enc}}$. Note that i is in $\mathcal{Q}_{\mathrm{e}}$, while j can be in $\mathcal{Q}_{\mathrm{e}}$ or $\mathcal{Q}_{\mathrm{d}}$.

If the i-th query is a decryption query, for $y \in [1..d/2]$, we define the following bad conditions:

$$\begin{aligned}
\text{Bad at } \widetilde{P}_{1,y}: \ & (M_i^{2y-1}, M_i^{2y}) = (M_j^{2y-1}, M_j^{2y}) \wedge S_i^{1,y} \neq S_j^{1,y} \\
& \text{or } (M_i^{2y-1}, S_i^{1,y}) = (M_j^{2y-1}, S_j^{1,y}) \wedge M_i^{2y} \neq M_j^{2y} \\
\text{Bad at } \widetilde{P}_{2,y}: \ & (M_i^{2y+1}, S_i^{1,y}) = (M_j^{2y+1}, S_j^{1,y}) \wedge S_i^{2,y} \neq S_j^{2,y} \\
& \text{or } (S_i^{1,y}, S_i^{2,y}) = (S_j^{1,y}, S_j^{2,y}) \wedge M_i^{2y+1} \neq M_j^{2y+1}
\end{aligned}$$

Here, $M^{d+1} = M^1$ for $y = d/2$. These conditions can hold only in the ideal world, and in the real world, the probability of the corresponding transcript is zero. We let $\mathsf{Bad}^2_{\mathrm{dec}}$ be the set of all these conditions. Since $1 \leq j < i \leq q$, we have $\sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ possible combinations of i and j, and hence $\mathsf{Bad}^2_{\mathrm{dec}}$ includes:

- $d/2 \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions of a $2n$-bit collision between two internal state blocks, which we write $\mathsf{coll}_{\mathrm{s,s}}$,
- $d \times \sum_{i \in \mathcal{Q}_{\mathrm{d}}}(i-1)$ conditions of a $2n$-bit collision between one internal state block and one plaintext block, which we write $\mathsf{coll}_{\mathrm{s,m}}$, and

- $d/2 \times \sum_{i \in \mathcal{Q}_\mathrm{d}} (i-1)$ conditions of a $2n$-bit collision between two plaintext blocks, which we write $\mathsf{coll}_{\mathrm{m,m}}$.

In total, we have $2d \times \sum_{i \in \mathcal{Q}_\mathrm{d}} (i-1)$ possible conditions of $2n$-bit variables in $\mathsf{Bad}^2_{\mathrm{dec}}$. We note that $i \in \mathcal{Q}_\mathrm{d}$, while $j \in \mathcal{Q}_\mathrm{e} \cup \mathcal{Q}_\mathrm{d}$.

Now the set of bad transcripts $\mathsf{T}_{\mathrm{bad}}$ is defined as the set of all the attainable transcripts that satisfy at least one of the conditions in $\mathsf{Bad}^2_{\mathrm{enc}} \cup \mathsf{Bad}^2_{\mathrm{dec}}$. Formally, we define

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \theta \text{ satisfies at least one of the conditions in } \mathsf{Bad}^2_{\mathrm{enc}} \cup \mathsf{Bad}^2_{\mathrm{dec}}\}\,.$$

The set of good transcripts is defined as $\mathsf{T}_{\mathrm{good}} = \mathsf{T}_{\mathrm{all}} \setminus \mathsf{T}_{\mathrm{bad}}$.

In what follows, we evaluate the probability to have bad transcripts. We consider the case $r = d$ first, and then $r = d + 2$.

6.2.1 Bad Probability for $r = d$

Let $r = d$. For each of the conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$, we have the following lemma.

Lemma 12. *Let $r = d$, and consider one of the $2d \times \sum_{i \in \mathcal{Q}_\mathrm{e}} (i-1)$ conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$ in the ideal world. Then, the probability of the condition is at most $(d-2)/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $1/2^n$ if it is in $\mathsf{coll}_{\mathrm{s,c}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{c,c}}$.*

Proof. We proceed as in the proof of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We analyze a condition in $\mathsf{coll}_{\mathrm{s,s}}$. All the conditions in $\mathsf{coll}_{\mathrm{s,s}}$ are collisions at $(S^{r-3,\ell}, S^{r-2,y})$ for $y \in [1..d/2]$ and $\ell = (y \bmod d/2) + 1$. From the symmetry in $\mathcal{E}_{2,d,r}$, each probability of the collision at $(S^{r-3,\ell}, S^{r-2,y})$ has the same upper bound. Here, we consider a collision at $(S^{r-3,2}, S^{r-2,1})$. For $r = d$, we evaluate

$$\begin{aligned} &\Pr[(S_i^{r-3,2}, S_i^{r-2,1}) = (S_j^{r-3,2}, S_j^{r-2,1}) \wedge C_i^d \neq C_j^d] \\ &\quad \leq \Pr[(S_i^{d-3,2}, S_i^{d-2,1}) = (S_j^{d-3,2}, S_j^{d-2,1})]\,. \end{aligned} \tag{16}$$

We first evaluate Eq. (16) when the plaintext difference is $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, where $\Delta M_{i,j}^2$ can take any difference. We then show that this gives us the upper bound on all the possible plaintext differences by showing that all other cases do not have a larger upper bound.

Now, for any $y \in [2..d/2]$, since we have $S^{1,y} = \widetilde{P}_{1,y}(M^{2y-1}, M^{2y})$ and from $M_i^{[3..d]} = M_j^{[3..d]}$, we must have $S_i^{1,y} = S_j^{1,y}$, i.e., $S_i^{1,[2..d/2]} = S_j^{1,[2..d/2]}$. From this and $S^{2,y} = \widetilde{P}_{2,y}(S^{1,y}, M^{2y+1})$ for any $y \in [2..d/2-1]$, we must have $S_i^{2,y} = S_j^{2,y}$, i.e., $S_i^{2,[2..d/2-1]} = S_j^{2,[2..d/2-1]}$. Furthermore, for any $y \in [2..d/2-1]$, we must have $S_i^{3,y} = S_j^{3,y}$ from $S^{3,y} = \widetilde{P}_{3,y}(S^{2,y}, S^{1,y+1})$. Similarly, for $\ell = \lceil (x-1)/2 \rceil$, $x \in [3..d-3]$ and $y \in [2..d/2-\ell]$, we must have $S_i^{x,y} = S_j^{x,y}$ from the fact that we always have collisions at the tweak block $S^{x-1,y}$ and the input block $S^{x-2,y+1}$ of $S^{x,y} = \widetilde{P}_{x,y}(S^{x-1,y}, S^{x-2,y+1})$. Therefore, we have $S_i^{[1..d-3],2} = S_j^{[1..d-3],2}$ and $\Pr[S_i^{d-3,2} = S_j^{d-3,2}] = 1$.

Next, the probability of a collision at $S^{1,1} = \widetilde{P}_{1,1}(M^1, M^2)$ is $\Pr[S_i^{1,1} = S_j^{1,1}] = 1/2^n$, since $M_i^1 \neq M_j^1$. From $M_i^3 = M_j^3$, the probability of a collision at $S^{2,1} = \widetilde{P}_{2,1}(S^{1,1}, M^3)$ is

$$\begin{aligned} \Pr[S_i^{2,1} = S_j^{2,1}] &= \Pr[S_i^{1,1} = S_j^{1,1}] + \Pr[S_i^{1,1} \neq S_j^{1,1}] \cdot \Pr[S_i^{2,1} = S_j^{2,1} \mid S_i^{1,1} \neq S_j^{1,1}] \\ &\leq \Pr[S_i^{1,1} = S_j^{1,1}] + \frac{1}{2^n} = \frac{2}{2^n}\,. \end{aligned}$$

Similarly, for any $x \in [3..d-2]$, since we have $S^{x,1} = \widetilde{P}_{x,1}(S^{x-1,1}, S^{x-2,2})$ and from $S_i^{[1..d-4],2} = S_j^{[1..d-4],2}$, if $S_i^{x-1,1} = S_j^{x-1,1}$, then we must have $S_i^{x,1} = S_j^{x,1}$. Therefore, for each $x \in [2..d-2]$, we have

$$\begin{aligned}
&\Pr[S_i^{x,1} = S_j^{x,1}] \\
&\quad = \Pr[S_i^{x-1,1} = S_j^{x-1,1}] + \Pr[S_i^{x-1,1} \neq S_j^{x-1,1}] \cdot \Pr[S_i^{x,1} = S_j^{x,1} \mid S_i^{x-1,1} \neq S_j^{x-1,1}] \\
&\quad \leq \Pr[S_i^{x-1,1} = S_j^{x-1,1}] + \frac{1}{2^n} \leq \Pr[S_i^{1,1} = S_j^{1,1}] + \sum_{\ell=2}^{x} \frac{1}{2^n} = \frac{x}{2^n}\,.
\end{aligned}$$

Therefore, from $\Pr[S_i^{d-3,2} = S_j^{d-3,2}] = 1$, we obtain

$$\text{Eq. (16)} = \Pr[(S_i^{d-3,2}, S_i^{d-2,1}) = (S_j^{d-3,2}, S_j^{d-2,1})] \leq \Pr[S_i^{d-2,1} = S_j^{d-2,1}] \leq \frac{d-2}{2^n}\,,$$

and this gives us an upper bound $(d-2)/2^n$ on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, and $\Delta M_{i,j}^2$ is any difference.

We next prove that this is the upper bound for all other plaintext differences by showing that any other plaintext difference does not have a larger upper bound. Observe that the event $(S_i^{d-3,2}, S_i^{d-2,1}) = (S_j^{d-3,2}, S_j^{d-2,1})$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,s}}$ in the proof of Lemma 2.

(C-7) First, let us assume that $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} \neq 0$, namely, for some $x \in [3..d]$, we have $\Delta M_{i,j}^x \neq 0$, where there may be multiple indices of x. If $x = 3$, we have $\Pr[S_i^{2,1} = S_j^{2,1}] \leq 1/2^n$ from $S^{2,1} = \widetilde{P}_{2,1}(S^{1,1}, M^3)$, and hence the probability would be smaller. If $x \in [4..d]$, the event $S_i^{[1..d-3],2} = S_j^{[1..d-3],2}$ would be a probabilistic event. Therefore, we have $\Pr[S_i^{d-3,2} = S_j^{d-3,2}] < 1$, and hence the probability would be smaller.

(C-8) Next, consider the case $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0$. From $S^{1,1} = \widetilde{P}_{1,1}(M^1, M^2)$, we must have $S_i^{1,1} \neq S_j^{1,1}$. Now if we further assume that $\Delta M_{i,j}^{[3..d]} = 0$, we are back to the initial case of $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ starting from the second round, and the analysis corresponds to the one with a reduced round version that cannot have a larger collision probability. The case $\Delta M_{i,j}^{[3..d]} \neq 0$ would have a smaller upper bound as in the case (C-7).

(C-9) Finally, we consider the case $\Delta M_{i,j}^{[1,2]} = 0$, in which case we necessarily have $\Delta M_{i,j}^{[3..d]} \neq 0$. Consider the smallest index $x \in [3..d]$ such that $\Delta M_{i,j}^x \neq 0$. Then since $\Delta M_{i,j}^{[1..x-1]} = 0$, it has the same input difference as $\Delta M_{i,j}^1 \neq 0$ at input of the x-th round, and hence the final bound cannot be larger as in the analysis of the case (C-8). Note that if $x = d$, the input of the $(d-1)$-th round is the same input difference as $\Delta M_{i,j}^2 \neq 0$, i.e., $\Pr[S_i^{d-3,2} = S_j^{d-3,2}] = 0$.

Therefore, the case $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, where $\Delta M_{i,j}^2$ is any difference, maximizes Eq. (16) and the corresponding upper bound $(d-2)/2^n$ is the upper bound for all the cases in $\mathsf{coll}_{\mathrm{s,s}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. Next, we consider a condition in $\mathsf{coll}_{\mathrm{s,c}}$. All the conditions in $\mathsf{coll}_{\mathrm{s,c}}$ are collisions between $S^{r-2,y}$ and a ciphertext block for $y \in [1..d/2]$. From the symmetry in $\mathcal{E}_{2,d,r}$ and since ciphertexts are computed with the dn-bit random permutation π in the ideal world, each probability of the collisions between $S^{r-2,y}$ and a ciphertext block

has the same upper bound. Here, we consider a collision at $(S^{r-2,2}, C^2)$. For $r = d$, we evaluate

$$\begin{aligned}&\Pr[(S_i^{r-2,2}, C_i^2) = (S_j^{r-2,2}, C_j^2) \wedge S_i^{r-3,3} \neq S_j^{r-3,3}] \\ &\quad \leq \Pr[(S_i^{d-2,2}, C_i^2) = (S_j^{d-2,2}, C_j^2)]\,.\end{aligned} \tag{17}$$

We first compute the upper bound on Eq. (17) when the plaintext difference is $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$. We then show that this upper bound covers all other cases.

Now from $M_i^{[3..d]} = M_j^{[3..d]}$, for $y \in [2..d/2]$, we have $S_i^{1,y} = S_j^{1,y}$ since $S^{1,y} = \widetilde{P}_{1,y}(M^{2y-1}, M^{2y})$, i.e., $S_i^{1,[2..d/2]} = S_j^{1,[2..d/2]}$. Since $S^{1,1} = \widetilde{P}_{1,1}(M^1, M^2)$, we also have $S_i^{1,1} \neq S_j^{1,1}$ from $M_i^1 = M_j^1$ and $M_i^2 \neq M_j^2$. Therefore, the difference of the input $S^{1,1} \parallel M^3 \parallel \cdots \parallel S^{1,d/2} \parallel M^1$ to the second round is the same as the plaintext difference $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ in the analysis of $\mathsf{coll}_{\mathrm{s,s}}$. By adding a round at the beginning, $S^{x,y}$ in the analysis of $\mathsf{coll}_{\mathrm{s,s}}$ corresponds to $S^{x+1,y}$ in this analysis. With the same argument, we have $\Pr[S_i^{d-2,2} = S_j^{d-2,2}] = 1$.

In the ideal world, ciphertexts are obtained as the output of the dn-bit random permutation π. This implies that regardless of the plaintext difference, by following the computation in Eq. (5), we similarly have $\Pr[C_i^2 = C_j^2] \leq 1/2^n$. We thus have

$$\text{Eq. (17)} = \Pr[(S_i^{d-2,2}, C_i^2) = (S_j^{d-2,2}, C_j^2)] \leq \Pr[C_i^2 = C_j^2] \leq \frac{1}{2^n}\,,$$

when the ciphertext difference is $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$.

Next, we show that this upper bound covers all other cases. Since $\Pr[C_i^2 = C_j^2]$ does not depend on the plaintext difference, and we cannot have a larger probability than $\Pr[S_i^{d-2,2} = S_j^{d-2,2}] = 1$, the case $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ maximizes Eq. (17) and $1/2^n$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,c}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{c,c}}$. From the same analysis as in Eq. (6), the probability of a condition in $\mathsf{coll}_{\mathrm{c,c}}$ is at most $1/2^{2n}$. This completes the proof of Lemma 12. □

The correctness of Lemma 12 is experimentally verified in the range of $4 \leq d \leq 16$, where d is even. See Appendix A for more details.

We now present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = d$.

Lemma 13. *For $r = d$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{0.25d^2q^2}{2^n} + \frac{0.25dq^2}{2^{2n}}\,.$$

Proof. We compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. Let p_i^{enc} and p_i^{dec} be the probability that $\mathsf{Bad}_{\mathrm{enc}}^2$ and $\mathsf{Bad}_{\mathrm{dec}}^2$ occur for the first time in the i-th query, respectively. In other words, we assume that neither $\mathsf{Bad}_{\mathrm{enc}}^2$ nor $\mathsf{Bad}_{\mathrm{dec}}^2$ occurs before the i-th query, and compute p_i^{enc} and p_i^{dec}. Then, we have

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] = \sum_{i=2}^{q}(p_i^{\mathrm{enc}} + p_i^{\mathrm{dec}}) = \sum_{i \in \mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i \in \mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}}\,. \tag{18}$$

We note that $p_i^{\mathrm{enc}} = 0$ if $i \notin \mathcal{Q}_{\mathrm{e}}$ and $p_i^{\mathrm{dec}} = 0$ if $i \notin \mathcal{Q}_{\mathrm{d}}$.

If the i-th query is encryption, we consider bad conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$. Since $\mathsf{Bad}^2_{\mathrm{enc}}$ contains $d/2 \times \sum_{i\in\mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,s}}$, $d \times \sum_{i\in\mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{s,c}}$, and $d/2 \times \sum_{i\in\mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{coll}_{\mathrm{c,c}}$, and from Lemma 12, we have

$$p_i^{\mathrm{enc}} \le (i-1)\cdot\left(\frac{d-2}{2^n}\cdot\frac{d}{2}+\frac{1}{2^n}\cdot d+\frac{1}{2^{2n}}\cdot\frac{d}{2}\right) = (i-1)\cdot\left(\frac{0.5d^2}{2^n}+\frac{0.5d}{2^{2n}}\right). \tag{19}$$

If the i-th query is decryption, we consider bad conditions in $\mathsf{Bad}^2_{\mathrm{dec}}$. From the symmetry between the encryption and decryption in $\mathcal{E}_{2,d,r}$, each probability of the conditions in $\mathsf{Bad}^2_{\mathrm{dec}}$ has the same upper bound as in Lemma 12. Therefore, we follow a similar argument to the case that the i-th query is encryption, and we have the same upper bound of p_i^{dec} as Eq. (19).

Therefore, we have

$$\begin{aligned}\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &= \sum_{i\in\mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i\in\mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}} \le \sum_{i=2}^{q}\left((i-1)\cdot\left(\frac{0.5d^2}{2^n}+\frac{0.5d}{2^{2n}}\right)\right)\\ &\le 0.5q^2\cdot\left(\frac{0.5d^2}{2^n}+\frac{0.5d}{2^{2n}}\right) = \frac{0.25d^2q^2}{2^n}+\frac{0.25dq^2}{2^{2n}},\end{aligned}$$

and this shows the bound in Lemma 13. □

6.2.2 Bad Probability for $r = d + 2$

When $r = d + 2$, for each of the conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$, we have the following lemma.

