IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2019, No. 4, pp. 54–80. DOI:10.13154/tosc.v2019.i4.54-80

Iterative Block Ciphers from Tweakable Block Ciphers with Long Tweaks

Ryota Nakamichi and Tetsu Iwata

Nagoya University, Nagoya, Japan
r_nakami@echo.nuee.nagoya-u.ac.jp,tetsu.iwata@nagoya-u.jp

Abstract. We consider a problem of constructing a secure block cipher from a tweakable block cipher (TBC) with long tweaks. Given a TBC with n-bit blocks and τn-bit tweaks for $\tau \geq 1$, one of the constructions by Minematsu in DCC 2015 shows that a simple iteration of the TBC for $3d$ rounds yields a block cipher with dn-bit blocks that is secure up to $2^{dn/2}$ queries, where $d = \tau + 1$. In this paper, we show three results.

1. Iteration of $3d - 2$ rounds is enough for the security up to $2^{dn/2}$ queries, i.e., the security remains the same even if we reduce the number of rounds by two.
2. When the number of queries is limited to 2^n, $d+1$ rounds are enough, and with $d + \ell$ rounds for $1 \leq \ell \leq d - 1$, the security bound improves as ℓ grows.
3. A d-round construction gives a block cipher secure up to $2^{n/2}$ queries, i.e., it achieves the classical birthday-bound security.

Our results show that a block cipher with beyond-birthday-bound (BBB) security (with respect to n) is obtained as low as $d + 1$ rounds, and we draw the security spectrum of $d + \ell$ round version in the range of $1 \leq \ell \leq d - 1$ and $\ell = 2d - 2$ for BBB security, and $\ell = 0$ for birthday-bound security.

Keywords: Beyond-birthday-bound security · Tweakable block cipher · Coefficient-H technique · Provable security

1 Introduction

Construction of a secure block cipher is a classical problem in symmetric cryptography. Many practical constructions follow the concept of confusion and diffusion, and for instance we see the examples of DES, Camellia, and AES that follow this approach. Another approach was initiated by Luby and Rackoff [LR88], where they proved that a simple iterative construction based on a pseudorandom function (PRF) is a pseudorandom permutation (PRP) or a strong pseudorandom permutation (SPRP), depending on the number of rounds. This approach yields a block cipher that is secure against any computationally-bounded adversaries, and the construction is often referred to as the Luby-Rackoff cipher. For instance, they proved that a $2n$-bit 4-round Feistel permutation based on an n-bit PRF is computationally indistinguishable from a $2n$-bit random permutation with chosen-ciphertext attacks (CCAs). The security bound of CCA-adversaries that make at most q queries is $O(q^2/2^n)$, and this is often called the birthday-bound security (with respect to n). This result implies that if $q \ll 2^{n/2}$, then it is computationally infeasible to distinguish the Luby-Rackoff cipher from a truly random permutation.

When higher security is required, the birthday-bound security, $O(q^2/2^n)$, does not offer sufficiently strong security. It is known that the Luby-Rackoff cipher can be broken with $q \approx 2^{n/2}$ queries, and higher security is achieved by increasing the number of rounds.

Received: 2019-01-09, Accepted: 2019-01-11, Published: 2020-31-01

Patarin [Pat04] proved that with 5 or 6 rounds, the Feistel permutation offers higher security than the birthday-bound security in an asymptotic sense. See also [MP03, MRS09, NR99]. The security bound that guarantees beyond $q \approx 2^{n/2}$ queries is often called beyond-birthday-bound security (BBB security).

Using TBCs. For the problem of obtaining a BBB secure block cipher, Minematsu [Min09] initiated the use of a tweakable block cipher (TBC) instead of a PRF. A TBC, introduced by Liskov et al. [LRW02, LRW11], is an extension of a block cipher that has an auxiliary input called a tweak. TBCs have wide applications, and many efficient cryptographic constructions such as (authenticated) encryption or authentication can be obtained, see e.g. [BGIM19, CLS17, GLN19, IMPS17, JNP14a, LN17, Min14, Nai15, NS20, PS16, Rog04]. Conventionally, TBCs are constructed from a block cipher as a mode of operation, such as XEX [Rog04]. However, after introduction of TWEAKEY framework [JNP14c], we see an increasing number of dedicated designs, including KIASU-BC [JNP14b], Deoxys-BC [JNP14a], SKINNY [BJK+16], QARMA [Ava17], and CRAFT [BLMR19]. There are also TBCs in the proposals for the NIST Lightweight Cryptography project [NIS]. These dedicated TBCs can be used to obtain a secure block cipher.