Lemma 14. *Let $r = d + 2$, and consider one of the $2d \times \sum_{i\in\mathcal{Q}_{\mathrm{e}}}(i-1)$ conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$. Then, the probability of the condition is at most $(d^2-d-2)/(2\cdot 2^{2n})$ if it is in $\mathsf{coll}_{\mathrm{s,s}}$, at most $(d-1)/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{s,c}}$, and at most $1/2^{2n}$ if it is in $\mathsf{coll}_{\mathrm{c,c}}$.*

We proceed as in the proof of Lemma 2. We present a proof sketch below, and a full proof is presented in Appendix D.

Proof sketch. The overall structure of the proof is similar to that of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. For $\mathsf{coll}_{\mathrm{s,s}}$, we only consider a collision at $(S^{r-3,2}, S^{r-2,1})$ from the symmetry of $\mathcal{E}_{2,d,r}$. For $r = d + 2$, we evaluate

$$\Pr[(S_i^{r-3,2}, S_i^{r-2,1}) = (S_j^{r-3,2}, S_j^{r-2,1}) \wedge C_i^d \neq C_j^d] \le \Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1})].$$

We derive the upper bound $(d^2-d-2)/(2\cdot 2^{2n})$ on $\Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1})]$ when the plaintext difference is $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, where $\Delta M_{i,j}^{4}$ is any difference. Then, we show that this is the upper bound on all the possible plaintext differences by showing that other cases do not have a larger upper bound.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. For $\mathsf{coll}_{\mathrm{s,c}}$, we only consider a collision at $(S^{r-2,1}, C^d)$ from the symmetry of $\mathcal{E}_{2,d,r}$ and ciphertexts are computed with π in the ideal world. For $r = d + 2$, we evaluate

$$\Pr[(S_i^{r-2,1}, C_i^d) = (S_j^{r-2,1}, C_j^d) \wedge S_i^{r-3,2} \neq S_j^{r-3,2}] \le \Pr[(S_i^{d,1}, C_i^d) = (S_j^{d,1}, C_j^d)].$$

Then, we compute the upper bound $(d-1)/2^{2n}$ of $\Pr[(S_i^{d,1}, C_i^d) = (S_j^{d,1}, C_j^d)]$ when the plaintext difference is $\Delta M_{i,j}^{1} = 0 \wedge \Delta M_{i,j}^{2} \neq 0 \wedge \Delta M^{[3..d]} = 0$. We can show that this upper bound covers all other cases.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{c,c}}$. The analysis is the same as in Eq. (6), and we obtain the upper bound $1/2^{2n}$ for all the conditions in $\mathsf{coll}_{\mathrm{c,c}}$. □

We experimentally verified the correctness of Lemma 14 for $4 \leq d \leq 16$, where d is even. See Appendix A for more details.

We now present the upper bound on the probability of $\mathsf{T}_{\mathrm{bad}}$ for the case $r = d + 2$.

Lemma 15. *For $r = d + 2$, we have*

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \frac{0.125d(d^2 + 3d - 4)q^2}{2^{2n}}.$$

Proof. We follow a similar argument to the proof of Lemma 13 to compute the probability of $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. Let p_i^{enc} and p_i^{dec} be the probability that $\mathsf{Bad}^2_{\mathrm{enc}}$ and $\mathsf{Bad}^2_{\mathrm{dec}}$ occur for the first time in the i-th query, respectively. Then, we have the same equation as Eq. (18).

If the i-th query is encryption, we consider bad conditions in $\mathsf{Bad}^2_{\mathrm{enc}}$. From Lemma 14, we have

$$\begin{aligned} p_i^{\mathrm{enc}} &\leq (i-1) \cdot \left(\frac{d^2 - d - 2}{2 \cdot 2^{2n}} \cdot \frac{d}{2} + \frac{d-1}{2^{2n}} \cdot d + \frac{1}{2^{2n}} \cdot \frac{d}{2} \right) \\ &= (i-1) \cdot \frac{(d^3 - d^2 - 2d) + 4(d^2 - d) + 2d}{4 \cdot 2^{2n}} = (i-1) \cdot \frac{0.25d(d^2 + 3d - 4)}{2^{2n}}. \end{aligned} \tag{20}$$

If the i-th query is decryption, we consider bad conditions in $\mathsf{Bad}^2_{\mathrm{dec}}$. Since encryption and decryption are symmetrical in $\mathcal{E}_{2,d,r}$, each probability of the conditions in $\mathsf{Bad}^2_{\mathrm{dec}}$ has the same upper bound as in Lemma 14. Therefore, we follow a similar argument to the case that the i-th query is encryption, and we have the same upper bound of p_i^{dec} as Eq. (20).

Therefore, we have

$$\begin{aligned} \Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &= \sum_{i \in \mathcal{Q}_{\mathrm{e}}} p_i^{\mathrm{enc}} + \sum_{i \in \mathcal{Q}_{\mathrm{d}}} p_i^{\mathrm{dec}} \leq \sum_{i=2}^{q} \left((i-1) \cdot \frac{0.25d(d^2 + 3d - 4)}{2^{2n}} \right) \\ &\leq 0.5q^2 \cdot \frac{0.25d(d^2 + 3d - 4)}{2^{2n}} = \frac{0.125d(d^2 + 3d - 4)q^2}{2^{2n}}, \end{aligned}$$

as claimed in Lemma 15. □

6.3 Probability Ratio of Good Transcript

Here, we prove the following lemma regarding a good transcript $\theta \in \mathsf{T}_{\mathrm{good}}$.

Lemma 16. *For any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have*

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq 1 - \frac{0.5q^2}{2^{dn}}.$$

Proof. Let q_{e} and q_{d} be the number of times that the adversary $\mathcal{A}$ makes encryption and decryption queries, respectively, i.e., we have $q_{\mathrm{e}} + q_{\mathrm{d}} = q$.

In the real world, the interpolation probability $\Pr[\Theta_{\mathcal{R}} = \theta]$ of $\theta \in \mathsf{T}_{\mathrm{good}}$ is the probability that $rd/2$ TPRs $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}$ interpolate θ. For $x \in [1..r]$ and $y \in [1..d/2]$, let $p_{\mathrm{all}}^{x,y}$ denote the probability that $\widetilde{P}_{x,y}$ interpolates all the q input-tweak-output associated to the TRP, and let $p_i^{x,y}$ denote the probability that $\widetilde{P}_{x,y}$ interpolates the input-tweak-output associated to the TRP in the i-th query, i.e., $p_{\mathrm{all}}^{x,y} = \prod_{i=1}^{q} p_i^{x,y}$. We also let $p_{\mathrm{e}}^{x,y}$ (resp. $p_{\mathrm{d}}^{x,y}$) denote the probability that $\widetilde{P}_{x,y}$ interpolates the q_{e} (resp. q_{d}) input-tweak-output associated to the TRP in the i-th query for any $i \in \mathcal{Q}_{\mathrm{e}}$ (resp. $i \in \mathcal{Q}_{\mathrm{d}}$). In other words, we let

$p_{\mathrm{e}}^{x,y} = \prod_{i \in \mathcal{Q}_{\mathrm{e}}} p_i^{x,y}$ and $p_{\mathrm{d}}^{x,y} = \prod_{i \in \mathcal{Q}_{\mathrm{d}}} p_i^{x,y}$, and we thus have $p_{\mathrm{all}}^{x,y} = p_{\mathrm{e}}^{x,y} \cdot p_{\mathrm{d}}^{x,y}$. Therefore, for any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have

$$\begin{aligned}
\Pr[\Theta_{\mathcal{R}} = \theta] &= \prod_{x=1}^{r} \prod_{y=1}^{d/2} p_{\mathrm{all}}^{x,y} \\
&\geq \left(\prod_{x=1}^{r-2} \prod_{y=1}^{d/2} p_{\mathrm{e}}^{x,y} \right) \cdot \left(\prod_{x=r-1}^{r} \prod_{y=1}^{d/2} \frac{1}{2^{nq_{\mathrm{e}}}} \right) \cdot \left(\prod_{x=3}^{r} \prod_{y=1}^{d/2} p_{\mathrm{d}}^{x,y} \right) \cdot \left(\prod_{x=1}^{2} \prod_{y=1}^{d/2} \frac{1}{2^{nq_{\mathrm{d}}}} \right) \\
&= \left(\prod_{x=1}^{r-2} \prod_{y=1}^{d/2} p_{\mathrm{e}}^{x,y} \right) \cdot \left(\prod_{x=3}^{r} \prod_{y=1}^{d/2} p_{\mathrm{d}}^{x,y} \right) \cdot \frac{1}{2^{dnq}} \,.
\end{aligned}$$

In the ideal world, the interpolation probability $\Pr[\Theta_{\mathcal{I}} = \theta]$ of $\theta \in \mathsf{T}_{\mathrm{good}}$ is the probability that the dn-bit random permutation π and simulated $(r-2)d/2$ TRPs ($\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r-2,d/2}$ in encryption or $\widetilde{P}_{3,1}^{-1}, \ldots, \widetilde{P}_{r,d/2}^{-1}$ in decryption) interpolate the relevant plaintext-ciphertext or input-tweak-output associated to it. Note that for simulated $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r-2,d/2}$ in encryption (resp. $\widetilde{P}_{3,1}^{-1}, \ldots, \widetilde{P}_{r,d/2}^{-1}$ in decryption), they generate the internal state with the same probability distribution as in the real world, and hence they have the same interpolation probability as $p_{\mathrm{e}}^{1,1}, \ldots, p_{\mathrm{e}}^{r-2,d/2}$ (resp. $p_{\mathrm{d}}^{3,1}, \ldots, p_{\mathrm{d}}^{r,d/2}$), respectively. Therefore, for any $\theta \in \mathsf{T}_{\mathrm{good}}$, we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \left(\prod_{x=1}^{r-2} \prod_{y=1}^{d/2} p_{\mathrm{e}}^{x,y} \right) \cdot \left(\prod_{x=3}^{r} \prod_{y=1}^{d/2} p_{\mathrm{d}}^{x,y} \right) \cdot \left(\prod_{i=1}^{q} \frac{1}{2^{dn} - (i-1)} \right) .$$

We now compute the ratio as

$$\frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq \prod_{i=1}^{q} \frac{2^{dn} - (i-1)}{2^{dn}} = \prod_{i=1}^{q} \left(1 - \frac{i-1}{2^{dn}} \right) \geq 1 - \sum_{i=2}^{q} \frac{i-1}{2^{dn}} \geq 1 - \frac{0.5q^2}{2^{dn}} \,,$$

and we obtain Lemma 16. □

7 Provable Security of TBC-based Type-3 GFS

In this section, we show SPRP security of $\mathcal{E}_{3,d,r}$, TBC-based type-3 GFS, where we use $r(d-1)$ independent (n,n)-TRPs. Proposition 1 shows a relation between TBC-based type-3 GFS and TBC-based type-1 GFS. The corresponding equivalence is well known for PRF-based type-3 GFS and PRF-based type-1 GFS, and Proposition 1 shows that a similar equivalence holds for TBC-based counterparts as well. From Proposition 1 and the results in Sect. 5, we obtain Corollary 1 showing the SPRP security result of TBC-based type-3 GFSs.

Proposition 1. *Fix $d \geq 3$. Then the encryption round function $\Phi_{3,d}$ of TBC-based type-3 GFS is equivalent to the r-round decryption $\mathcal{E}_{1,d,r}^{-1}$ of TBC-based type-1 GFS, where $r = d-1$.*

A proof is elementary, and is presented in Appendix E. We now present our result on the security of TBC-based type-3 GFSs.

Corollary 1 (TBC-based type-3 GFS, SPRP security)**.** *Fix $d \geq 3$, and let $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d-1}$ be $r(d-1)$ independent (n,n)-TRPs and $E = \mathcal{E}_{3,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d-1}]$ be the TBC-based*

type-3 GFS. Then for any SPRP-adversary $\mathcal{A}$ that makes q queries, if $r = d$ rounds, we have

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.5(d^2-2d+2)q^2}{2^n} + \frac{0.5q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,, \tag{21}$$

and if $r = d+1$ rounds, we have

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) \leq \frac{0.25(d^3-3d+4)q^2}{2^{2n}} + \frac{0.5q^2}{2^{dn}}\,. \tag{22}$$

In Corollary 1, Eq. (21) shows birthday-bound security and is obtained from Proposition 1 and Eq. (7) in Theorem 2. From Proposition 1, $\mathcal{E}_{3,d,r}$ with $r = d$ rounds is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ with $r = d(d-1) = d^2 - d$ rounds, which is larger than the number of rounds in Eq. (7). Therefore, we obtain Eq. (21) from the bound in Theorem 2.

Similarly, Eq. (22) shows BBB security and is obtained from Proposition 1 and Eq. (8) in Theorem 2. Proposition 1 shows that $\mathcal{E}_{3,d,r}$ with $r = d+1$ rounds is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ with $r = (d+1)(d-1) = d^2 - 1$ rounds, which is larger than, or is equal to the number of rounds in Eq. (8).

8 Matching Attacks

In this section, we focus on distinguishing attacks to show the tightness of the bounds presented in Sect. 4–Sect. 7. More precisely, we consider birthday-bound security, and we present our analysis of TBC-based type-1 GFS, type-2 GFS, and type-3 GFS in Sect. 8.1, Sect. 8.2, and in Sect. 8.3, respectively. The attacks we present use $q = 2^{n/2}$ queries, and they show the tightness of our birthday-bound provable security results. Furthermore, let r_{bb} be the number of rounds that allows proving birthday-bound security, and r_{bbb} be the number of rounds that allows proving BBB security. Our attacks work for any number of rounds r such that $r_{\mathrm{bb}} \leq r < r_{\mathrm{bbb}}$ with the same complexity, implying that r_{bbb} is the optimal number of rounds for BBB security. We also point out that if the number of rounds satisfies $r < r_{\mathrm{bb}}$, then there is an efficient attack with $q = 2$ queries, implying that r_{bb} is the optimal number of rounds for birthday-bound security.

Table 2 shows the summary of our distinguishing attacks and security proofs. We note that the attack against TBC-based type-1 GFS showing the tightness of SPRP security is CCA, which is different from CPCA in that encryption queries are not used in the attack, and we observe a gap in the number of rounds needed for PRP security and SPRP security. This is due to the fact that the diffusion characteristic of TBC-based type-1 GFS in encryption and decryption is different. We will later elaborate on this point. We also observe that the number of rounds for PRP security of TBC-based type-2 GFS is the same as that for SPRP security, since the model of the attacks against type-2 GFS is CPA. Similarly, TBC-based type-3 GFS has the same characteristic. However, we remark that due to the equivalence between TBC-based type-1 and type-3 GFSs in Proposition 1, the diffusion of decryption of the latter is faster than encryption.

8.1 Attacks against TBC-based Type-1 GFS

We show a CPA birthday distinguisher against TBC-based type-1 GFS in Theorem 4, showing the tightness of Eq. (1) in Theorem 1. We also show a CCA birthday distinguisher in Theorem 5, showing the tightness of Eq. (7) in Theorem 2. See Fig. 14 for an example of the attacks against type-1 GFS.

Theorem 4 (TBC-based type-1 GFS, CPA birthday distinguisher)**.** *Fix $d \geq 3$, and let $\widetilde{P}_1, \ldots, \widetilde{P}_r$ be r independent (n,n)-TRPs, and consider TBC-based type-1 GFS $E =$*

Table 2: Summary of distinguishing attacks against TBC-based GFSs. "Const." is a dn-BC and "Security proof" shows the results in Sect. 4–Sect. 7, where r_{bb} (resp. r_{bbb}) denotes the number of rounds for birthday-bound security (resp. BBB security). In "Attack," (a) is for $r < r_{\mathrm{bb}}$, (b) is for $r_{\mathrm{bb}} \le r < r_{\mathrm{bbb}}$, "$O(1)$" denotes the constant time attacks with $q = 2$ queries, and "$O(2^{n/2})$" denotes the birthday attacks with $q = 2^{n/2}$ queries. Note that "CCA" is different from CPCA, namely, this distinguisher makes only decryption queries.

Const.	Security proof				Attack			
	Model	r_{bb}	r_{bbb}	Ref.	Model	(a)	(b)	Ref.
Type-1	PRP	$2d-2$	$3d-2$	Theorem 1	CPA	$O(1)$	$O(2^{n/2})$	Sect. 8.1
	SPRP	d^2-2d+2	d^2-d+2	Theorem 2	CCA	$O(1)$	$O(2^{n/2})$	
Type-2	SPRP	d	$d+2$	Theorem 3	CPA	$O(1)$	$O(2^{n/2})$	Sect. 8.2
Type-3	SPRP	d	$d+1$	Corollary 1	CPA	$O(1)$	$O(2^{n/2})$	Sect. 8.3

$\mathcal{E}_{1,d,r}[\widetilde{P}_1,\ldots,\widetilde{P}_r]$ *with* r *rounds, where* $2d-2 \le r < 3d-2$. *Then there exists an adversary* $\mathcal{A}$ *that makes* $q = 2^{n/2}$ *encryption queries and*

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \gtrapprox 0.5 - \exp(-0.5(d-1))\,.$$

For instance, we have $\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \ge 0.276$ when $d = 4$, and $\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \ge 0.469$ when $d = 8$.

Proof. We first present the procedure of our $\mathcal{A}$ for the case $r = 3d-3$:

1. Fix $q = 2^{n/2}$ plaintexts $M_1^{[1..d]},\ldots,M_q^{[1..d]}$ such that $\Delta M_{i,j}^{[1..d-1]} = 0 \wedge \Delta M_{i,j}^{d} \neq 0$ for any $1 \le j < i \le q$, and make q encryption queries.
2. If a collision is found among the q values of C_i^2, then output 1, else output 0.

In the real world, we have $S_i^{[1..d-2]} = S_j^{[1..d-2]}$ and $S_i^{d-1} \neq S_j^{d-1}$, since the plaintext difference satisfies $\Delta M_{i,j}^{[1..d-1]} = 0 \wedge \Delta M_{i,j}^{d} \neq 0$ and we have $S^1 = \widetilde{P}_1(M^1, M^2)$ and $S^x = \widetilde{P}_x(S^{x-1}, M^{x+1})$ for any $x \in [2..d-1]$. In other words, the input $S^{d-1} \,\|\, M^1 \,\|\, S^{[1..d-2]}$ of the d-th round has the same difference that gives the maximum collision probability of $\mathsf{coll}_{\mathrm{s,s}}$ analyzed in Lemma 2, which is $\Delta M_{i,j}^{1} \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$. Therefore, we analyze the probability to have a collision at C^2 by adding $(d-1)$ more rounds at the beginning, implying that $S^1,\ldots,S^{d-2}$ in the proof of Lemma 2 corresponds to $S^d,\ldots,S^{2d-3}$ in the attack.

We follow a similar argument to the proof of Lemma 2 to see that for any $x \in [d+1..2d-3]$, if $S_i^{x-1} = S_j^{x-1}$, then we have $S_i^{[x..2d-3]} = S_j^{[x..2d-3]}$. From $C^2 = \widetilde{P}_{2d-2}(S^{2d-3}, S^{d-2})$, if $S_i^{2d-3} = S_j^{2d-3}$, then we have $C_i^2 = C_j^2$. From the observations so far, we compute the collision probability at C^2 in the real world as follows:

$$\begin{aligned}
\Pr[\mathcal{A}^{\mathcal{R}} = 1] &= 1 - \Pr[\forall \Delta S_{i,j}^{d} \neq 0] \cdot \prod_{x=d+1}^{2d-2} \Pr\left[\forall \Delta S_{i,j}^{x} \neq 0 \;\middle|\; \bigwedge_{\ell=d}^{x-1} \forall \Delta S_{i,j}^{\ell} \neq 0\right] \\
&= 1 - \left(\prod_{i=2}^{q} \frac{2^n - (i-1)}{2^n}\right)^{1+(d-2)} = 1 - \left(\prod_{i=2}^{q}\left(1 - \frac{i-1}{2^n}\right)\right)^{d-1} \\
&\ge 1 - \left(\prod_{i=2}^{q} \exp\left(-\frac{i-1}{2^n}\right)\right)^{d-1} = 1 - \left(\exp\left(-\frac{0.5q(q-1)}{2^n}\right)\right)^{d-1} \\
&\approx 1 - \exp(-0.5(d-1))
\end{aligned} \tag{23}$$

Note that $\forall \Delta S^x_{i,j} \neq 0$ implies $\Delta S^x_{i,j} \neq 0$ for any $1 \leq j < i \leq q$. We also note that $S^{2d-2} = C^2$ when $r = 3d-3$.

On the other hand, in the ideal world, ciphertexts are obtained as the output of the dn-bit random permutation π. It follows that for any $a \in [1..d]$, a collision probability at C^a in the ideal world can be bounded as

$$\Pr[\mathcal{A}^{\mathcal{I}} = 1] \leq \sum_{i=2}^{q}((i-1) \cdot \Pr[C^a_i = C^a_j]) \leq 0.5q(q-1) \cdot \frac{1}{2^n} \leq \frac{0.5q^2}{2^n} = 0.5\,. \tag{24}$$

Therefore, we obtain the lower bound of the advantage as

$$\mathbf{Adv}^{\mathrm{prp}}_E(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{R}} = 1] - \Pr[\mathcal{A}^{\mathcal{I}} = 1]| \gtrapprox 0.5 - \exp(-0.5(d-1))\,.$$

Note that, in the real world, C^2 for $r = 3d-3$ corresponds to C^1 for $r = 2d-2$. In general, this corresponds to $C^{d-(x-1)}$ for $r = 2d-2+x$, where $x \in [1..d-2]$. Therefore, for $2d-2 \leq r < 3d-2$, the position of the ciphertext block to search for a collision changes, while the same attack procedure works for any case. □

Example 7. We show the real world of this attack in Fig. 14(b) for the case $d = 4$ and $r = 3d-3 = 9$. When $\Delta M^{[1..3]}_{i,j} = 0 \wedge \Delta M^4_{i,j} \neq 0$, we must have $S^{[1,2]}_i = S^{[1,2]}_j$ and $S^3_i \neq S^3_j$ from $S^1 = \widetilde{P}_1(M^1, M^2)$, $S^2 = \widetilde{P}_2(S^1, M^3)$, and $S^3 = \widetilde{P}_3(S^2, M^4)$. Therefore, since $S^4 = \widetilde{P}_4(S^3, M^1)$, $S^5 = \widetilde{P}_5(S^4, S^1)$, and $C^2 = \widetilde{P}_6(S^5, S^2)$, we also have

$$\Pr[C^2_i = C^2_j] \approx \Pr[S^5_i = S^5_j] + \frac{1}{2^n} \approx \Pr[S^4_i = S^4_j] + \frac{2}{2^n} \approx \frac{3}{2^n}\,,$$

i.e., the probability of a collision at C^2 is about $(d-1)$ times larger than the probability in the ideal world. The distinguisher uses this probability difference in the attack.

As shown in the proof above, when we make encryption queries with $\Delta M^{[1..d-1]}_{i,j} = 0 \wedge \Delta M^d_{i,j} \neq 0$, we always have $S^{d-2}_i = S^{d-2}_j$ in the real world. When $r = 2d-3$, since $S^{d-2} = C^2$, if we make two encryption queries with $\Delta M^{[1..d-1]}_{1,2} = 0 \wedge \Delta M^d_{1,2} \neq 0$, then we have $\Pr[C^2_2 = C^2_1] = 1$ in the real world. The analysis in the ideal world is the same as in Eq. (5), and we have $\Pr[C^2_2 = C^2_1] \leq 1/2^n$, allowing an efficient attack for any $r < 2d-2$ with $q = 2$ queries.

Example 8. See Fig. 14(a) for an example of this attack with $d = 4$ and $r = 2d-3 = 5$. If $\Delta M^{[1..3]}_{1,2} = 0 \wedge \Delta M^4_{1,2} \neq 0$, we have $S^1_2 = S^1_1$ from $S^1 = \widetilde{P}_1(M^1, M^2)$. Therefore, since $C^2 = \widetilde{P}_2(S^1, M^3)$, we always have $C^2_2 = C^2_1$, i.e., $\Pr[C^2_2 = C^2_1] = 1$.

We next present a CCA birthday distinguisher showing the tightness of Eq. (7) in Theorem 2.

Theorem 5 (TBC-based type-1 GFS, CCA birthday distinguisher)**.** *Fix $d \geq 3$, and let $\widetilde{P}_1, \ldots, \widetilde{P}_r$ be r independent (n,n)-TRPs, and consider TBC-based type-1 GFS $E = \mathcal{E}_{1,d,r}[\widetilde{P}_1, \ldots, \widetilde{P}_r]$ with r rounds, where $d^2 - 2d + 2 \leq r < d^2 - d + 2$. Then there exists an adversary $\mathcal{A}$ that makes $q = 2^{n/2}$ decryption queries and*

$$\mathbf{Adv}^{\mathrm{sprp}}_E(\mathcal{A}) \gtrapprox 0.5 - \exp(-0.5(d-1))\,.$$

We note that this distinguisher makes *only* decryption queries. We proceed as in the proof of Theorem 4. We present a proof sketch below, and a full proof is presented in Appendix F.

Proof sketch. First, we present the procedure of $\mathcal{A}$ for the case $r = d^2 - d + 1$:

1. Fix $q = 2^{n/2}$ ciphertexts $C_1^{[1..d]}, \ldots, C_q^{[1..d]}$ such that $\Delta C_{i,j}^1 \neq 0 \wedge \Delta C_{i,j}^{[2..d]} = 0$, and make q decryption queries.

2. If a collision is found among the q values of M_i^1, then output 1, else output 0.

In the real world, following the proof of Lemma 7 and by following the computation of Eq. (23), we can derive the lower bound to have a collision at M^1, and we obtain

$$\Pr[\mathcal{A}^{\mathcal{R},\mathcal{R}^{-1}} = 1] \gtrapprox 1 - \exp(-0.5(d-1)) .$$

In the ideal world, with the same argument as in Eq. (24) except that we use π^{-1} to compute plaintexts, we have $\Pr[\mathcal{A}^{\mathcal{I},\mathcal{I}^{-1}} = 1] \leq 0.5$, and we thus have

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{R},\mathcal{R}^{-1}} = 1] - \Pr[\mathcal{A}^{\mathcal{I},\mathcal{I}^{-1}} = 1]| \gtrapprox 0.5 - \exp(-0.5(d-1)) .$$

It is easy to show an attack with the same complexity for $d^2 - 2d + 2 \leq r < d^2 - d + 2$. See Appendix F for a full proof. □

Example 9. In Fig. 14(d), we present the real world of the attack for the case $d = 4$ and $r = d^2 - d + 1 = 13$. As shown in the figure, if $\Delta C_{i,j}^1 \neq 0 \wedge \Delta C_{i,j}^{[2..4]} = 0$, S^9 always has a non-zero difference and $S^{[4,7]}$ always has a zero difference, i.e., we have $S_i^9 \neq S_j^9$ and $S_i^{[4,7]} = S_j^{[4,7]}$. Therefore, since $S^6 = \widetilde{P}_{10}^{-1}(S^9, C^2)$, $S^3 = \widetilde{P}_7^{-1}(S^6, S^7)$, and $M^1 = \widetilde{P}_4^{-1}(S^3, S^4)$, we have

$$\Pr[M_i^1 = M_j^1] \approx \Pr[S_i^3 = S_j^3] + \frac{1}{2^n} \approx \Pr[S_i^6 = S_j^6] + \frac{2}{2^n} \approx \frac{3}{2^n} .$$

We see that a collision probability at M^1 is about $(d-1)$ times larger than the probability in the ideal world.

We note that it is straightforward to see that an attack with $q = 2$ queries is possible when $r < d^2 - 2d + 2$. Decryption queries with $\Delta C_{i,j}^1 \neq 0 \wedge \Delta C_{i,j}^{[2..d]} = 0$ yield $T_i^{d^2-3d+2} = T_j^{d^2-3d+2}$ in the real world. Since $T^{d^2-3d+2} = M^1$ when $r = d^2 - 2d + 1$, we have $\Pr[M_2^1 = M_1^1] = 1$ in the real world if we make two queries, while the same analysis as Eq. (5) shows $\Pr[M_2^1 = M_1^1] \leq 1/2^n$ in the ideal world.

Example 10. See Fig. 14(c) for an example of this attack with $d = 4$ and $r = d^2 - 2d + 1 = 9$. If $\Delta C_{1,2}^1 \neq 0 \wedge \Delta C_{1,2}^{[2..4]} = 0$, we have $S_2^{[3,4]} = S_1^{[3,4]}$ from $S^4 = \widetilde{P}_8^{-1}(C^3, C^4)$ and $S^3 = \widetilde{P}_7^{-1}(C^2, C^3)$. Therefore, since $M^1 = \widetilde{P}_4^{-1}(S^3, S^4)$, we always have $M_2^1 = M_1^1$, i.e., $\Pr[M_2^1 = M_1^1] = 1$.

Discussions. The result by Maurer, Pietrzak, and Renner shows that the composition $F \circ G^{-1}$ is CPCA secure[2] if F and G are non-adaptive CPA secure block ciphers [MPR07]. Given that TBC-based type-1 GFS is CPA secure with $O(d)$ rounds, one may hope that it is CPCA secure with $O(d)$ rounds. However, the security of TBC-based type-1 GFS is different depending on the direction of the operation. The diffusion in encryption direction is faster than decryption, and this explains the gap in the number of rounds for PRP and SPRP security in Table 2. This implies that the result in [MPR07] cannot be used directly, and indeed, as stated above, we have a distinguishing attack with $q = 2$ decryption queries for any number of rounds r such that $r < d^2 - 2d + 2$. See Fig. 14(c) for an

[2]Here, $F \circ G^{-1}$ means that we first apply F to a plaintext and then we apply G^{-1}, which is different from the order in Sect. 3.

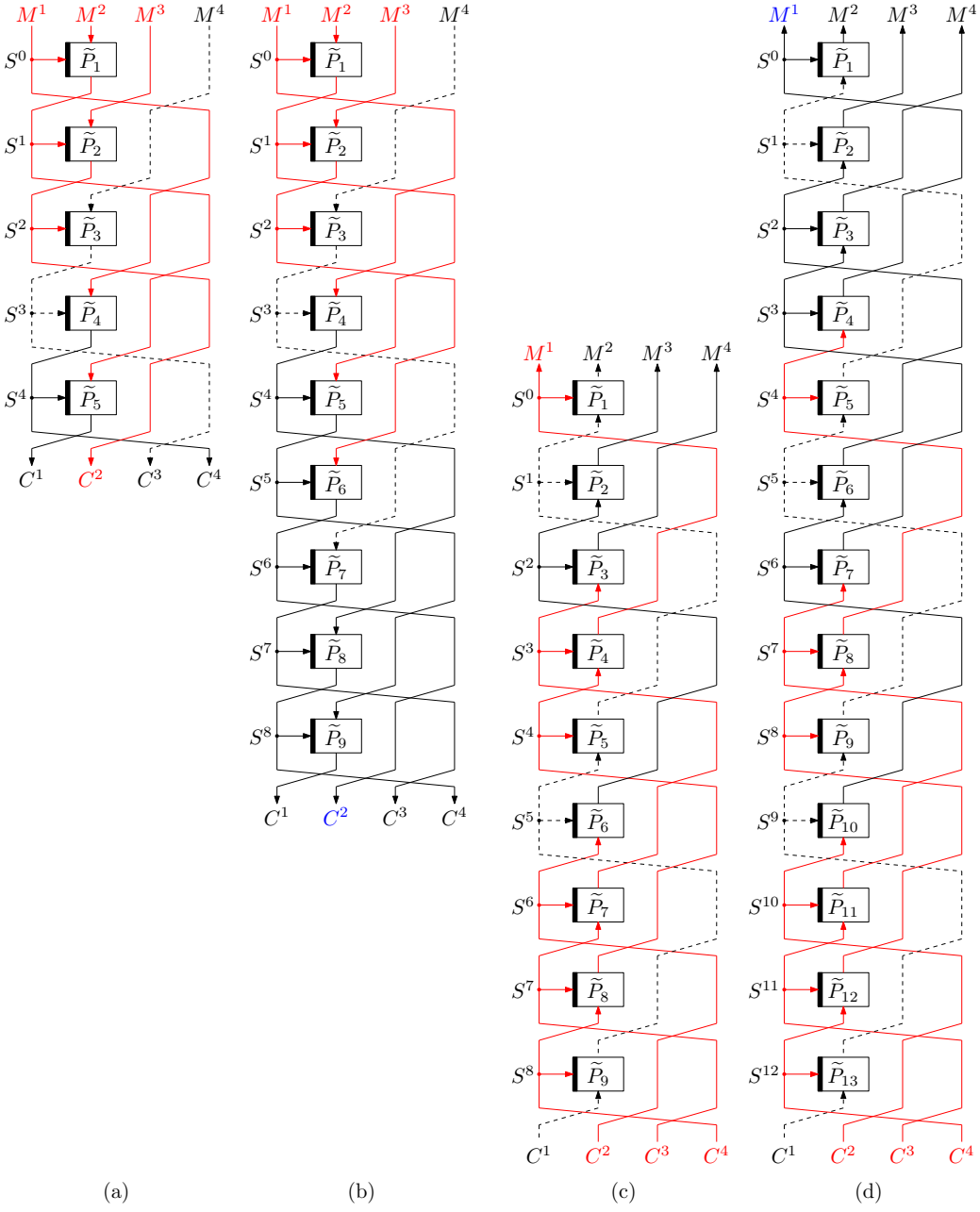

Figure 14: Examples of our attacks against TBC-based type-1 GFS with $d = 4$ (red: zero difference, dashed: non-zero difference, black: random difference, blue text: the target for finding a collision). (a) The constant CPA with $q = 2$ for $r = 2d - 3 = 5$. (b) The birthday CPA with $q = 2^{n/2}$ for $r = 3d - 3 = 9$. (c) The constant CCA with $q = 2$ for $r = d^2 - 2d + 1 = 9$. (d) The birthday CCA with $q = 2^{n/2}$ for $r = d^2 - d + 1 = 13$.

example. We note that the same observation was previously made for PRF-based type-1 GFS. See [HR10b, Page 5, Eratta].

While TBC-based type-1 GFS needs $O(d^2)$ rounds for CPCA security, we remark that the composition $F \circ F^{-1}$ has $O(d)$ rounds and is CPCA secure if F is non-adaptive CPA secure TBC-based type-1 GFS with $O(d)$ rounds. This implies that $F \circ F^{-1}$ has fewer rounds than TBC-based type-1 GFS for large d. For instance, we can use $(2d-2)$-round TBC-based type-1 GFS as F from Eq. (1) in Theorem 1. Then, $F \circ F^{-1}$ is CPCA secure with $4d-4$ rounds from [MPR07], where the middle round could be merged to further reduce the number of rounds. We remark that this construction $F \circ F^{-1}$ does not have an iterative structure, i.e., the linear layer of the first half F is the left cyclic shift and that of the second half F^{-1} is the right cyclic shift.

8.2 Attacks against TBC-based Type-2 GFS

We show a CPA birthday distinguisher against TBC-based type-2 GFS in Theorem 6, showing the tightness of Eq. (13) in Theorem 3.

Theorem 6 (TBC-based type-2 GFS, CPA birthday distinguisher)**.** *Fix $d \geq 4$, where d is even, and let $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}$ be $rd/2$ independent (n,n)-TRPs, and consider TBC-based type-2 GFS $E = \mathcal{E}_{2,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d/2}]$ with r rounds, where $d \leq r < d+2$. Then there exists an adversary $\mathcal{A}$ that makes $q = 2^{n/2}$ encryption queries and*

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \gtrapprox 0.5 - \exp(-0.5(d-1))\,.$$

We proceed as in the proof of Theorem 4. We present a proof sketch below, and a full proof is presented in Appendix G.

Proof sketch. We consider the case $r = d+1$, and our $\mathcal{A}$ works as follows:

1. Fix $q = 2^{n/2}$ plaintexts $M_1^{[1..d]}, \ldots, M_q^{[1..d]}$ such that $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ for any $1 \leq j < i \leq q$, and make q encryption queries.