In [Min09], a construction of a $2n$-bit block cipher by combining an n-bit TBC with m-bit tweaks for some $1 \leq m \leq n$ and some hash functions is proposed, and it was proved that its security bound is $O(q^2/2^{n+m})$, i.e., it achieves BBB security, as the security bound remains small even $q \approx 2^{n/2}$. Later, Minematsu and Iwata [MI11] constructed block ciphers of larger and smaller block lengths by using the same TBC as [Min09] and some hash functions.

Suppose that we have a TBC of block length n bits and tweak length τn bits for some $\tau \geq 1$, say $\tau = 2$ or 3, i.e., the tweak length is larger than the block length. With such a TBC, Minematsu [Min15] constructed a dn-bit block cipher, where $d = \tau + 1$, and proved that its security bound is $O(q^2/2^{dn})$ (described in Fig. 1(a)). The construction requires d TBC calls and $2d^2$ $\mathrm{GF}(2^n)$ multiplications to instantiate G_1 and G_2 in Fig. 1(a). There are several ways to instantiate G_1 and G_2, and instead of $\mathrm{GF}(2^n)$ multiplications, the d-round iterative construction with the TBC can be used, i.e., we obtain a construction with a total of $3d$ rounds, which is shown in Fig. 1(b). The entire construction is based only on a TBC, and it consists of $3d$ rounds in total. This construction can be seen as the generalization of the result by Coron et al. [CDMS10], where a block cipher based only on a TBC (described in Fig. 1(c)) is analyzed. Their $2n$-bit block cipher is based on an n-bit TBC with n-bit tweaks and requires 3 rounds.[1] They also considered the indifferentiability framework, where an n-bit ideal cipher with n-bit keys is used to obtain a $2n$-bit public random permutation. See also [GL15] for the indifferentiability analysis where the ideal cipher has a large key space.

Our Results. We continue studying a problem of constructing a block cipher from a TBC in the provable security paradigm, where we assume that the TBC is secure and has long tweaks. The assumption is relevant as there are practical designs with long tweaks, e.g., SKINNY [BJK+16], and there are also known tweak length extension schemes [MI15].

Our target construction is illustrated in Fig. 1(d), which is the r-round version of the construction in [Min15] (Fig. 1(b)). Given an n-bit TBC with τn-bit tweaks, this gives a dn-bit block cipher for $d = \tau + 1$. We show the following three results.

1. In Sect. 5, we show that $r = 3d - 2$ rounds are enough for the security up to $2^{dn/2}$ queries, i.e., the security remains the same as the $3d$-round construction of Minematsu even if we reduce the number of rounds by two.

[1] [CDMS10] shows a construction of a $2n$-bit TBC from n-bit TBCs with longer tweaks. The argument here considers the special case where the tweak length of the $2n$-bit TBC is zero. See [CDMS10] for details.

2. In Sect. 6, we consider the case where the number of queries made by an adversary is limited. Seeing a lot of practical constructions of a TBC with $n = 128$, guaranteeing the security up to $2^{dn/2}$ queries can be overkill even for a small d like $d = 3$. When the number of queries is limited to 2^n, which is still sufficiently large in practice when $n = 128$, we show that $d + 1$ rounds are enough to achieve the security bound of $O(q^2/2^{2n})$.

   Furthermore, with $r = d + \ell$ rounds for $1 \leq \ell \leq d - 1$, we obtain the security bound of $O(q^2/2^{(1+\ell)n})$, i.e., the security bound improves as ℓ grows.

3. In Sect. 7, we prove that with $r = d$ rounds, the security bound is the classical birthday-bound of $O(q^2/2^n)$. This can be regard as the case $\ell = 0$ of the second result.