2. If a collision is found among the q values of C_i^d, then output 1, else output 0.

In the real world, following the proof of Lemma 12 and by following the computation of Eq. (23), we can derive the lower bound to have a collision at C^d, and we obtain

$$\Pr[\mathcal{A}^{\mathcal{R}} = 1] \gtrapprox 1 - \exp(-0.5(d-1))\,.$$

In the ideal world, with the same argument as in Eq. (24), we have $\Pr[\mathcal{A}^{\mathcal{I},\mathcal{I}^{-1}} = 1] \leq 0.5$, and we thus have

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{R}} = 1] - \Pr[\mathcal{A}^{\mathcal{I}} = 1]| \gtrapprox 0.5 - \exp(-0.5(d-1))\,.$$

In the real world, C^d for $r = d+1$ corresponds to C^1 for $r = d$, and the attack works with the same complexity for the case $r = d$. □

In the real world, we have $S_i^{d-2,2} = S_j^{d-2,2}$ with encryption queries that satisfy $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$. If $r = d-1$, since $S^{d-2,2} = C^2$, we have $\Pr[C_2^2 = C_1^2] = 1$ in the real world, while we have $\Pr[C_2^2 = C_1^2] \leq 1/2^n$ following Eq. (5) in the ideal world, allowing an attack with $q = 2$ queries for any r with $r < d$.

Table 3: The number of TBC calls for TBC-based GFSs. "Const." is a dn-BC and "Model" shows the attack model. "# of parallel TBCs" shows the number of TBCs that can be processed in parallel for encryption (written as "Enc.") and decryption (written as "Dec."), and "time" shows the minimum processing time if the TBCs are processed in parallel. In the table, r_{bb} (resp. r_{bbb}) denotes the number of rounds for birthday-bound security (resp. BBB security), and t_{tbc} denotes the processing time of a single TBC.

		TBC calls		# of parallel TBCs			
Const.	Model	for $r = r_{\mathrm{bb}}$	for $r = r_{\mathrm{bbb}}$	Enc.	time	Dec.	time
Type-1	PRP	$2d-2$	$3d-2$	1	rt_{tbc}	$d-1$	$\lceil \frac{r}{d-1} \rceil t_{\mathrm{tbc}}$
	SPRP	d^2-2d+2	d^2-d+2				
Type-2	SPRP	$d^2/2$	$d^2/2+d$	$d/2$	rt_{tbc}	$d/2$	rt_{tbc}
Type-3	SPRP	d^2-d	d^2-1	$d-1$	rt_{tbc}	1	$r(d-1)t_{\mathrm{tbc}}$

8.3 Attacks against TBC-based Type-3 GFS

In Corollary 2, we show a CPA birthday distinguisher against TBC-based type-3 GFS, showing the tightness of Eq. (21) in Corollary 1.

Corollary 2 (TBC-based type-3 GFS, CPA birthday distinguisher)**.** *Fix $d \geq 3$, and let $\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d-1}$ be $r(d-1)$ independent (n,n)-TRPs, and consider TBC-based type-3 GFS $E = \mathcal{E}_{3,d,r}[\widetilde{P}_{1,1}, \ldots, \widetilde{P}_{r,d-1}]$ with r rounds, where $r = d$. Then there exists an adversary $\mathcal{A}$ that makes $q = 2^{n/2}$ encryption queries and*

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) \gtrapprox 0.5 - \exp(-0.5(d-1)) \,.$$

Corollary 2 is obtained from Proposition 1 and Theorem 5. From Proposition 1, $\mathcal{E}_{3,d,r}$ with $r = d$ is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ with $r = d(d-1) = d^2 - d$. Therefore, a similar attack to Theorem 5 works.

We also note that, from Proposition 1, $\mathcal{E}_{3,d,r}$ with $r = d-1$ is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ with $r = (d-1)^2 = d^2 - 2d + 1$, allowing an attack with $q = 2$ queries as shown in Sect. 8.1.

9 Conclusions

In this paper, we formalized TBC-based type-1, type-2, and type-3 GFSs, and presented their provable security treatments. We identified the number of rounds to achieve birthday-bound security and BBB security. We experimentally verified the correctness of our proofs in the range of $d \leq 16$. We also presented attacks to show the optimality of our results with respect to the number of rounds and attack complexity.

Regarding the efficiency comparison among the TBC-based GFSs we considered, we summarize the number of TBC calls in Table 3. If only encryption is needed, type-1 GFS is efficient since the number of TBC calls is the smallest among the three constructions. If we focus on SPRP security, type-2 GFS has the smallest number of TBC calls. For example, when $r = r_{\mathrm{bb}}$, the number of TBC calls for type-1/2/3 GFS is 10/8/12 with $d = 4$, and 50/32/56 with $d = 8$, respectively. Furthermore, for type-2 GFS, $d/2$ TBCs can be processed in parallel for both encryption and decryption, i.e., type-2 GFS can be made more efficient by parallel processing.

As open questions, we presented attacks with birthday complexity when $r_{\mathrm{bb}} \leq r < r_{\mathrm{bbb}}$, while we do not know if an attack with $q = O(2^n)$ complexity exists when $r \geq r_{\mathrm{bbb}}$. Also, as mentioned in Sect. 1, we leave the analysis with the coupling technique to obtain stronger security bounds by increasing the number of rounds as an interesting future work. This paper focuses on the indistinguishability notion, while indifferentiability [MRH04] of

TBC-based Feistel structure has been analyzed in [CDMS10, BNR21], and [NI20] shows indifferentiability of TBC-based unbalanced GFSs. It would be interesting to see the security of TBC-based type-1, type-2, and type-3 GFSs in this security notion.

Acknowledgments

The authors would like to thank the anonymous reviewers for helpful comments and Jooyoung Lee for shepherding the paper. This work was supported in part by JSPS KAKENHI Grant Number JP20K11675.

References

[AB96] Ross J. Anderson and Eli Biham. Two practical and provably secure block ciphers: BEARS and LION. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 113–120. Springer, 1996.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BLN18] Ritam Bhaumik, Eik List, and Mridul Nandi. ZCZ - achieving n-bit SPRP security with a minimal number of tweakable-block-cipher calls. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 336–366. Springer, 2018.

[BN15] Ritam Bhaumik and Mridul Nandi. An inverse-free single-keyed tweakable enciphering scheme. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 159–180. Springer, 2015.

[BNR21] Ritam Bhaumik, Mridul Nandi, and Anik Raychaudhuri. Improved indifferentiability security proof for 3-round tweakable luby-rackoff. *Des. Codes Cryptogr.*, 89(10):2255–2281, 2021.

[CDK+18] Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable security of (tweakable) block ciphers based on substitution-permutation networks. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 722–753. Springer, 2018.

[CDMS10] Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In Daniele Micciancio, editor, *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, volume 5978 of *Lecture Notes in Computer Science*, pages 273–289. Springer, 2010.

[CEL+21] Benoît Cogliati, Jordan Ethan, Virginie Lallemand, ByeongHak Lee, Jooyoung Lee, and Marine Minier. CTET+: A beyond-birthday-bound secure tweakable enciphering scheme using a single pseudorandom permutation. *IACR Trans. Symmetric Cryptol.*, 2021(4):1–35, 2021.

[CLMP17] Yu Long Chen, Atul Luykx, Bart Mennink, and Bart Preneel. Efficient length doubling from tweakable block ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(3):253–270, 2017.

[CMN18] Yu Long Chen, Bart Mennink, and Mridul Nandi. Short variable length domain extenders with beyond birthday bound security. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 244–274. Springer, 2018.

[CS06a] Debrup Chakraborty and Palash Sarkar. HCH: A new tweakable enciphering scheme using the hash-encrypt-hash approach. In Rana Barua and Tanja Lange, editors, *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*, volume 4329 of *Lecture Notes in Computer Science*, pages 287–302. Springer, 2006.

[CS06b] Debrup Chakraborty and Palash Sarkar. A new mode of encryption providing a tweakable strong pseudo-random permutation. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 293–309. Springer, 2006.

[CS14] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014.

[DN18] Avijit Dutta and Mridul Nandi. Tweakable HCTR: A BBB secure tweakable enciphering scheme. In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*, volume 11356 of *Lecture Notes in Computer Science*, pages 47–69. Springer, 2018.

[GM16] Shay Gueron and Nicky Mouha. Simpira v2: A family of efficient permutations using the AES round function. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 95–125, 2016.

[Hal04] Shai Halevi. Eme*: Extending EME to handle arbitrary-length messages with associated data. In Anne Canteaut and Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, pages 315–327. Springer, 2004.

[HR03] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer, 2003.

[HR04] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, volume 2964 of *Lecture Notes in Computer Science*, pages 292–304. Springer, 2004.

[HR10a] Viet Tung Hoang and Phillip Rogaway. On generalized feistel networks. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer, 2010.

[HR10b] Viet Tung Hoang and Phillip Rogaway. On generalized feistel networks. *IACR Cryptol. ePrint Arch.*, page 301, 2010.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2014.

[JNPS21] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. The deoxys AEAD family. *J. Cryptol.*, 34(3):31, 2021.

[LL18] ByeongHak Lee and Jooyoung Lee. Tweakable block ciphers secure beyond the birthday bound in the ideal cipher model. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 305–335. Springer, 2018.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[LRW11] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. *J. Cryptol.*, 24(3):588–613, 2011.

[Luc96] Stefan Lucks. Faster luby-rackoff ciphers. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 189–203. Springer, 1996.

[MF07] David A. McGrew and Scott R. Fluhrer. The security of the extended codebook (XCB) mode of operation. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers*, volume 4876 of *Lecture Notes in Computer Science*, pages 311–327. Springer, 2007.

[MI11] Kazuhiko Minematsu and Tetsu Iwata. Building blockcipher from tweakable blockcipher: Extending FSE 2009 proposal. In Liqun Chen, editor, *Cryptography and Coding - 13th IMA International Conference, IMACC 2011, Oxford, UK, December 12-15, 2011. Proceedings*, volume 7089 of *Lecture Notes in Computer Science*, pages 391–412. Springer, 2011.

[Min09] Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*, pages 308–326. Springer, 2009.

[Min15] Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. *Des. Codes Cryptogr.*, 74(3):645–663, 2015.

[MP03] Ueli M. Maurer and Krzysztof Pietrzak. The security of many-round luby-rackoff pseudo-random permutations. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 544–561. Springer, 2003.

[MPR07] Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2007.

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[NI19] Ryota Nakamichi and Tetsu Iwata. Iterative block ciphers from tweakable block ciphers with long tweaks. *IACR Trans. Symmetric Cryptol.*, 2019(4):54–80, 2019.

[NI20] Ryota Nakamichi and Tetsu Iwata. Beyond-birthday-bound secure cryptographic permutations from ideal ciphers with long keys. *IACR Trans. Symmetric Cryptol.*, 2020(2):68–92, 2020.

[NIS05] NIST. Secure hash standard (SHS). Federal Information Processing Standards Publication 180-4, 2005.

[NR99] Moni Naor and Omer Reingold. On the construction of pseudorandom permutations: Luby-rackoff revisited. *J. Cryptol.*, 12(1):29–66, 1999.

[Nyb96] Kaisa Nyberg. Generalized feistel networks. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, volume 1163 of *Lecture Notes in Computer Science*, pages 91–104. Springer, 1996.

[Pat98] Jacques Patarin. About feistel schemes with six (or more) rounds. In Serge Vaudenay, editor, *Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings*, volume 1372 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 1998.

[Pat03] Jacques Patarin. Luby-rackoff: 7 rounds are enough for $2^{n(1\text{-epsilon})}$security. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 513–529. Springer, 2003.

[Pat04] Jacques Patarin. Security of random feistel schemes with 5 or more rounds. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.

[Pat08] Jacques Patarin. The "Coefficients H" technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

[RRSY98] Ronald L. Rivest, Matthew J.B. Robshaw, Ray Sidney, and Yiqun Lisa Yin. The RC6 block cipher. Submission to NIST AES competition, 1998.

[Sar07] Palash Sarkar. Improving upon the TET mode of operation. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings*, volume 4817 of *Lecture Notes in Computer Science*, pages 180–192. Springer, 2007.

[Sar09] Palash Sarkar. Efficient tweakable enciphering schemes from (block-wise) universal hash functions. *IEEE Trans. Inf. Theory*, 55(10):4749–4760, 2009.

[SGW20] Yaobin Shen, Chun Guo, and Lei Wang. Improved security bounds for generalized feistel networks. *IACR Trans. Symmetric Cryptol.*, 2020(1):425–457, 2020.

[SK96] Bruce Schneier and John Kelsey. Unbalanced feistel networks and block cipher design. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 121–144. Springer, 1996.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov,

editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[ST13] Thomas Shrimpton and R. Seth Terashima. A modular framework for building variable-input-length tweakable ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 405–423. Springer, 2013.

[Vau03] Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptol.*, 16(4):249–286, 2003.

[WFW05] Peng Wang, Dengguo Feng, and Wenling Wu. HCTR: A variable-input-length enciphering mode. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology, First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings*, volume 3822 of *Lecture Notes in Computer Science*, pages 175–188. Springer, 2005.

[ZMI89] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer, 1989.

A Program for Bad Probability

In the proofs of Lemmas 2, 4, 7, 9, 12, and 14, a collision probability of conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$, $\mathsf{Bad}^1_{\mathrm{dec}}$, and $\mathsf{Bad}^2_{\mathrm{enc}}$ depend only on whether each block in a plaintext or a ciphertext chosen by $\mathcal{A}$ has a non-zero difference or not. Since $M_i^{[1..d]} \neq M_j^{[1..d]}$ and $C_i^{[1..d]} \neq C_j^{[1..d]}$ hold, there are $(2^d - 1)$ possible ways for $\mathcal{A}$ to choose the plaintext/ciphertext difference. The number of possibility exponentially grows as a function of d, and we developed a program in order to verify the correctness of our results.

The program exhaustively computes the probability of all the conditions in $\mathsf{Bad}^1_{\mathrm{enc}}$, $\mathsf{Bad}^1_{\mathrm{dec}}$, and $\mathsf{Bad}^2_{\mathrm{enc}}$ for all the $(2^d - 1)$ possible choices of plaintext/ciphertext difference, and outputs, for each of the condition, the maximum probability and the corresponding plaintext/ciphertext difference that gives the maximum probability. That is, for each $\mathtt{State} \in \mathsf{Bad}^1_{\mathrm{enc}}$, we are interested in deriving

$$\mathtt{MaxProb} = \max \left\{ \mathtt{Prob}(\Delta M^{[1..d]}, \mathtt{State}) \;\middle|\; \Delta M^{[1..d]} \in \{0,1\}^d \setminus \{0^d\} \right\}, \tag{25}$$

and we are also interested in the plaintext difference $\mathtt{MaxDiff} = \Delta M^{[1..d]}$ that gives $\mathtt{MaxProb}$, where $\mathtt{Prob}(\Delta M^{[1..d]}, \mathtt{State})$ denotes the probability to have an output difference in $\mathtt{State}$ given the plaintext difference $\Delta M^{[1..d]}$. We also would like to know $(\mathtt{MaxDiff}, \mathtt{MaxProb})$ for $\mathtt{State} \in \mathsf{Bad}^1_{\mathrm{dec}}$ and $\mathtt{State} \in \mathsf{Bad}^2_{\mathrm{enc}}$. An overview of our program is presented in Algorithm 11 in Fig. 15. The program faithfully computes Eq. (25).

For example, with $d = 4$, $r = 10$, and $\mathtt{Type} = \mathsf{Bad}^1_{\mathrm{enc}}$, $\mathsf{Bad}^1_{\mathrm{enc}}$ consists of eight conditions: $\Delta S^3 \parallel \Delta S^6 = 00$, $\Delta S^6 \parallel \Delta C^2 = 00$, $\Delta S^4 \parallel \Delta C^2 = 00$, $\Delta C^2 \parallel \Delta C^3 = 00$, $\Delta S^5 \parallel \Delta C^3 = 00$, $\Delta C^3 \| \Delta C^4 = 00$, $\Delta S^6 \| \Delta C^4 = 00$, and $\Delta C^4 \| \Delta C^1 = 00$. Our program treats $\Delta S^1, \ldots, \Delta S^6$ as random variables, and does not evaluate $\Delta C^1, \ldots, \Delta C^4$ as they are generated with a random permutation that has independent randomness allowing separate treatments. That

Algorithm 11: Program to compute the collision probability of bad conditions.

Input: $(d, r, \mathtt{Type})$
Output: $(\mathtt{MaxDiff}, \mathtt{MaxProb})$

1: $\mathtt{MaxDiff} \leftarrow$ empty
2: $\mathtt{MaxProb} \leftarrow 0$
3: **for** $\mathtt{State} \in \mathsf{Bad}^1_{\mathrm{enc}}$, $\mathsf{Bad}^1_{\mathrm{dec}}$, or $\mathsf{Bad}^2_{\mathrm{enc}}$ **do**
4: **for** $\Delta M^{[1..d]} \in \{0,1\}^d \setminus \{0^d\}$ **do** // $\Delta C^{[1..d]}$ for $\mathtt{State} \in \mathsf{Bad}^1_{\mathrm{dec}}$
5: $P \leftarrow \mathtt{Prob}(\Delta M^{[1..d]}, \mathtt{State})$
6: **if** $P > \mathtt{MaxProb}$ **then**
7: $\mathtt{MaxProb} \leftarrow P$
8: $\mathtt{MaxDiff} \leftarrow \Delta M^{[1..d]}$
9: **end if**
10: **end for** (Line 4)
11: **end for** (Line 3)
12: **return** $(\mathtt{MaxDiff}, \mathtt{MaxProb})$

Figure 15: Overview of our program to compute the collision probability of bad conditions. The input Type is used to specify $\mathsf{Bad}^1_{\mathrm{enc}}$, $\mathsf{Bad}^1_{\mathrm{dec}}$, or $\mathsf{Bad}^2_{\mathrm{enc}}$ in Line 3.

State	MaxDiff	MaxProb
$\Delta S^3 \,\|\|\, \Delta S^6 = 00$	1000	$5/2^{2n}$
$\Delta S^4 = 0$	0100	$3/2^n$
$\Delta S^5 = 0$	0010	$3/2^n$
$\Delta S^6 = 0$	0001	$3/2^n$

Figure 16: An example of the output of our program with $d = 4$, $r = 10$, and $\mathtt{Type} = \mathsf{Bad}^1_{\mathrm{enc}}$. MaxProb shows the leading terms only. Note that, for $\mathtt{Type} = \mathsf{Bad}^1_{\mathrm{enc}}$, $\Delta M^{[1..4]} = 1000$, 0100 and 0010 are equivalent to $\Delta M^{[1..4]} = 1100$, 0110 and 0011, respectively.

is, we evaluate the probabilities of $\Delta S^3 \,\|\, \Delta S^6 = 00$, $\Delta S^4 = 0$, $\Delta S^5 = 0$, and $\Delta S^6 = 0$. An example of the output of our program is in Fig. 16. See also Fig. 17 showing all the intermediate results to obtain Fig. 16.

The program was executed in the range of $d \leq 16$, and the result fully confirms the correctness of Lemmas 2, 4, 7, 9, 12, and 14 in this range.

B Proof of Lemma 4

We proceed as in the proof of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a condition in $\mathsf{coll}_{\mathrm{s,s}}$, which is a unique $2n$-bit collision at (S^{r-2d+1}, S^{r-d}). When $r = 3d - 2$, we have $S^{r-2d+1} = S^{d-1}$ and $S^{r-d} = S^{2d-2}$, and we therefore evaluate

$$\Pr[S_i^{[r-2d+1,r-d]} = S_j^{[r-2d+1,r-d]} \wedge C_i^2 \neq C_j^2] \leq \Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]}]\,. \tag{26}$$

We first evaluate Eq. (26) when the plaintext difference is $\Delta M^1_{i,j} \neq 0 \wedge \Delta M^{[3..d]}_{i,j} = 0$, where $\Delta M^2_{i,j}$ can take any difference. We then show that this gives us the upper bound on

$\Delta M^{[1..d]}$	$\Delta S^3 \parallel \Delta S^6 = 00$	$\Delta S^4 = 0$	$\Delta S^5 = 0$	$\Delta S^6 = 0$
0001	0	$1/2^n$	$2/2^n$	$3/2^n$
0010	0	$2/2^n$	$3/2^n$	$1/2^n$
0011	0	$2/2^n$	$3/2^n$	$1/2^n$
0100	$2/2^{2n}$	$3/2^n$	$1/2^n$	$1/2^n$
0101	$1/2^{2n}$	$2/2^n$	$1/2^n$	$1/2^n + 1/2^{3n}$
0110	$2/2^{2n}$	$3/2^n$	$1/2^n$	$1/2^n$
0111	$1/2^{2n}$	$2/2^n$	$1/2^n$	$1/2^n + 1/2^{3n}$
1000	$5/2^{2n}$	$1/2^n$	$1/2^n$	$1/2^n + 1/2^{2n}$
1001	$1/2^{2n}$	$1/2^n$	$1/2^n + 1/2^{3n}$	$1/2^n + 2/2^{2n}$
1010	$3/2^{2n}$	$1/2^n$	$1/2^n + 1/2^{3n}$	$1/2^n$
1011	$1/2^{2n}$	$1/2^n$	$1/2^n$	$1/2^n$
1100	$5/2^{2n}$	$1/2^n$	$1/2^n$	$1/2^n + 1/2^{2n}$
1101	$1/2^{2n}$	$1/2^n$	$1/2^n + 1/2^{3n}$	$1/2^n + 2/2^{2n}$
1110	$3/2^{2n}$	$1/2^n$	$1/2^n + 1/2^{3n}$	$1/2^n$
1111	$1/2^{2n}$	$1/2^n$	$1/2^n$	$1/2^n$

Figure 17: A table of $\mathtt{Prob}(\Delta M^{[1..d]}, \mathtt{State})$ with $d = 4$, $r = 10$, and $\mathtt{Type} = \mathsf{Bad}^1_{\mathrm{enc}}$. Only the upper bounds are shown, i.e., low order terms that do not contribute to the upper bound (e.g., terms with a negative coefficient) are neglected.

all the possible plaintext differences by showing that all other cases do not have a larger upper bound.

Now, from $M_i^1 \neq M_j^1$, the probability of a collision at $S^1 = \widetilde{P}_1(M^1, M^2)$ is $\Pr[S_i^1 = S_j^1] = 1/2^n$. Next, for any $x \in [2..d-1]$, since we have $S^x = \widetilde{P}_x(S^{x-1}, M^{x+1})$ and from $M_i^{[3..d]} = M_j^{[3..d]}$, if $S_i^{x-1} = S_j^{x-1}$, then we must have $S_i^{[x..d-1]} = S_j^{[x..d-1]}$. Therefore, for each $x \in [2..d-1]$, we have

$$\begin{aligned}\Pr[S_i^x = S_j^x] &= \Pr[S_i^{x-1} = S_j^{x-1}] + \Pr[S_i^{x-1} \neq S_j^{x-1}] \cdot \Pr[S_i^x = S_j^x \mid S_i^{x-1} \neq S_j^{x-1}] \\ &\leq \Pr[S_i^{x-1} = S_j^{x-1}] + \frac{1}{2^n} \leq \Pr[S_i^1 = S_j^1] + \sum_{\ell=2}^{x} \frac{1}{2^n} = \frac{x}{2^n}\,,\end{aligned}$$

and this yields $\Pr[S_i^2 = S_j^2] \leq 2/2^n$.

Assume that we have a collision at S^2, in which case $S_i^{[3..d-1]} = S_j^{[3..d-1]}$ holds. Recall that $M_i^1 \neq M_j^1$, and from $S^d = \widetilde{P}_d(S^{d-1}, M^1)$, we must have $S_i^d \neq S_j^d$. From this, the probability of a collision at $S^{d+1} = \widetilde{P}_{d+1}(S^d, S^1)$ is obtained as $\Pr[S_i^{d+1} = S_j^{d+1} \mid S_i^2 = S_j^2] = 1/2^n$. We also observe that for any $x \in [d+2..2d-2]$, if $S_i^{x-1} = S_j^{x-1}$, then we have $S_i^{[x..2d-2]} = S_j^{[x..2d-2]}$. This follows from the fact that $S_i^{[2..d-2]} = S_j^{[2..d-2]}$ holds, and for any $x \in [d+2..2d-2]$, S^{x-d} is the input block of $S^x = \widetilde{P}_x(S^{x-1}, S^{x-d})$. From the observation, for any $x \in [d+2..2d-2]$, we have

$$\begin{aligned}&\Pr[S_i^x = S_j^x \mid S_i^2 = S_j^2] \\ &\quad= \Pr[S_i^{x-1} = S_j^{x-1} \mid S_i^2 = S_j^2] \\ &\qquad+ \Pr[S_i^{x-1} \neq S_j^{x-1} \mid S_i^2 = S_j^2] \cdot \Pr[S_i^x = S_j^x \mid S_i^{x-1} \neq S_j^{x-1} \wedge S_i^2 = S_j^2] \\ &\quad\leq \Pr[S_i^{x-1} = S_j^{x-1} \mid S_i^2 = S_j^2] + \frac{1}{2^n} \\ &\quad\leq \Pr[S_i^{d+1} = S_j^{d+1} \mid S_i^2 = S_j^2] + \sum_{\ell=d+2}^{x} \frac{1}{2^n} = \frac{x-(d+1)+1}{2^n} = \frac{x-d}{2^n}\,.\end{aligned}$$

Therefore, from $\Pr[S_i^{d-1} = S_j^{d-1} \mid S_i^2 = S_j^2] = 1$, we obtain

$$\Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]} \mid S_i^2 = S_j^2] \le \frac{(2d-2)-d}{2^n} = \frac{d-2}{2^n}\,.$$

We proceed similarly for $\ell \in [3..d-1]$ as follows. We assume $S_i^{\ell-1} \neq S_j^{\ell-1}$ and we also assume that we have a collision at S^ℓ. Note that this step is non-existent when $d = 3$. Let us denote the assumption $S_i^{\ell-1} \neq S_j^{\ell-1} \wedge S_i^\ell = S_j^\ell$ by if_ℓ. Then, we have $S_i^{[\ell+1..d-1]} = S_j^{[\ell+1..d-1]}$, and from $S_i^{\ell-1} \neq S_j^{\ell-1}$ and $S^\ell = \widetilde{P}_\ell(S^{\ell-1}, S^{\ell-d})$, we have $\Pr[\mathsf{if}_\ell] \le 1/2^n$. We also observe that if $S_i^{\ell-1} \neq S_j^{\ell-1}$, from $S^{\ell+d-1} = \widetilde{P}_{\ell+d-1}(S^{\ell+d-2}, S^{\ell-1})$, a collision at $S^{\ell+d-1}$ is possible only if $S_i^{\ell+d-2} \neq S_j^{\ell+d-2}$. Therefore, we have

$$\Pr[S_i^{\ell+d-1} = S_j^{\ell+d-1} \mid \mathsf{if}_\ell] \le \Pr[S_i^{\ell+d-1} = S_j^{\ell+d-1} \mid S_i^{\ell+d-2} \neq S_j^{\ell+d-2}] = \frac{1}{2^n}\,.$$

Furthermore, for any $x \in [\ell+d..2d-2]$, if $S_i^{x-1} = S_j^{x-1}$, then $S_i^{[x..2d-2]} = S_j^{[x..2d-2]}$ holds. This follows from $S_i^{[\ell..d-2]} = S_j^{[\ell..d-2]}$, and S^{x-d} is the input block of $S^x = \widetilde{P}_x(S^{x-1}, S^{x-d})$. It follows that for any $x \in [\ell+d..2d-2]$, we have

$$\begin{aligned}
&\Pr[S_i^x = S_j^x \mid \mathsf{if}_\ell] \\
&\quad = \Pr[S_i^{x-1} = S_j^{x-1} \mid \mathsf{if}_\ell] + \Pr[S_i^{x-1} \neq S_j^{x-1} \mid \mathsf{if}_\ell] \cdot \Pr[S_i^x = S_j^x \mid S_i^{x-1} \neq S_j^{x-1} \wedge \mathsf{if}_\ell] \\
&\quad \le \Pr[S_i^{x-1} = S_j^{x-1} \mid \mathsf{if}_\ell] + \frac{1}{2^n} \\
&\quad \le \Pr[S_i^{\ell+d-1} = S_j^{\ell+d-1} \mid \mathsf{if}_\ell] + \sum_{m=\ell+d}^{x} \frac{1}{2^n} \le \frac{x-(\ell+d-1)+1}{2^n} = \frac{x-d-(\ell-2)}{2^n}\,.
\end{aligned}$$

From $\Pr[S_i^{d-1} = S_j^{d-1} \mid \mathsf{if}_\ell] = 1$, we obtain

$$\Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]} \mid \mathsf{if}_\ell] \le \frac{(2d-2)-d-(\ell-2)}{2^n} = \frac{d-\ell}{2^n}\,.$$

From all the observations above, we obtain the upper bound on Eq. (26) as

$$\begin{aligned}
\text{Eq. (26)} &= \Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]}] \\
&\le \Pr[S_i^2 = S_j^2] \cdot \Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]} \mid S_i^2 = S_j^2] \\
&\quad + \sum_{\ell=3}^{d-1} \left(\Pr[\mathsf{if}_\ell] \cdot \Pr[S_i^{[d-1,2d-2]} = S_j^{[d-1,2d-2]} \mid \mathsf{if}_\ell] \right) \\
&\le \frac{2}{2^n} \cdot \frac{d-2}{2^n} + \sum_{\ell=3}^{d-1} \left(\frac{1}{2^n} \cdot \frac{d-\ell}{2^n} \right) \\
&= \frac{2(d-2)}{2^{2n}} + \frac{1}{2^{2n}} \cdot \frac{((d-3)+1)(d-3)}{2} = \frac{d^2-d-2}{2 \cdot 2^{2n}}\,,
\end{aligned}$$

and we conclude that $(d^2-d-2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, where $\Delta M_{i,j}^2$ is any difference.

We next prove that the upper bound above is the upper bound for all other plaintext differences.

(C-10) First, let us assume that $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} \neq 0$, namely, for some $x \in [3..d]$, we have $\Delta M_{i,j}^x \neq 0$, where there may be multiple indices of x. If $x = 3$, we have

$\Pr[S_i^2 = S_j^2] \le 1/2^n$ from $S^2 = \widetilde{P}_2(S^1, M^3)$, and hence the probability would be smaller. If $x \in [4..d]$, then from $S^{x-1} = \widetilde{P}_{x-1}(S^{x-2}, M^x)$, even if we assume $S_i^{x-2} = S_j^{x-2}$, the event $S_i^{[x-1..d-1]} = S_j^{[x-1..d-1]}$ would be a probabilistic event. Therefore, for $\ell \in [3..d-2]$, we have $\Pr[S_i^{d-1} = S_j^{d-1} \mid S_i^2 = S_j^2 \vee \mathsf{if}_\ell] < 1$, and hence the probability would be smaller.

(C-11) Next, consider the case $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0$. In this case, we must have $S_i^1 \neq S_j^1$ from $S^1 = \widetilde{P}_1(M^1, M^2)$. Now if we further assume that $\Delta M_{i,j}^{[4..d]} = 0$, where $\Delta M_{i,j}^3$ can take any difference, we are back to the initial case of $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ starting from the second round, and the analysis corresponds to the one with a reduced round version that cannot have a larger collision probability. The case $\Delta M_{i,j}^{[4..d]} \neq 0$ would have a smaller upper bound as in the case (C-10).

(C-12) Finally, we consider the case $\Delta M_{i,j}^{[1,2]} = 0$, in which case we necessarily have $\Delta M_{i,j}^{[3..d]} \neq 0$. Consider the smallest index $x \in [3..d]$ such that $\Delta M_{i,j}^x \neq 0$. Then since $\Delta M_{i,j}^{[1..x-1]} = 0$, from $S^{x-1} = \widetilde{P}_{x-1}(S^{x-2}, M^x)$, we must have $S_i^{x-1} \neq S_j^{x-1}$. This implies that, at the input of the x-th round, it has the same input difference as $\Delta M_{i,j}^1 \neq 0$, and hence the final bound cannot be larger as in the analysis of the case (C-11).

Therefore, the case $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, where $\Delta M_{i,j}^2$ is any difference, maximizes Eq. (26) and $(d^2 - d - 2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. We next analyze a condition in $\mathsf{coll}_{\mathrm{s,c}}$. We consider a collision at (S^{r-2d+2}, C^2) that involves an internal state with the smallest index in the number of round, as a collision at other places cannot have a larger collision probability. Since $S^{r-2d+2} = S^d$ holds when $r = 3d - 2$, we evaluate

$$\Pr[(S_i^{r-2d+2}, C_i^2) = (S_j^{r-2d+2}, C_j^2) \wedge C_i^3 \neq C_j^3] \le \Pr[(S_i^d, C_i^2) = (S_j^d, C_j^2)]\,. \tag{27}$$

We first compute the upper bound on Eq. (27) when the plaintext difference is $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M^{[4..d]} = 0$, where $\Delta M_{i,j}^3$ is an arbitrary difference. We then show that this upper bound covers all other cases.

Now from $M_i^1 = M_j^1$ and $M_i^2 \neq M_j^2$, we have $S_i^1 \neq S_j^1$ since $S^1 = \widetilde{P}_1(M^1, M^2)$. It follows that a collision probability at $S^2 = \widetilde{P}_1(S^1, M^3)$ is $\Pr[S_i^2 = S_j^2] = 1/2^n$. It is easy to see that for any $x \in [3..d]$, if $S_i^{x-1} = S_j^{x-1}$, then $S_i^{[x..d]} = S_j^{[x..d]}$, since we have $S^x = \widetilde{P}_x(S^{x-1}, M^{x+1})$ and $S^d = \widetilde{P}_d(S^{d-1}, M^1)$, and we also have $M_i^{[4..d]} = M_j^{[4..d]}$ and $M_i^1 = M_j^1$. Therefore, for any $x \in [3..d]$,

$$\begin{aligned}\Pr[S_i^x = S_j^x] &= \Pr[S_i^{x-1} = S_j^{x-1}] + \Pr[S_i^{x-1} \neq S_j^{x-1}] \cdot \Pr[S_i^x = S_j^x \mid S_i^{x-1} \neq S_j^{x-1}] \\ &\le \Pr[S_i^{x-1} = S_j^{x-1}] + \frac{1}{2^n} \le \Pr[S_i^2 = S_j^2] + \sum_{\ell=3}^{x} \frac{1}{2^n} = \frac{x-1}{2^n}\,.\end{aligned}$$

In the ideal world, ciphertexts are computed with the dn-bit random permutation π, and thus for any plaintext difference, by following the computation in Eq. (5), we have $\Pr[C_i^2 = C_j^2] \le 1/2^n$. Given the analysis so far, we obtain the upper bound on Eq. (27) as

$$\text{Eq. (27)} = \Pr[(S_i^d, C_i^2) = (S_j^d, C_j^2)] = \Pr[S_i^d = S_j^d] \cdot \Pr[C_i^2 = C_j^2] \le \frac{d-1}{2^n} \cdot \frac{1}{2^n} = \frac{d-1}{2^{2n}}\,,$$

when the plaintext difference is $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[4..d]} = 0$, where $\Delta M^3_{i,j}$ is an arbitrary difference.

Next, we show that the upper bound above covers all other cases. Since $\Pr[C^2_i = C^2_j]$ does not depend on the plaintext difference, we focus on the analysis of $\Pr[S^d_i = S^d_j]$.

(C-13) First, consider the case $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[4..d]} \neq 0$. In this case, since $S^x = \widetilde{P}_x(S^{x-1}, M^{x+1})$ for $x \in [3..d-1]$, there exists a term $\Pr[S^{x-1}_i = S^{x-1}_j]$ that is not added to derive the upper bound on $\Pr[S^x_i = S^x_j]$, and hence the final probability would be smaller.

(C-14) Next, consider the case $\Delta M^{[1,2]}_{i,j} = 0$, which implies $\Delta M^{[3..d]}_{i,j} \neq 0$. For the smallest index $x \in [3..d]$ such that $\Delta M^x_{i,j} \neq 0$, the input of the $(x-1)$-th round is the same as $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0$, and hence this case corresponds to the analysis of the reduced round version by $(x-2)$ rounds, and this would result in the reduction on the number of terms added to the upper bound.

(C-15) Finally, assume that $\Delta M^1_{i,j} \neq 0$. Then from $S^d = \widetilde{P}_d(S^{d-1}, M^1)$, we have a collision at S^d only if $S^{d-1}_i \neq S^{d-1}_j$. We thus have $\Pr[S^d_i = S^d_j] \leq 1/2^n$, implying that the final bound would be smaller.