We also show that the birthday-bound $O(q^2/2^n)$ of $r = d$ round version is tight by presenting a matching attack in Sect. 8, while the tightness of the security bounds of $r = d + \ell$ round versions for $\ell \geq 1$ is left as an open question.

Table 1 summaries these results. Our results show that a block cipher with BBB security (with respect to n) is obtained as low as $d + 1$ rounds, and we draw the security spectrum of $d + \ell$ round version in the range of $1 \leq \ell \leq d - 1$ and $\ell = 2d - 2$ for BBB security, and $\ell = 0$ for birthday-bound security. Note that, in this paper, we use BBB security to mean that the construction remains secure beyond $q \approx 2^{n/2}$ queries with respect n, the block length of the underlying primitive, which is the output length and *not* the input length. When we let $d = 2$, then we obtain the result of Coron et al. [CDMS10], and hence our result can be considered as the generalization.

We clarify that our work is a domain extension of TBCs, rather than constructing a stronger block cipher from a weaker TBC, i.e., our results assume that underlying TBCs are secure as a tweakable strong pseudorandom permutation (TSPRP) [LRW02, LRW11].

Implication. Our results can be used to obtain a BBB secure block cipher by instantiating the TBC with any secure practical design. For instance if we use a version of SKINNY with $n = 128$ bit blocks, $t = 256$ bit tweaks, and 128-bit keys (or 384-bit "tweakey"), which corresponds to $\tau = 2$ and $d = 3$, we obtain a 384-bit block cipher with $128r$-bit keys for r rounds. The result in [Min15] shows that with 9 rounds, the distinguishing probability is $O(q^2/2^{384})$ for q queries, while we show that with only 7 rounds, it is already $O(q^2/2^{384})$. If we consider adversaries that make at most $q \leq 2^{128}$ queries, then the distinguishing probability is $O(q^2/2^{384})$ with 5 rounds, it is $O(q^2/2^{256})$ with 4 rounds, and it is $O(q^2/2^{128})$ with 3 rounds. We show the relationship between the number of rounds and the security in Fig. 2.

We comment that as the construction is iterative, this could be seen as the soundness proof of the structure. That is, the results of Luby and Rackoff can be interpreted that the Feistel permutation is a sound structure to obtain an SPRP from a PRF. In practical designs, however, we do not use a PRF but instantiate it with an imperfect round function and increase the number of rounds to meet efficiency requirements. Our result could be seen as an alternative way to obtain an SPRP, where the TBC could be instantiated with an "imperfect TBC," and we could build a practically efficient block cipher by using the structure as a starting point of dedicated designs.

Related Work. As related works, Chen et al. [CLMP17, CMN18] studied constructions of enciphering schemes, that can be considered as a block cipher that takes any bit strings of length from n bits to $2n - 1$ bits. The result can be seen as the generalization of the results in [CDMS10] to handle flexible input lengths. Unlike their work, this paper considers a fixed input length that is determined by the block and tweak lengths of the underlying TBC. Related to the enciphering scheme using a TBC, Bhaumik et al. [BLN18]

Table 1: Summary of our results and other related block ciphers based only on a TBC. (n, t) in TBC denotes an n-bit TBC with t-bit tweaks. Note that $d = \tau + 1$, and the bounds neglect constants. For the TBC calls of the result in Sect. 6, $\ell = 1, \ldots, d-1$.

Construction	Block (bit)	TBC	TBC Calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Section 5	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Section 6	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Section 7	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

also studied a variable-input-length SPRP which has high efficiency and BBB security. The primal purpose is to construct a highly secure block cipher with the minimal number of TBC calls. Related to [BLN18], Dutta and Nandi [DN18] presented a construction of a tweakable enciphering scheme which also has BBB security. The work of [DN18] can be seen as a construction of a variable-input-length TBC from a fixed-input-length TBC. Shrimpton and Terashima proposed a construction of a variable-input-length TBC called PIV by combining a fixed-input-TBC and a variable-input-length TBC [ST13]. It consists of 3 rounds and is similar to [CDMS10] when the input-length is fixed. The construction we consider in this paper is simpler but is not flexible in the input length, and does not take a tweak as input. However, since the construction is iterative, it is flexible in that it gives trade-off between the security and number of rounds.

In addition to these (tweakable) enciphering schemes, there is a long history of constructions of (tweakable) enciphering schemes from block ciphers (rather than TBCs), including NR-mode [NR99], CMC [HR03], EME [HR04], EME* [Hal04], HCTR [WFW05], PEP [CS06a], HCH [CS06b], TET [Hal07], HEH [Sar07], and XCB [MF07]. See also [Sar09, BN15].

2 Preliminaries

Notation. For a positive integer n, $\{0,1\}^n$ is the set of bit strings of length n bits. We write $x \,\|\, y$ for the concatenation of two bit strings x and y. For two integers a and b with $a \leq b$, we let $[a..b] = \{a, a+1, \ldots, b\}$. For (possibly negative) integers a, b, c and a positive integer d with $c + 1 \leq a \leq b \leq c + d$, and d strings $X^{c+1}, \ldots, X^{c+d} \in \{0,1\}^n$ of length n bits, we write $X^{[a..b]} = X^a \,\|\, X^{a+1} \,\|\, \cdots \,\|\, X^b$, i.e., $X^{[a..b]}$ is a substring of $X^{c+1} \,\|\, \cdots \,\|\, X^{c+d}$ starting from X^a and ending with X^b, inclusive.

For a finite set $\mathcal{S}$, $s \xleftarrow{\$} \mathcal{S}$ denotes the process of uniformly random selection of an element from $\mathcal{S}$, and assigning it to s.

For a keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, where $\mathcal{K}$ is the key space, $\mathcal{X}$ is the domain, and $\mathcal{Y}$ is the range, we interchangeably write $Y = F(K, X)$, $Y = F_K(X)$, or $Y = F[K](X)$. If for any $K \in \mathcal{K}$, $F_K(\cdot)$ is a permutation over $\mathcal{X}$, then we write $F^{-1}(K, \cdot)$, $F_K^{-1}(\cdot)$, or $F^{-1}[K](\cdot)$ for its inverse function.

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 n is the block length and $\mathcal{K}$ is the key space, and for any key $K \in \mathcal{K}$, $E_K(\cdot)$ is a permutation over $\{0,1\}^n$. The ciphertext $C \in \{0,1\}^n$ for a key $K \in \mathcal{K}$ and a plaintext $M \in \{0,1\}^n$ is $C = E_K(M)$. The decryption function is