Therefore, the case $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[4..d]} = 0$ maximizes Eq. (27) and $(d-1)/2^{2n}$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,c}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{c,c}}$. From the same analysis as in Eq. (6), the probability of a condition in $\mathsf{coll}_{\mathrm{c,c}}$ is at most $1/2^{2n}$. This completes the proof of Lemma 4. □

C Proof of Lemma 9

Following the proof of Lemma 7, we write $\widetilde{P}'_1, \ldots, \widetilde{P}'_{r-d}$ for $\widetilde{P}^{-1}_r, \ldots, \widetilde{P}^{-1}_{d+1}$, i.e., for $x \in [d+1..r]$, we let $\widetilde{P}^{-1}_x(\cdot) = \widetilde{P}'_{r-x+1}(\cdot)$. Similarly, we write $T^1, \ldots, T^{r-d}$ for the internal states $S^{r-d}, \ldots, S^1$ that are computed with $\widetilde{P}^{-1}_r, \ldots, \widetilde{P}^{-1}_{d+1}$, respectively, i.e., we let $S^x = T^{r-d-x+1}$ for $x \in [1..r-d]$.

We proceed as in the proof of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,m}}$ and $\mathsf{coll}_{\mathrm{m,m}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a condition in $\mathsf{coll}_{\mathrm{s,s}}$. Among the conditions in $\mathsf{coll}_{\mathrm{s,s}}$, we focus on the analysis of (S^{d-1}, S^d) that involves an internal state with the largest index in the number of round, as a collision at other places cannot have a larger collision probability. When $r = d^2 - d + 2$, we have $S^{d-1} = T^{r-2d+2} = T^{d^2-3d+4}$, $S^d = T^{d^2-3d+3}$, and we therefore consider

$$\Pr[S^{[d-1,d]}_i = S^{[d-1,d]}_j \wedge M^1_i \neq M^1_j] \leq \Pr[T^{[d^2-3d+3,d^2-3d+4]}_i = T^{[d^2-3d+3,d^2-3d+4]}_j]. \quad (28)$$

We first evaluate Eq. (28) when the ciphertext difference is $\Delta C^{[2..d-1]}_{i,j} = 0 \wedge \Delta C^d_{i,j} \neq 0$, where $\Delta C^1_{i,j}$ can take any difference. We then show that this is the upper bound on all the possible ciphertext differences.

This ciphertext difference $\Delta C^{[2..d-1]}_{i,j} = 0 \wedge \Delta C^d_{i,j} \neq 0$ is the same ciphertext difference as $\mathsf{coll}_{\mathrm{s,s}}$ analyzed in the proof of Lemma 7. Therefore, we follow the same argument in the proof of Lemma 7, and we have $T^{[d-1..(d-3)(d-1):d-1]}_i = T^{[d-1..(d-3)(d-1):d-1]}_j$. Note that this deterministic collision at internal state blocks are non-existent when $d = 3$.

Now from $C_i^d \neq C_j^d$, the probability of a collision at $T^1 = \widetilde{P}'_1(C^d, C^1)$ is $\Pr[T_i^1 = T_j^1] = 1/2^n$. Next, for any $x \in [0..d-3]$, since we have $T^d = \widetilde{P}'_d(T^1, C^2), T^{x(d-1)+d} = \widetilde{P}'_{x(d-1)+d}(T^{x(d-1)+1}, T^{x(d-1)})$, $C_i^2 = C_j^2$, and $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$, if $T_i^{x(d-1)+1} = T_j^{x(d-1)+1}$, then we must have $T_i^{\ell(d-1)+d} = T_j^{\ell(d-1)+d}$ for $\ell \in [x..d-3]$. Therefore, for each $x \in [0..d-3]$, we have

$$\begin{aligned}
&\Pr[T_i^{x(d-1)+d} = T_j^{x(d-1)+d}] \\
&\quad = \Pr[T_i^{x(d-1)+1} = T_j^{x(d-1)+1}] + \Pr[T_i^{x(d-1)+1} \neq T_j^{x(d-1)+1}] \\
&\qquad \cdot \Pr[T_i^{x(d-1)+d} = T_j^{x(d-1)+d} \mid T_i^{x(d-1)+1} \neq T_j^{x(d-1)+1}] \\
&\quad \leq \Pr[T_i^{x(d-1)+1} = T_j^{x(d-1)+1}] + \frac{1}{2^n} \leq \Pr[T_i^1 = T_j^1] + \sum_{\ell=0}^{x} \frac{1}{2^n} = \frac{x+2}{2^n}
\end{aligned}$$

and this yields $\Pr[T_i^d = T_j^d] \leq 2/2^n$.

Assume that we have a collision at T^d, in which case $T_i^{\ell(d-1)+d} = T_j^{\ell(d-1)+d}$ holds for $\ell \in [1..d-3]$. In other words, from $(d-3)(d-1)+d = d^2-3d+3$, we have $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3} \mid T_i^d = T_j^d] = 1$. Since $T^2 = \widetilde{P}'_2(C^{d-1}, C^d)$, we have $T_i^2 \neq T_j^2$ from $C_i^{d-1} = C_j^{d-1}$ and $C_i^d \neq C_j^d$. It follows that a collision probability at $T^{d+1} = \widetilde{P}'_{d+1}(T^2, T^1)$ is $\Pr[T_i^{d+1} = T_j^{d+1}] = 1/2^n$. We also observe that for any $x \in [0..d-4]$, if $T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1}$, then we have $T_i^{\ell(d-1)+2d} = T_j^{\ell(d-1)+2d}$, where $\ell \in [x..d-4]$. This follows from the fact that $T_i^{[d..(d-4)(d-1)+d:d-1]} = T_j^{[d..(d-4)(d-1)+d:d-1]}$ holds, and for any $x \in [0..d-4]$, $T^{x(d-1)+d}$ is the input block of $T^{x(d-1)+2d} = \widetilde{P}'_{x(d-1)+2d}(T^{x(d-1)+d+1}, T^{x(d-1)+d})$. From the observation, for any $x \in [0..d-4]$, we have

$$\begin{aligned}
&\Pr[T_i^{x(d-1)+2d} = T_j^{x(d-1)+2d} \mid T_i^d = T_j^d] \\
&\quad = \Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1} \mid T_i^d = T_j^d] \\
&\qquad + \Pr[T_i^{x(d-1)+d+1} \neq T_j^{x(d-1)+d+1} \mid T_i^d = T_j^d] \\
&\qquad \cdot \Pr[T_i^{x(d-1)+2d} = T_j^{x(d-1)+2d} \mid T_i^{x(d-1)+d+1} \neq T_j^{x(d-1)+d+1} \wedge T_i^d = T_j^d] \\
&\quad \leq \Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1} \mid T_i^d = T_j^d] + \frac{1}{2^n} \\
&\quad \leq \Pr[T_i^{d+1} = T_j^{d+1} \mid T_i^d = T_j^d] + \sum_{\ell=0}^{x} \frac{1}{2^n} = \frac{x+2}{2^n},
\end{aligned}$$

i.e., we have $\Pr[T_i^{d^2-3d+4} = T_j^{d^2-3d+4} \mid T_i^d = T_j^d] \leq (d-2)/2^n$ from $(d-4)(d-1)+2d = d^2-3d+4$. Therefore, from $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3} \mid T_i^d = T_j^d] = 1$, we obtain

$$\Pr[T_i^{[d^2-3d+3, d^2-3d+4]} = T_j^{[d^2-3d+3, d^2-3d+4]} \mid T_i^d = T_j^d] \leq \frac{d-2}{2^n}.$$

We proceed similarly for $\ell \in [1..d-3]$ as follows. We assume $T_i^{\ell(d-1)+1} \neq T_j^{\ell(d-1)+1}$ and we also assume that we have a collision at $T^{\ell(d-1)+d}$. Note that this step is non-existent when $d = 3$. Let us denote the assumption $T_i^{\ell(d-1)+1} \neq T_j^{\ell(d-1)+1} \wedge T_i^{\ell(d-1)+d} = T_j^{\ell(d-1)+d}$ by if_ℓ. Then, we have $T_i^{m(d-1)+d} = T_j^{m(d-1)+d}$ for $m \in [\ell+1..d-3]$, and we also have $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3} \mid \mathsf{if}_\ell] = 1$ from $(d-3)(d-1)+d = d^2-3d+3$. From $T_i^{\ell(d-1)+1} \neq T_j^{\ell(d-1)+1}$ and $T^{\ell(d-1)+d} = \widetilde{P}'_{\ell(d-1)+d}(T^{\ell(d-1)+1}, T^{\ell(d-1)})$, we have

$\Pr[\mathsf{if}_\ell] \le 1/2^n$. We also observe that if $T_i^{\ell(d-1)+1} \neq T_j^{\ell(d-1)+1}$, from $T^{\ell(d-1)+d+1} = \widetilde{P}'_{\ell(d-1)+d+1}(T^{\ell(d-1)+2}, T^{\ell(d-1)+1})$, a collision at $T^{\ell(d-1)+d+1}$ is possible only if $T_i^{\ell(d-1)+2} \neq T_j^{\ell(d-1)+2}$. Therefore, we have

$$\begin{aligned}&\Pr[T_i^{\ell(d-1)+d+1} = T_j^{\ell(d-1)+d+1} \mid \mathsf{if}_\ell]\\ &\quad\le \Pr[T_i^{\ell(d-1)+d+1} = T_j^{\ell(d-1)+d+1} \mid T_i^{\ell(d-1)+2} \neq T_j^{\ell(d-1)+2}] = \frac{1}{2^n}\,.\end{aligned}$$

Furthermore, for any $x \in [\ell..d-4]$, if $T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1}$, then $T_i^{x(d-1)+2d} = T_j^{x(d-1)+2d}$, which follows from $T_i^{[\ell(d-1)+d..(d-4)(d-1)+d:d-1]} = T_j^{[\ell(d-1)+d..(d-4)(d-1)+d:d-1]}$, and $T^{x(d-1)+d}$ is the input block of $T^{x(d-1)+2d} = \widetilde{P}'_{x(d-1)+2d}(T^{x(d-1)+d+1}, T^{x(d-1)+d})$. It follows that for any $x \in [\ell..d-4]$, we have

$$\begin{aligned}&\Pr[T_i^{x(d-1)+2d} = T_j^{x(d-1)+2d} \mid \mathsf{if}_\ell]\\ &\quad= \Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1} \mid \mathsf{if}_\ell] + \Pr[T_i^{x(d-1)+d+1} \neq T_j^{x(d-1)+d+1} \mid \mathsf{if}_\ell]\\ &\qquad\cdot \Pr[T_i^{x(d-1)+2d} = T_j^{x(d-1)+2d} \mid T_i^{x(d-1)+d+1} \neq T_j^{x(d-1)+d+1} \wedge \mathsf{if}_\ell]\\ &\quad\le \Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1} \mid \mathsf{if}_\ell] + \frac{1}{2^n}\\ &\quad\le \Pr[T_i^{\ell(d-1)+d+1} = T_j^{\ell(d-1)+d+1} \mid \mathsf{if}_\ell] + \sum_{m=\ell}^{x} \frac{1}{2^n} \le \frac{x-(\ell-1)+1}{2^n} = \frac{x-\ell+2}{2^n}\,.\end{aligned}$$

In short, from $(d-4)(d-1)+2d = d^2-3d+4$, we have $\Pr[T_i^{d^2-3d+4} = T_j^{d^2-3d+4} \mid \mathsf{if}_\ell] \le (d-\ell-2)/2^n$. From $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3} \mid \mathsf{if}_\ell] = 1$, we obtain

$$\Pr[T_i^{[d^2-3d+3,d^2-3d+4]} = T_j^{[d^2-3d+3,d^2-3d+4]} \mid \mathsf{if}_\ell] \le \frac{d-\ell-2}{2^n}\,.$$

From all the observations above, we obtain the upper bound on Eq. (28) as

$$\begin{aligned}\text{Eq. (28)} &= \Pr[T_i^{[d^2-3d+3,d^2-3d+4]} = T_j^{[d^2-3d+3,d^2-3d+4]}]\\ &\le \Pr[T_i^d = T_j^d] \cdot \Pr[T_i^{[d^2-3d+3,d^2-3d+4]} = T_j^{[d^2-3d+3,d^2-3d+4]} \mid T_i^d = T_j^d]\\ &\quad + \sum_{\ell=1}^{d-3} \left(\Pr[\mathsf{if}_\ell] \cdot \Pr[T_i^{[d^2-3d+3,d^2-3d+4]} = T_j^{[d^2-3d+3,d^2-3d+4]} \mid \mathsf{if}_\ell]\right)\\ &\le \frac{2}{2^n} \cdot \frac{d-2}{2^n} + \sum_{\ell=1}^{d-3} \left(\frac{1}{2^n} \cdot \frac{d-\ell-2}{2^n}\right)\\ &= \frac{2(d-2)}{2^{2n}} + \frac{1}{2^{2n}} \cdot \frac{((d-3)+1)(d-3)}{2} = \frac{d^2-d-2}{2 \cdot 2^{2n}}\end{aligned}$$

and we conclude that $(d^2-d-2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^d \neq 0$, where $\Delta C_{i,j}^1$ is any difference.

We next prove that the upper bound above is the upper bound for all other ciphertext differences. Observe that the event $T_i^{[d^2-3d+3,d^2-3d+4]} = T_j^{[d^2-3d+3,d^2-3d+4]}$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,s}}$ in Appendix B.

(C-16) First, let us assume that $\Delta C_{i,j}^{[2..d-1]} \neq 0 \wedge \Delta C_{i,j}^d \neq 0$, namely, for some $y \in [2..d-1]$, we have $\Delta C_{i,j}^y \neq 0$, where there may be multiple indices of y. If $y = 2$, we have $\Pr[T_i^d = T_j^d] \le 1/2^n$ from $T^d = \widetilde{P}'_d(T^1, C^2)$, and hence the probability would be

smaller. If $y \in [3..d-1]$, the event $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$ would be a probabilistic event. Then, for any $x \in [1..d-3]$, from $T^{x(d-1)+d} = \widetilde{P}'_{x(d-1)+d}(T^{x(d-1)+1}, T^{x(d-1)})$, even if we assume $T_i^{x(d-1)+1} = T_j^{x(d-1)+1}$, the event $T_i^{\ell(d-1)+d} = T_j^{\ell(d-1)+d}$ for $\ell \in [x..d-3]$ would be a probabilistic event. Therefore, for $\ell \in [1..d-4]$, we have $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3} \mid T_i^d = T_j^d \vee \mathsf{if}_\ell] < 1$, and hence the probability would be smaller.

(C-17) Next, consider the case $\Delta C_{i,j}^1 \neq 0 \wedge \Delta C_{i,j}^d = 0$, which is the same difference as (C-5). With the same argument, if $\Delta C_{i,j}^{[2..d-1]} = 0$, this case corresponds to the analysis of the reduced round version by $(d-1)$ rounds. This would result in the reduction on the number of terms added to the upper bound. The case $\Delta C_{i,j}^{[2..d-1]} \neq 0$ would have a smaller upper bound as in the case (C-16).

(C-18) Finally, we consider the case $\Delta C_{i,j}^{[1,d]} = 0$. This difference is the same as (C-6), and we can thus follow the same argument. For the largest index $y \in [2..d-1]$ such that $\Delta C_{i,j}^y \neq 0$, this case corresponds to the analysis of the reduced round version by $(d-y)$ rounds.

If $y = d-1$ and $\Delta C_{i,j}^{[2..d-2]} = 0$, we have $T_i^{d^2-4d+4} = T_j^{d^2-4d+4}$ and $T_i^{d^2-4d+3} \neq T_j^{d^2-4d+3}$ by following the argument in (C-6). It follows that we have $T_i^{d^2-3d+3} \neq T_j^{d^2-3d+3}$ since $T^{d^2-3d+3} = \widetilde{P}'_{d^2-3d+3}(T^{d^2-4d+4}, T^{d^2-4d+3})$. That is, $\Pr[T_i^{d^2-3d+3} = T_j^{d^2-3d+3}] = 0$ holds in this case.

In other cases, the event $T_i^{[d-1..(d-3)(d-1):d-1]} = T_j^{[d-1..(d-3)(d-1):d-1]}$ would be a probabilistic event, and hence the final bound cannot be larger as in the analysis of the case (C-16).

Therefore, the case $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^d \neq 0$, where $\Delta C_{i,j}^1$ is any difference, maximizes Eq. (28) and $(d^2-d-2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{s,m}}$. We next analyze a condition in $\mathsf{coll}_{\mathrm{s,m}}$. We consider a collision at (M^1, S^{d-1}) that involves an internal state with the largest index in the number of round. Since $S^{d-1} = T^{r-2d+2} = T^{d^2-3d+4}$ holds when $r = d^2-d+2$, we evaluate

$$\Pr[(M_i^1, S_i^{d-1}) = (M_j^1, S_j^{d-1}) \wedge S_i^d \neq S_j^d] \leq \Pr[(M_i^1, T_i^{d^2-3d+4}) = (M_j^1, T_j^{d^2-3d+4})]. \quad (29)$$

We first compute the upper bound on Eq. (29) when the ciphertext difference is $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^d = 0$. We then show that this upper bound covers all other cases.

This ciphertext difference $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^d = 0$ is the same ciphertext difference as $\mathsf{coll}_{\mathrm{s,m}}$ analyzed in the proof of Lemma 7. Therefore, we follow the same argument as in the proof of Lemma 7, and we have $T_i^{[1..(d-3)(d-1)+1:d-1]} = T_j^{[1..(d-3)(d-1)+1:d-1]}$.

Now from $C_i^{d-1} \neq C_j^{d-1}$, we have $\Pr[T_i^2 = T_j^2] = 1/2^n$ as $T^2 = \widetilde{P}'_2(C^{d-1}, C^d)$. Next, for any $x \in [0..d-3]$, if $T_i^{x(d-1)+2} = T_j^{x(d-1)+2}$, then $T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1}$, since we have $T^{x(d-1)+d+1} = \widetilde{P}'_{x(d-1)+d+1}(T^{x(d-1)+2}, T^{x(d-1)+1})$ and $T_i^{[1..(d-3)(d-1)+1:d-1]} =$

$T_j^{[1..(d-3)(d-1)+1:d-1]}$. Therefore, for any $x \in [0..d-3]$,

$$\begin{aligned}
&\Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1}] \\
&\quad = \Pr[T_i^{x(d-1)+2} = T_j^{x(d-1)+2}] + \Pr[T_i^{x(d-1)+2} \neq T_j^{x(d-1)+2}] \\
&\qquad \cdot \Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1} \mid T_i^{x(d-1)+2} \neq T_j^{x(d-1)+2}] \\
&\quad \leq \Pr[T_i^{x(d-1)+2} = T_j^{x(d-1)+2}] + \frac{1}{2^n} \leq \Pr[T_i^2 = T_j^2] + \sum_{\ell=0}^{x} \frac{1}{2^n} = \frac{x+2}{2^n}\,.
\end{aligned}$$

From $(d-3)(d-1)+d+1 = d^2-3d+4$, we obtain $\Pr[T_i^{d^2-3d+4} = T_j^{d^2-3d+4}] \leq ((d-3)+2)/2^n = (d-1)/2^n$.