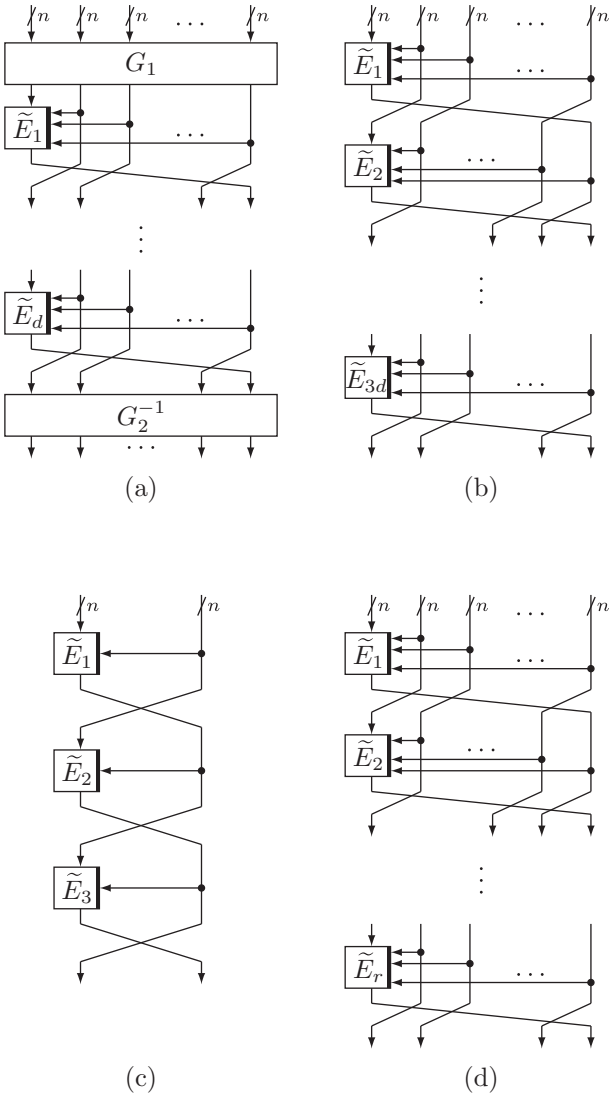


Figure 1: The constructions of previous works and the construction we study in this paper. (a) and (b) are Minematsu's constructions [Min15] and (c) is Coron et al.'s construction [CDMS10]. We prove the security of (d) for various values of r.

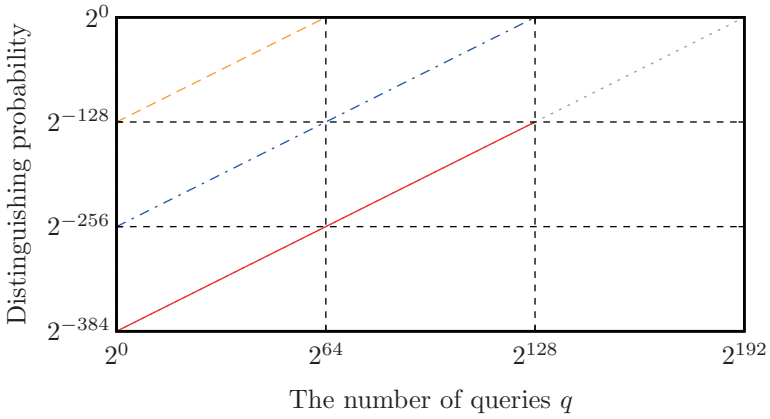


Figure 2: Comparison of security bounds with $d = 3$ and $n = 128$. The orange dashed line (- - -) shows the upper bound on the distinguishing probability of 3 rounds, the blue chain line (-·-·-) shows 4 rounds, the red solid line (——) shows 5 rounds, and the red solid line and violet dotted line (·····) together show 7 rounds (and they also show the result of 9 rounds in [Min15]). Note that the security bound of the 5-round version is only proved in the range of $q \leq 2^{128}$.

$E_K^{-1}(\cdot)$, and the plaintext M for a key K and a ciphertext C is $M = E_K^{-1}(C)$. We say that $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ is an n-bit BC.

A tweakable block cipher (TBC), introduced by Liskov, Rivest, and Wagner [LRW02, LRW11], is a keyed permutation with an auxiliary input called a tweak, i.e., a TBC is a family of keyed permutations indexed by the tweak. Let n and t be positive integers, where n is the block length and t is the tweak length. A TBC with key space $\mathcal{K}$ is $\widetilde{E} : \mathcal{K} \times \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$, and we call it an (n,t)-bit TBC. A ciphertext $C \in \{0,1\}^n$ of the TBC for a key $K \in \mathcal{K}$, a plaintext $M \in \{0,1\}^n$, and a tweak $T \in \{0,1\}^t$ is $C = \widetilde{E}(K,M,T) = \widetilde{E}_K(M,T)$. We require that for any $K \in \mathcal{K}$ and $T \in \{0,1\}^t$, $\widetilde{E}_K(\cdot,T)$ is a permutation over $\{0,1\}^n$, and we write the decryption function of the TBC as $M = \widetilde{E}_K^{-1}(C,T)$.

Let $\mathrm{Perm}(n)$ denote the set of all permutations on $\{0,1\}^n$, and we say that $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ is a random permutation on $\{0,1\}^n$. Let $\widetilde{\mathrm{Perm}}(n,t)$ denote the set of all functions $\widetilde{P} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ such that for every $T \in \{0,1\}^t$, $\widetilde{P}(\cdot,T) \in \mathrm{Perm}(n)$, and we say that $\widetilde{P} \xleftarrow{\$} \widetilde{\mathrm{Perm}}(n,t)$ is an (n,t)-bit random tweakable permutation. We see that for any $T \in \{0,1\}^t$, $\widetilde{P}(\cdot,T)$ is a random permutation on $\{0,1\}^n$, and we write $\widetilde{P}^{-1}(\cdot,T)$ for the inverse function of $\widetilde{P}(\cdot,T)$.

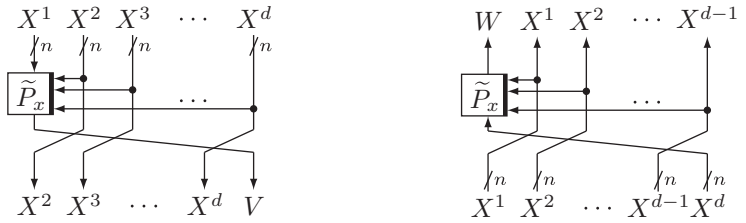
3 dn-bit BC from $(n, \tau n)$-bit TBC with $d = \tau + 1$

Let $r \geq 1$ be the number of rounds, and suppose that we have r independent $(n,\tau n)$-bit TBCs $\widetilde{P}_1, \ldots, \widetilde{P}_r$. We consider a construction of a dn-bit BC from $\widetilde{P}_1, \ldots, \widetilde{P}_r$, where $d = \tau + 1$.

We first define one encryption round ε. It takes $(X^1 \,\|\, \cdots \,\|\, X^d) \in \{0,1\}^{dn}$ as input and $\widetilde{P}_x \in \mathrm{Perm}(n,\tau n)$ for some $x \in [1..r]$ as a key, and works as follows (see Fig. 3(a)).

$$\varepsilon[\widetilde{P}_x](X^1 \,\|\, \cdots \,\|\, X^d) = (X^2 \,\|\, \cdots \,\|\, X^d \,\|\, V)\,,$$

where $V = \widetilde{P}_x(X^1, X^2 \,\|\, \cdots \,\|\, X^d)$. Note that one encryption round is a permutation on



(a) (b)

Figure 3: (a) $\varepsilon[\widetilde{P}_x](X^1 \,\|\, \cdots \,\|\, X^d) = (X^2 \,\|\, \cdots \,\|\, X^d \,\|\, V)$ (b) $\varepsilon^{-1}[\widetilde{P}_x](X^1 \,\|\, \cdots \,\|\, X^d) = (W \,\|\, X^1 \,\|\, \cdots \,\|\, X^{d-1})$

$\{0,1\}^{dn}$, and one decryption round ε^{-1} is naturally defined by using the decryption of $\widetilde{P}_x$, which we write as $\widetilde{P}_x^{-1}$, as follows (see Fig. 3(b)).

$$\varepsilon^{-1}[\widetilde{P}_x](X^1 \,\|\, \cdots \,\|\, X^d) = (W \,\|\, X^1 \,\|\, \cdots \,\|\, X^{d-1})\,,$$

where $W = \widetilde{P}_x^{-1}(X^d, X^1 \,\|\, \cdots \,\|\, X^{d-1})$.

We now define the r-round encryption algorithm $\mathcal{E}_r$ of the dn-bit BC. It takes $M \in \{0,1\}^{dn}$ as input and $\widetilde{P}_1, \ldots, \widetilde{P}_r$ as a key, and successively applies $\varepsilon[\widetilde{P}_1], \ldots, \varepsilon[\widetilde{P}_r]$ on M, i.e.,

$$\mathcal{E}_r[\widetilde{P}_1, \ldots, \widetilde{P}_r](M) = \varepsilon[\widetilde{P}_r] \circ \varepsilon[\widetilde{P}_{r-1}] \circ \cdots \circ \varepsilon[\widetilde{P}_1](M)\,.$$

We will omit $\widetilde{P}_1, \ldots, \widetilde{P}_r$ and write $\mathcal{E}_r$ if $\widetilde{P}_1, \ldots, \widetilde{P}_r$ are clear from the context. The r-round decryption algorithm $\mathcal{E}_r^{-1}$ takes $C \in \{0,1\}^{dn}$ as input and $\widetilde{P}_1, \ldots, \widetilde{P}_r$ as a key, and is defined as

$$\mathcal{E}_r^{-1}[\widetilde{P}_1, \ldots, \widetilde{P}_r](C) = \varepsilon^{-1}[\widetilde{P}_1] \circ \varepsilon^{-1}[\widetilde{P}_2] \circ \cdots \circ \varepsilon^{-1}[\widetilde{P}_r](C)\,.$$

We note that the original definition by Minematsu in [Min15] uses an (n, dn)-bit TBC to define the dn-bit BC, where one of the d tweak inputs is used for the domain separation. The above formulation is the same as the original one by assuming that we have r independently keyed $(n, (d-1)n)$-bit TBCs.