In the ideal world, plaintexts are computed with the dn-bit random permutation π^{-1}, and thus regardless of the ciphertext difference, by following the computation in Eq. (5), we have $\Pr[M_i^1 = M_j^1] \leq 1/2^n$. Given the analysis so far, we obtain the upper bound on Eq. (29) as

$$\begin{aligned}
\text{Eq. (29)} &= \Pr[(M_i^1, T_i^{d^2-3d+4}) = (M_j^1, T_j^{d^2-3d+4})] \\
&= \Pr[T_i^{d^2-3d+4} = T_j^{d^2-3d+4}] \cdot \Pr[M_i^1 = M_j^1] \leq \frac{d-1}{2^n} \cdot \frac{1}{2^n} = \frac{d-1}{2^{2n}}\,,
\end{aligned}$$

when the ciphertext difference is $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$.

Next, we show that the upper bound above covers all other cases. Observe that the event $(M_i^1, T_i^{d^2-3d+4}) = (M_j^1, T_j^{d^2-3d+4})$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,c}}$ in Appendix B. Since $\Pr[M_i^1 = M_j^1]$ does not depend on the ciphertext difference, we focus on the analysis of $\Pr[T_i^{d^2-3d+4} = T_j^{d^2-3d+4}]$.

(C-19) First, consider the case $\Delta C_{i,j}^{[1..d-2]} \neq 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$. In this case, the event $T_i^{[1..(d-3)(d-1)+1:d-1]} = T_j^{[1..(d-3)(d-1)+1:d-1]}$ would be a probabilistic event. Then, for any $x \in [0..d-3]$, from $T^{x(d-1)+d+1} = \widetilde{P}'_{x(d-1)+d+1}(T^{x(d-1)+2}, T^{x(d-1)+1})$, even if we assume $T_i^{x(d-1)+2} = T_j^{x(d-1)+2}$, the event $T_i^{\ell(d-1)+d+1} = T_j^{\ell(d-1)+d+1}$ for $\ell \in [x..d-3]$ would be a probabilistic event. This implies that there exists a term $\Pr[T_i^{x(d-1)+2} = T_j^{x(d-1)+2}]$ that is not added to derive the upper bound on $\Pr[T_i^{x(d-1)+d+1} = T_j^{x(d-1)+d+1}]$, and hence the final probability would be smaller.

(C-20) Next, consider the case $\Delta C_{i,j}^{[d-1,d]} = 0$, which implies $\Delta C_{i,j}^{[1..d-2]} \neq 0$. For the largest index $x \in [1..d-2]$ such that $\Delta C_{i,j}^{x} \neq 0$, the input of the $(d-x)$-th round is the same as $\Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$, and this case corresponds to the analysis of the reduced round version by $(d-x-1)$ rounds. Then, the event $T_i^{[1..(d-3)(d-1)+1:d-1]} = T_j^{[1..(d-3)(d-1)+1:d-1]}$ would be a probabilistic event, and hence the final bound cannot be larger as in the analysis of the case (C-19).

(C-21) Finally, assume that $\Delta C_{i,j}^{d} \neq 0$. Now if we further assume that $\Delta C_{i,j}^{[1..d-1]} = 0$, this ciphertext difference is the same difference as the input of the second round in the initial case of $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$, and hence this case corresponds to the analysis of the increased round version by one round. Therefore, the event $T_i^{[1..(d-3)(d-1)+1:d-1]} = T_j^{[1..(d-3)(d-1)+1:d-1]}$ would be a probabilistic event, and hence the final bound would be smaller as in the case (C-19).

Therefore, the case $\Delta C_{i,j}^{[1..d-2]} = 0 \wedge \Delta C_{i,j}^{d-1} \neq 0 \wedge \Delta C_{i,j}^{d} = 0$ maximizes Eq. (29) and $(d-1)/2^{2n}$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,m}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{m,m}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{m,m}}$. From a similar analysis to Eq. (6), the probability of a condition in $\mathsf{coll}_{\mathrm{m,m}}$ is at most $1/2^{2n}$. This completes the proof of Lemma 9. □

D Proof of Lemma 14

We proceed as in the proof of Lemma 2. We first consider $\mathsf{coll}_{\mathrm{s,s}}$, followed by $\mathsf{coll}_{\mathrm{s,c}}$ and $\mathsf{coll}_{\mathrm{c,c}}$.

Analysis of $\mathsf{coll}_{\mathrm{s,s}}$. We consider a condition in $\mathsf{coll}_{\mathrm{s,s}}$. All the conditions in $\mathsf{coll}_{\mathrm{s,s}}$ are collisions at $(S^{r-3,\ell}, S^{r-2,y})$ for $y \in [1..d/2]$ and $\ell = (y \bmod d/2) + 1$. From the symmetry in $\mathcal{E}_{2,d,r}$, each probability of the collisions at $(S^{r-3,\ell}, S^{r-2,y})$ has a same upper bound. Here, we consider a collision at $(S^{r-3,2}, S^{r-2,1})$. For $r = d + 2$, we evaluate

$$\begin{aligned}&\Pr[(S_i^{r-3,2}, S_i^{r-2,1}) = (S_j^{r-3,2}, S_j^{r-2,1}) \wedge C_i^d \neq C_j^d] \\ &\quad \leq \Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1})]\,.\end{aligned} \tag{30}$$

We first evaluate Eq. (30) when the plaintext difference is $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, where $\Delta M_{i,j}^{4}$ can take any difference. We then show that this gives us the upper bound on all the possible plaintext differences by showing that all other cases do not have a larger upper bound.

If we cyclically shift this plaintext difference $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$ by 2 blocks, the shifted difference is the same difference $\Delta M_{i,j}^{1} \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ that maximizes the collision probability of $\mathsf{coll}_{\mathrm{s,s}}$ in the proof of Lemma 12. From the symmetry in $\mathcal{E}_{2,d,r}$, for $\ell = (y \bmod d/2) + 1$, $S^{x,y}$ in the proof of Lemma 12 corresponds to $S^{x,\ell}$ in this analysis. With the same argument, we have $S_i^{[1..d-3],3} = S_j^{[1..d-3],3}$. Note that we have $S_i^{1,1} = S_j^{1,1}$ when $d = 4$.

Now, from $M_i^3 \neq M_j^3$, the probability of a collision at $S^{1,2} = \widetilde{P}_{1,2}(M^3, M^4)$ is $\Pr[S_i^{1,2} = S_j^{1,2}] = 1/2^n$. Next, for any $x \in [2..d-1]$, since we have $S^{2,2} = \widetilde{P}_{2,2}(S^{1,2}, M^5)$ and $S^{x,2} = \widetilde{P}_{x,2}(S^{x-1,2}, S^{x-2,3})$, and from $M_i^5 = M_j^5$ and $S_i^{[1..d-3],3} = S_j^{[1..d-3],3}$, if $S_i^{x-1,2} = S_j^{x-1,2}$, then we must have $S_i^{[x..d-1],2} = S_j^{[x..d-1],2}$. When $d = 4$, M^5 and $S^{[1..d-3],3}$ correspond to M^1 and $S^{1,1}$, respectively. Therefore, for each $x \in [2..d-1]$, we have

$$\begin{aligned}&\Pr[S_i^{x,2} = S_j^{x,2}] \\ &\quad = \Pr[S_i^{x-1,2} = S_j^{x-1,2}] + \Pr[S_i^{x-1,2} \neq S_j^{x-1,2}] \cdot \Pr[S_i^{x,2} = S_j^{x,2} \mid S_i^{x-1,2} \neq S_j^{x-1,2}] \\ &\quad \leq \Pr[S_i^{x-1,2} = S_j^{x-1,2}] + \frac{1}{2^n} \leq \Pr[S_i^{1,2} = S_j^{1,2}] + \sum_{\ell=2}^{x} \frac{1}{2^n} = \frac{x}{2^n}\end{aligned}$$

and this yields $\Pr[S_i^{2,2} = S_j^{2,2}] \leq 2/2^n$.

Assume that we have a collision at $S^{2,2}$, in which case $S_i^{[3..d-1],2} = S_j^{[3..d-1],2}$ holds. Since $S^{1,1} = \widetilde{P}_{1,1}(M^1, M^2)$, we have $S_i^{1,1} = S_j^{1,1}$ from $M_i^{[1,2]} = M_j^{[1,2]}$. We also have $S_i^{2,1} \neq S_j^{2,1}$ from $S_i^{1,1} = S_j^{1,1}$ and $M_i^3 \neq M_j^3$ since $S^{2,1} = \widetilde{P}_{2,1}(S^{1,1}, M^3)$. It follows that a collision probability at $S^{3,1} = \widetilde{P}_{3,1}(S^{2,1}, S^{1,2})$ is $\Pr[S_i^{3,1} = S_j^{3,1}] = 1/2^n$. We also observe that for any $x \in [4..d]$, if $S_i^{x-1,1} = S_j^{x-1,1}$, then we have $S_i^{[x..d],1} = S_j^{[x..d],1}$. This follows from the fact that $S_i^{[2..d-2],2} = S_j^{[2..d-2],2}$ holds, and for any $x \in [4..d]$, $S^{x-2,2}$ is the input

block of $S^{x,1} = \widetilde{P}_{x,1}(S^{x-1,1}, S^{x-2,2})$. From the observation, for any $x \in [4..d]$, we have

$$\begin{aligned}
&\Pr[S_i^{x,1} = S_j^{x,1} \mid S_i^{2,2} = S_j^{2,2}] \\
&\quad = \Pr[S_i^{x-1,1} = S_j^{x-1,1} \mid S_i^{2,2} = S_j^{2,2}] + \Pr[S_i^{x-1,1} \neq S_j^{x-1,1} \mid S_i^{2,2} = S_j^{2,2}] \\
&\qquad \cdot \Pr[S_i^{x,1} = S_j^{x,1} \mid S_i^{x-1,1} \neq S_j^{x-1,1} \wedge S_i^{2,2} = S_j^{2,2}] \\
&\quad \leq \Pr[S_i^{x-1,1} = S_j^{x-1,1} \mid S_i^{2,2} = S_j^{2,2}] + \frac{1}{2^n} \\
&\quad \leq \Pr[S_i^{3,1} = S_j^{3,1} \mid S_i^{2,2} = S_j^{2,2}] + \sum_{\ell=4}^{x} \frac{1}{2^n} = \frac{(x-3)+1}{2^n} = \frac{x-2}{2^n}\,.
\end{aligned}$$

Therefore, from $\Pr[S_i^{d-1,2} = S_j^{d-1,2} \mid S_i^{2,2} = S_j^{2,2}] = 1$, we obtain

$$\Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1}) \mid S_i^{2,2} = S_j^{2,2}] \leq \frac{d-2}{2^n}\,.$$

We proceed similarly for $\ell \in [3..d-1]$ as follows. We assume $S_i^{\ell-1,2} \neq S_j^{\ell-1,2}$ and we also assume that we have a collision at $S^{\ell,2}$. We denote the assumption $S_i^{\ell-1,2} \neq S_j^{\ell-1,2} \wedge S_i^{\ell,2} = S_j^{\ell,2}$ by if_ℓ. Then, we have $S_i^{[\ell+1..d-1],2} = S_j^{[\ell+1..d-1],2}$, and from $S_i^{\ell-1,2} \neq S_j^{\ell-1,2}$ and $S^{\ell,2} = \widetilde{P}_{\ell,2}(S^{\ell-1,2}, S^{\ell-2,3})$, we have $\Pr[\mathsf{if}_\ell] \leq 1/2^n$. We also observe that if $S_i^{\ell-1,2} \neq S_j^{\ell-1,2}$, from $S^{\ell+1,1} = \widetilde{P}_{\ell+1,1}(S^{\ell,1}, S^{\ell-1,2})$, a collision at $S^{\ell+1,1}$ is possible only if $S_i^{\ell,1} \neq S_j^{\ell,1}$. Therefore, we have

$$\Pr[S_i^{\ell+1,1} = S_j^{\ell+1,1} \mid \mathsf{if}_\ell] \leq \Pr[S_i^{\ell+1,1} = S_j^{\ell+1,1} \mid S_i^{\ell,1} \neq S_j^{\ell,1}] = \frac{1}{2^n}\,.$$

Furthermore, for any $x \in [\ell+2..d]$, if $S_i^{x-1,1} = S_j^{x-1,1}$, then $S_i^{[x..d],1} = S_j^{[x..d],1}$ holds. This follows from $S_i^{[\ell..d-2],2} = S_j^{[\ell..d-2],2}$, and $S^{x-2,2}$ is the input block of $S^{x,1} = \widetilde{P}_{x,1}(S^{x-1,1}, S^{x-2,2})$. It follows that for any $x \in [\ell+2..d]$, we have

$$\begin{aligned}
&\Pr[S_i^{x,1} = S_j^{x,1} \mid \mathsf{if}_\ell] \\
&\quad = \Pr[S_i^{x-1,1} = S_j^{x-1,1} \mid \mathsf{if}_\ell] \\
&\qquad + \Pr[S_i^{x-1,1} \neq S_j^{x-1,1} \mid \mathsf{if}_\ell] \cdot \Pr[S_i^{x,1} = S_j^{x,1} \mid S_i^{x-1,1} \neq S_j^{x-1,1} \wedge \mathsf{if}_\ell] \\
&\quad \leq \Pr[S_i^{x-1,1} = S_j^{x-1,1} \mid \mathsf{if}_\ell] + \frac{1}{2^n} \\
&\quad \leq \Pr[S_i^{\ell+1,1} = S_j^{\ell+1,1} \mid \mathsf{if}_\ell] + \sum_{m=\ell+2}^{x} \frac{1}{2^n} \leq \frac{x-(\ell+1)+1}{2^n} = \frac{x-\ell}{2^n}\,.
\end{aligned}$$

From $\Pr[S_i^{d-1,2} = S_j^{d-1,2} \mid \mathsf{if}_\ell] = 1$, we obtain

$$\Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1}) \mid \mathsf{if}_\ell] \leq \frac{d-\ell}{2^n}\,.$$

From all the observations above, we obtain the upper bound on Eq. (30) as

$$\begin{aligned}
\text{Eq. (30)} &= \Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1})] \\
&\le \Pr[S_i^{2,2} = S_j^{2,2}] \cdot \Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1}) \mid S_i^{2,2} = S_j^{2,2}] \\
&\quad + \sum_{\ell=3}^{d-1} \left(\Pr[\mathsf{if}_\ell] \cdot \Pr[(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1}) \mid \mathsf{if}_\ell] \right) \\
&\le \frac{2}{2^n} \cdot \frac{d-2}{2^n} + \sum_{\ell=3}^{d-1} \left(\frac{1}{2^n} \cdot \frac{d-\ell}{2^n} \right) \\
&= \frac{2(d-2)}{2^{2n}} + \frac{1}{2^{2n}} \cdot \frac{((d-3)+1)(d-3)}{2} = \frac{d^2-d-2}{2 \cdot 2^{2n}},
\end{aligned}$$

and we conclude that $(d^2-d-2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for the case $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, where $\Delta M_{i,j}^{4}$ is any difference.

We next prove that the upper bound above is the upper bound for all other plaintext differences. Observe that the event $(S_i^{d-1,2}, S_i^{d,1}) = (S_j^{d-1,2}, S_j^{d,1})$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,s}}$ in Appendix B.

(C-22) First, let us assume that $\Delta M_{i,j}^{3} \neq 0 \wedge (\Delta M_{i,j}^{[1,2]} \neq 0 \vee \Delta M_{i,j}^{[5..d]} \neq 0)$, namely, for some $y \in [1..d] \setminus \{3,4\}$, we have $\Delta M_{i,j}^{y} \neq 0$, where there may be multiple indices of y. If $y = 5$, we have $\Pr[S_i^{2,2} = S_j^{2,2}] \le 1/2^n$ from $S^{2,2} = \widetilde{P}_{2,2}(S^{1,2}, M^5)$, and hence the probability would be smaller. If $y \in [1..d] \setminus [3..5]$, the event $S_i^{[1..d-3],3} = S_j^{[1..d-3],3}$ would be a probabilistic event. Then, for any $x \in [3..d-1]$, from $S^{x,2} = \widetilde{P}_{x,2}(S^{x-1,2}, S^{x-2,3})$, even if we assume $S_i^{x-1,2} = S_j^{x-1,2}$, the event $S_i^{[x..d-1],2} = S_j^{[x..d-1],2}$ would be a probabilistic event. Therefore, for $\ell \in [3..d-2]$, we have $\Pr[S_i^{d-1,2} = S_j^{d-1,2} \mid S_i^{2,2} = S_j^{2,2} \vee \mathsf{if}_\ell] < 1$, and hence the probability would be smaller.

(C-23) Next, consider the case $\Delta M_{i,j}^{3} = 0 \wedge \Delta M_{i,j}^{4} \neq 0$. In this case, we must have $S_i^{1,2} \neq S_j^{1,2}$ from $S^{1,2} = \widetilde{P}_{1,2}(M^3, M^4)$. Now if we further assume that $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, the input at the second round is the same difference as the initial case of $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, and the analysis corresponds to the one with a reduced round version that cannot have a larger collision probability. The case $\Delta M_{i,j}^{[1,2]} \neq 0 \vee \Delta M_{i,j}^{[5..d]} \neq 0$ would have a smaller upper bound as in the case (C-22).

(C-24) Finally, we consider the case $\Delta M_{i,j}^{[3,4]} = 0$, in which case we necessarily have $\Delta M_{i,j}^{[1,2]} \neq 0 \vee \Delta M_{i,j}^{[5..d]} \neq 0$. If $\Delta M_{i,j}^{[5..d]} \neq 0$, we consider the smallest index $x \in [5..d]$ such that $\Delta M_{i,j}^{x} \neq 0$. Then since $\Delta M_{i,j}^{[3..x-1]} = 0$, it has the same input difference as $\Delta M_{i,j}^{3} \neq 0$ at the input of the $(x-2)$-th round. In the case of $\Delta M_{i,j}^{[1,2]} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, for the smallest index $x \in \{1,2\}$ such that $\Delta M_{i,j}^{x} \neq 0$, the input difference of the $(d+x-2)$-th round is the same as $\Delta M_{i,j}^{3} \neq 0$, and hence the final bound cannot be larger as in the analysis of the case (C-23).

Therefore, the case $\Delta M_{i,j}^{[1,2]} = 0 \wedge \Delta M_{i,j}^{3} \neq 0 \wedge \Delta M_{i,j}^{[5..d]} = 0$, where $\Delta M_{i,j}^{4}$ is any difference, maximizes Eq. (30) and $(d^2-d-2)/(2 \cdot 2^{2n})$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,s}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{s,c}}$. We next analyze a condition in $\mathsf{coll}_{\mathrm{s,c}}$. All the conditions in $\mathsf{coll}_{\mathrm{s,c}}$ are collisions between $S^{r-2,y}$ and a ciphertext block for $y \in [1..d/2]$. From the symmetry in $\mathcal{E}_{2,d,r}$ and since ciphertexts are computed with the dn-bit random permutation π in the ideal world, each probability of the collisions between $S^{r-2,y}$ and a ciphertext block has the same upper bound. Here, we consider a collision at $(S^{r-2,1}, C^d)$. For $r = d+2$, we evaluate

$$\Pr[(S_i^{r-2,1}, C_i^d) = (S_j^{r-2,1}, C_j^d) \wedge S_i^{r-3,2} \neq S_j^{r-3,2}] \leq \Pr[(S_i^{d,1}, C_i^d) = (S_j^{d,1}, C_j^d)]\,. \quad (31)$$

We first compute the upper bound on Eq. (31) when the plaintext difference is $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M^{[3..d]} = 0$. We then show that this upper bound covers all other cases.

This plaintext difference $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M^{[3..d]} = 0$ is the same plaintext difference as $\mathsf{coll}_{\mathrm{s,c}}$ analyzed in the proof of Lemma 12. Therefore, we follow the same argument as in the proof of Lemma 12, and we have $S_i^{[1..d-2],2} = S_j^{[1..d-2],2}$.

Now from $M_i^1 = M_j^1$ and $M_i^2 \neq M_j^2$, we have $S_i^{1,1} \neq S_j^{1,1}$ since $S^{1,1} = \widetilde{P}_{1,1}(M^1, M^2)$. It follows that a collision probability at $S^{2,1} = \widetilde{P}_{2,1}(S^{1,1}, M^3)$ is $\Pr[S_i^{2,1} = S_j^{2,1}] = 1/2^n$. It is easy to see that for any $x \in [3..d]$, if $S_i^{x-1,1} = S_j^{x-1,1}$, then $S_i^{[x..d],1} = S_j^{[x..d],1}$, since we have $S^{x,1} = \widetilde{P}_{x,1}(S^{x-1,1}, S^{x-2,2})$ and $S_i^{[1..d-2],2} = S_j^{[1..d-2],2}$. Therefore, for any $x \in [3..d]$,

$$\begin{aligned}
&\Pr[S_i^{x,1} = S_j^{x,1}] \\
&\quad = \Pr[S_i^{x-1,1} = S_j^{x-1,1}] + \Pr[S_i^{x-1,1} \neq S_j^{x-1,1}] \cdot \Pr[S_i^{x,1} = S_j^{x,1} \mid S_i^{x-1,1} \neq S_j^{x-1,1}] \\
&\quad \leq \Pr[S_i^{x-1,1} = S_j^{x-1,1}] + \frac{1}{2^n} \leq \Pr[S_i^{2,1} = S_j^{2,1}] + \sum_{\ell=3}^{x} \frac{1}{2^n} = \frac{x-1}{2^n}\,.
\end{aligned}$$

In the ideal world, ciphertexts are computed with the dn-bit random permutation π, and thus regardless of the plaintext difference, by following the computation in Eq. (5), we have $\Pr[C_i^d = C_j^d] \leq 1/2^n$. Given the analysis so far, we obtain the upper bound on Eq. (31) as

$$\begin{aligned}
\text{Eq. (31)} &= \Pr[(S_i^{d,1}, C_i^d) = (S_j^{d,1}, C_j^d)] = \Pr[S_i^{d,1} = S_j^{d,1}] \cdot \Pr[C_i^d = C_j^d] \\
&\leq \frac{d-1}{2^n} \cdot \frac{1}{2^n} = \frac{d-1}{2^{2n}}\,,
\end{aligned}$$

when the plaintext difference is $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M^{[3..d]} = 0$.

Next, we show that the upper bound above covers all other cases. Observe that the event $(S_i^{d,1}, C_i^d) = (S_j^{d,1}, C_j^d)$ and the computation above are similar to $\mathsf{coll}_{\mathrm{s,c}}$ in Appendix B. Since $\Pr[C_i^d = C_j^d]$ does not depend on the plaintext difference, we focus on the analysis of $\Pr[S_i^{d,1} = S_j^{d,1}]$.

(C-25) First, consider the case $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M^{[3..d]} \neq 0$. In this case, the event $S_i^{[1..d-2],2} = S_j^{[1..d-2],2}$ would be a probabilistic event. Then, for any $x \in [3..d]$, from $S^{x,1} = \widetilde{P}_{x,1}(S^{x-1,1}, S^{x-2,2})$, even if we assume $S_i^{x-1,1} = S_j^{x-1,1}$, the event $S_i^{[x..d],1} = S_j^{[x..d],1}$ would be a probabilistic event. Therefore, there exists a term $\Pr[S_i^{x-1,1} = S_j^{x-1,1}]$ that is not added to derive the upper bound on $\Pr[S_i^{x,1} = S_j^{x,1}]$, and hence the final probability would be smaller.

(C-26) Next, consider the case $\Delta M_{i,j}^{[1,2]} = 0$, which implies $\Delta M_{i,j}^{[3..d]} \neq 0$. For the smallest index $x \in [3..d]$ such that $\Delta M_{i,j}^x \neq 0$, it has the same input difference as $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0$ at the input of the $(x-1)$-th round, i.e., this case corresponds to the analysis of the reduced round version by $(x-2)$ rounds, which cannot have a larger collision probability.

(C-27) Finally, assume that $\Delta M^1_{i,j} \neq 0$. Now if we further assume that $\Delta M^{[2..d]}_{i,j} = 0$, this plaintext difference is the same difference as the input of the second round in the initial case of $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[3..d]} = 0$, and hence this case corresponds to the analysis of the increased round version by one round. This would result in $\Pr[S_i^{d-2,2} = S_j^{d-2,2}] \neq 1$, i.e., $S_i^{d-2,2} = S_j^{d-2,2}$ could be a probabilistic event, or it could be $\Pr[S_i^{d-2,2} = S_j^{d-2,2}] = 0$, where the latter case occurs when $\Delta M^{[2..d]}_{i,j} = 0$. Therefore, the final bound would be smaller as in the case (C-25).

Therefore, the case $\Delta M^1_{i,j} = 0 \wedge \Delta M^2_{i,j} \neq 0 \wedge \Delta M^{[3..d]} = 0$ maximizes Eq. (31) and $(d-1)/2^{2n}$ is the upper bound on a condition in $\mathsf{coll}_{\mathrm{s,c}}$ for all the cases.

Analysis of $\mathsf{coll}_{\mathrm{c,c}}$. Finally, we consider a condition in $\mathsf{coll}_{\mathrm{c,c}}$. From the same analysis as in Eq. (6), the probability of a condition in $\mathsf{coll}_{\mathrm{c,c}}$ is at most $1/2^{2n}$. This completes the proof of Lemma 14. □

E Proof of Proposition 1

From the definition in Sect. 3, $\mathcal{E}^{-1}_{1,d,r}[\widetilde{E}_1, \ldots, \widetilde{E}_{d-1}]$ with $r = d-1$ rounds is

$$\begin{aligned}\mathcal{E}^{-1}_{1,d,r}[\widetilde{E}_1, \ldots, \widetilde{E}_{d-1}](X^{[1..d]}) &= \Phi^{-1}_{1,d}[\widetilde{E}_1] \circ \cdots \circ \Phi^{-1}_{1,d}[\widetilde{E}_{d-2}] \circ \Phi^{-1}_{1,d}[\widetilde{E}_{d-1}](X^{[1..d]}) \\ &= (X^2 \,\|\, \widetilde{E}_1^{-1}(X^2, X^3) \,\|\, \cdots \,\|\, \widetilde{E}_{d-2}^{-1}(X^{d-1}, X^d) \,\|\, \widetilde{E}_{d-1}^{-1}(X^d, X^1))\,,\end{aligned} \tag{32}$$

where $X^{[1..d]} = X^1 \,\|\, \cdots \,\|\, X^d$ is the input. We also write $\Phi_{3,d}[\widetilde{E}'_1, \ldots, \widetilde{E}'_{d-1}]$, which is

$$\begin{aligned}&\Phi_{3,d}[\widetilde{E}'_1, \ldots, \widetilde{E}'_{d-1}](Y^{[1..d]}) \\ &\quad = (\widetilde{E}'_1(Y^1, Y^2) \,\|\, \cdots \,\|\, \widetilde{E}'_{d-2}(Y^{d-2}, Y^{d-1}) \,\|\, \widetilde{E}'_{d-1}(Y^{d-1}, Y^d) \,\|\, Y^1)\,,\end{aligned} \tag{33}$$

where $Y^{[1..d]} = Y^1 \,\|\, \cdots \,\|\, Y^d$ is the input.

Now let $Y^\ell = X^{\ell+1}$ for $\ell \in [1..d-1]$, $Y^d = X^1$, and $\widetilde{E}'_x(\cdot) = \widetilde{E}_x^{-1}(\cdot)$ for $x \in [1..d-1]$. Then Eq. (33) is

$$\begin{aligned}\Phi_{3,d}[\widetilde{E}'_1, \ldots, \widetilde{E}'_{d-1}](Y^{[1..d]}) &= \Phi_{3,d}[\widetilde{E}_1^{-1}, \ldots, \widetilde{E}_{d-1}^{-1}](X^{[2..d]} \,\|\, X^1) \\ &= (\widetilde{E}_1^{-1}(X^2, X^3) \,\|\, \cdots \,\|\, \widetilde{E}_{d-2}^{-1}(X^{d-1}, X^d) \,\|\, \widetilde{E}_{d-1}^{-1}(X^d, X^1) \,\|\, X^2)\,.\end{aligned} \tag{34}$$

Therefore, $\Phi_{3,d}$ in Eq. (34) is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ in Eq. (32), where the input and output are rotated to the left by one block. Therefore, $\Phi_{3,d}$ is equivalent to $\mathcal{E}^{-1}_{1,d,r}$ with $r = d-1$ rounds. □

F Proof of Theorem 5

First, we recall the procedure of $\mathcal{A}$ for the case $r = d^2 - d + 1$:

1. Fix $q = 2^{n/2}$ ciphertexts $C_1^{[1..d]}, \ldots, C_q^{[1..d]}$ such that $\Delta C^1_{i,j} \neq 0 \wedge \Delta C^{[2..d]}_{i,j} = 0$, and make q decryption queries (See Fig. 14(d)).
2. If a collision is found among the q values of M_i^1, then output 1, else output 0.

We first consider the real world. Following the proof of Lemma 7, we write $\widetilde{P}'_1, \ldots, \widetilde{P}'_r$ for $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_1^{-1}$, i.e., for $x \in [1..r]$, we let $\widetilde{P}_x^{-1}(\cdot) = \widetilde{P}'_{r-x+1}(\cdot)$. Similarly, we write

$T^1, \ldots, T^{r-d}$ for the internal states $S^{r-d}, \ldots, S^1$ that are computed with $\widetilde{P}_r^{-1}, \ldots, \widetilde{P}_{d+1}^{-1}$, respectively, i.e., we let $S^x = T^{r-d-x+1}$ for $x \in [1..r-d]$.

In the real world, for ciphertexts with $\Delta C_{i,j}^1 \neq 0 \wedge \Delta C_{i,j}^{[2..d]} = 0$, we always have $T_i^1 \neq T_j^1$ and $T_i^{[2..d-1]} = T_j^{[2..d-1]}$, since $T^1 = \widetilde{P}'_1(C^d, C^1)$ and $T^x = \widetilde{P}'_x(C^{d-x+1}, C^{d-x+2})$ for $x \in [2..d-1]$. That is, the difference of the input $C^2 \| T^{d-1} \| T^{d-2} \| \cdots \| T^1$ to the d-th round in the decryption direction is the same as the ciphertext difference $\Delta C_{i,j}^{[2..d-1]} = 0 \wedge \Delta C_{i,j}^d \neq 0$ that maximizes the collision probability among the differences in $\mathsf{coll}_{\mathrm{s,s}}$ in the proof of Lemma 7. We can then follow a similar argument to the proof of Lemma 7 by adding $(d-1)$ rounds, and $T^1, \ldots, T^{d^2-4d+4}$ in the proof of Lemma 7 corresponds to $T^d, \ldots, T^{d^2-3d+3}$ in this attack. We observe that for $x \in [1..d-3]$, if $T_i^{x(d-1)+1} = T_j^{x(d-1)+1}$, then we have $T_i^{x(d-1)+d} = T_j^{x(d-1)+d}$, and since $M^1 = \widetilde{P}'_{d^2-2d+2}(T^{d^2-3d+3}, T^{d^2-3d+2})$, we also observe that if $T_i^{d^2-3d+3} = T_j^{d^2-3d+3}$, then we have $M_i^1 = M_j^1$.

From the analysis above and by following the computation of Eq. (23), we compute the lower bound to have a collision at M^1 in the real world as follows:

$$\begin{aligned}\Pr[\mathcal{A}^{\mathcal{R},\mathcal{R}^{-1}} = 1] &= 1 - \Pr[\forall \Delta T_{i,j}^d \neq 0] \cdot \prod_{x=1}^{d-2} \Pr\left[\forall \Delta T_{i,j}^{x(d-1)+d} \neq 0 \;\middle|\; \bigwedge_{\ell=1}^{x} \forall \Delta T_{i,j}^{\ell(d-1)+1} \neq 0\right] \\ &= 1 - \left(\prod_{i=2}^{q} \frac{2^n - (i-1)}{2^n}\right)^{1+(d-2)} \gtrapprox 1 - \exp(-0.5(d-1))\end{aligned}$$

Note that $T^{(d-2)(d-1)+d} = T^{d^2-2d+2} = M^1$ when $r = d^2 - d + 1$.

The analysis of the ideal world is the same as in Eq. (24), except that we use π^{-1} to compute plaintexts, and we thus have $\Pr[\mathcal{A}^{\mathcal{I},\mathcal{I}^{-1}} = 1] \leq 0.5$.

Finally, we compute the lower bound of the advantage as

$$\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{R},\mathcal{R}^{-1}} = 1] - \Pr[\mathcal{A}^{\mathcal{I},\mathcal{I}^{-1}} = 1]| \gtrapprox 0.5 - \exp(-0.5(d-1)) \,.$$

In the real world, M^1 for $r = d^2 - d + 1$ corresponds to M^{d-x} for $r = d^2 - d - x$, where $x \in [0..d-2]$. Therefore, it is easy to see that there is an attack with the same complexity for $d^2 - 2d + 2 \leq r < d^2 - d + 2$. □

G Proof of Theorem 6

We consider the case $r = d + 1$. We first recall the procedure of $\mathcal{A}$:

1. Fix $q = 2^{n/2}$ plaintexts $M_1^{[1..d]}, \ldots, M_q^{[1..d]}$ such that $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ for any $1 \leq j < i \leq q$, and make q encryption queries.
2. If a collision is found among the q values of C_i^d, then output 1, else output 0.

In the real world, with encryption queries with $\Delta M_{i,j}^1 = 0 \wedge \Delta M_{i,j}^2 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$, we always have $S_i^{1,1} \neq S_j^{1,1}$ and $S_i^{1,[2..d/2]} = S_j^{1,[2..d/2]}$, since $S^{1,y} = \widetilde{P}_{1,y}(M^{2y-1}, M^{2y})$ for $y \in [1..d/2]$. Then the input difference $S^{1,1} \parallel M^3 \parallel \cdots \parallel S^{1,d/2} \parallel M^1$ of the second round is identical to the plaintext difference $\Delta M_{i,j}^1 \neq 0 \wedge \Delta M_{i,j}^{[3..d]} = 0$ in Lemma 12 that maximizes the collision probability of $\mathsf{coll}_{\mathrm{s,s}}$. By adding a round at the beginning, $S^{x,y}$ in the proof of Lemma 12 corresponds to $S^{x+1,y}$ in this attack. With the same argument, for $x \in [3..d-1]$, if $S_i^{x-1,1} = S_j^{x-1,1}$, then we have $S_i^{[x..d-1],1} = S_j^{[x..d-1],1}$, and from $C^d = \widetilde{P}_{d,1}(S^{d-1,1}, S^{d-2,2})$, if $S_i^{d-1,1} = S_j^{d-1,1}$, then we have $C_i^d = C_j^d$.

From the analysis above and by following Eq. (23), we derive the lower bound on the collision probability at C^d in the real world as follows:

$$\begin{aligned}\Pr[\mathcal{A}^{\mathcal{R}} = 1] &= 1 - \Pr[\forall \Delta S^{2,1}_{i,j} \neq 0] \cdot \prod_{x=3}^{d} \Pr\left[\forall \Delta S^{x,1}_{i,j} \neq 0 \;\middle|\; \bigwedge_{\ell=2}^{x-1} \forall \Delta S^{\ell,1}_{i,j} \neq 0\right] \\ &= 1 - \left(\prod_{i=2}^{q} \frac{2^n - (i-1)}{2^n}\right)^{1+(d-2)} \gtrapprox 1 - \exp(-0.5(d-1))\end{aligned}$$

Note that $S^{d,1} = C^d$ when $r = d + 1$.

The analysis of the ideal world is the same as in Eq. (24), and we have $\Pr[\mathcal{A}^{\mathcal{I}} = 1] \leq 0.5$. Finally, we obtain the lower bound of the advantage as follows:

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}) = |\Pr[\mathcal{A}^{\mathcal{R}} = 1] - \Pr[\mathcal{A}^{\mathcal{I}} = 1]| \gtrapprox 0.5 - \exp(-0.5(d-1))$$

As noted in the proof sketch, in the real world, C^d for $r = d + 1$ corresponds to C^1 for $r = d$, and the attack works with the same complexity for the case $r = d$. □