4 Security Definitions and Coefficient-H Technique

Let $\mathcal{E}_r$ and $\mathcal{E}_r^{-1}$ be the encryption and decryption algorithms of the dn-bit BC, $\pi \xleftarrow{\$} \mathrm{Perm}(dn)$ be a random permutation, and π^{-1} be the inverse function of π.

We consider the security of $\mathcal{E}_r$ as a strong pseudorandom permutation (SPRP) [LR88]. For an adversary $\mathcal{A}$ that makes at most q queries, we define

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

where the first probability is taken over the randomness of $\mathcal{A}$ and the key $\widetilde{P}_1, \ldots, \widetilde{P}_r$ of $\mathcal{E}_r$ and $\mathcal{E}_r^{-1}$, and the last probability is taken over $\mathcal{A}$ and π.

As the security of an (n,t)-bit TBC $\widetilde{E}$, we consider a tweakable SPRP (TSPRP) [LRW02, LRW11]. For an adversary $\mathcal{A}$ that makes at most q queries, we define

$$\mathbf{Adv}^{\mathrm{tsprp}}_{\widetilde{E}}(\mathcal{A}) = \left| \Pr[\mathcal{A}^{\widetilde{E}_K(\cdot,\cdot), \widetilde{E}_K^{-1}(\cdot,\cdot)} = 1] - \Pr[\mathcal{A}^{\widetilde{P}(\cdot,\cdot), \widetilde{P}^{-1}(\cdot,\cdot)} = 1] \right|,$$

where the first probability is taken over $\mathcal{A}$ and the key K, and the last probability is taken over $\mathcal{A}$ and $\widetilde{P} \xleftarrow{\$} \widetilde{\mathrm{Perm}}(n,t)$.

Our security proofs rely on the Coefficient-H technique by Patarin [Pat08] and its refinement by Chen and Steinberger [CS14]. We follow [CS14] and we leak some of the internal variables to $\mathcal{A}$ during the computation of $\mathcal{E}_r(\cdot)$ and $\mathcal{E}_r^{-1}(\cdot)$, and we make necessary modifications to $\pi(\cdot)$ and $\pi^{-1}(\cdot)$ to eliminate the obvious discrepancy. Let $\mathcal{R}(\cdot)$ and $\mathcal{R}^{-1}(\cdot)$ be the oracles that implement the real world (i.e., oracles to compute $\mathcal{E}_r(\cdot)$ and $\mathcal{E}_r^{-1}(\cdot)$), and $\mathcal{I}(\cdot)$ and $\mathcal{I}^{-1}(\cdot)$ be the oracles that implement the ideal world ($\pi(\cdot)$ and $\pi^{-1}(\cdot)$).

Since $\mathcal{A}$ makes at most q queries, we can define a transcript θ that summarizes all query-response tuples seen by $\mathcal{A}$ during its interaction with $\mathcal{R}(\cdot)$ and $\mathcal{R}^{-1}(\cdot)$, or $\mathcal{I}(\cdot)$ and $\mathcal{I}^{-1}(\cdot)$. We denote by $\Theta_{\mathcal{R}}$ (resp. $\Theta_{\mathcal{I}}$) the probability distribution of transcripts when $\mathcal{A}$ interacts with $\mathcal{R}(\cdot)$ and $\mathcal{R}^{-1}(\cdot)$ (resp. $\mathcal{I}(\cdot)$ and $\mathcal{I}^{-1}(\cdot)$). We call a transcript θ attainable if $\Pr[\Theta_{\mathcal{I}} = \theta] > 0$, i.e., if θ can be obtained with interacting $\mathcal{I}(\cdot)$ and $\mathcal{I}^{-1}(\cdot)$. Let $\mathsf{T}_{\mathrm{all}}$ be the set of all attainable transcripts. Then, the Coefficient-H technique is the following lemma.

Lemma 1. *Consider a deterministic adversary $\mathcal{A}$. Let $\mathsf{T}_{\mathrm{bad}}$ be the subset of $\mathsf{T}_{\mathrm{all}}$ with all "bad" transcripts, and $\mathsf{T}_{\mathrm{good}} = \mathsf{T}_{\mathrm{all}} \setminus \mathsf{T}_{\mathrm{bad}}$. Suppose that there exists $0 \le \epsilon \le 1$ such that*

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

holds for all $\theta \in \mathsf{T}_{\mathrm{good}}$. Then we have $\mathbf{Adv}^{\mathrm{sprp}}_{\mathcal{E}_r}(\mathcal{A}) \le \epsilon + \Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}]$.

5 Security of $\mathcal{E}_{3d-2}$ for $q \le 2^{dn/2}$

In this section, we prove that the dn-bit BC $\mathcal{E}_{3d-2}$ is BBB secure.

Theorem 1. *Fix $d \ge 2$. For $x \in [1..3d-2]$, let $\widetilde{P}_x : \{0,1\}^n \times \{0,1\}^{(d-1)n} \to \{0,1\}^n$ be a random tweakable permutation, and consider $\mathcal{E}_{3d-2} = \mathcal{E}_{3d-2}[\widetilde{P}_1, \ldots, \widetilde{P}_{3d-2}]$. Then for any $\mathcal{A}$ that makes at most $q \le 2^{dn/2}$ queries, it holds that*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathcal{E}_{3d-2}}(\mathcal{A}) \le \frac{0.5dq^2}{2^{dn}}\,.$$

Proof. Without loss of generality, we assume that $\mathcal{A}$ is deterministic, makes exactly q queries, does not repeat a query, and does not make a redundant query, i.e., if $\mathcal{A}$ makes an encryption query M and obtains C, then it does not make a decryption query C, and vice versa. We start with defining the oracles $(\mathcal{R}, \mathcal{R}^{-1})$ and $(\mathcal{I}, \mathcal{I}^{-1})$.

Oracle $\mathcal{R}$ represents $\mathcal{E}_{3d-2}$ and $\mathcal{R}^{-1}$ is its inverse, and we call $(\mathcal{R}, \mathcal{R}^{-1})$ the real world. Oracle $\mathcal{I}$ represents a random permutation $\pi \xleftarrow{\$} \mathrm{Perm}(dn)$ and $\mathcal{I}^{-1}$ is its inverse, and we call $(\mathcal{I}, \mathcal{I}^{-1})$ the ideal world.

Procedures of the Oracles. In the real world, the definitions of $\mathcal{R}$ and $\mathcal{R}^{-1}$ are in Algorithms 1 and 2 in Fig. 4. For the i-th query $M_i^{[1..d]} \in \{0,1\}^{dn}$ to $\mathcal{R}$, we compute $C_i^{[1..d]} \in \{0,1\}^{dn}$ by following the definition of $\mathcal{E}_{3d-2}$, and return it to $\mathcal{A}$. We also save $S_i^{[1..2d-2]} \in \{0,1\}^{(2d-2)n}$ that is maintained through S in Fig. 4, which is the $2d-2$ output bit strings of the internal random tweakable permutations in $\mathcal{R}$, and return it to $\mathcal{A}$ after making all the q queries and before $\mathcal{A}$ returns the decision bit. If $d = 3$, then this corresponds to $S_i^{[1..4]}$ in Fig. 5. $\mathcal{R}^{-1}$ is similarly defined, and for a decryption query $C_i^{[1..d]}$, $\mathcal{A}$ obtains $M_i^{[1..d]}$ during the interaction and $S_i^{[1..2d-2]}$ after making all the queries.

In the ideal world, we define $\mathcal{I}$ and $\mathcal{I}^{-1}$ as in Algorithms 3 and 4 in Fig. 6. $\mathcal{I}$ and $\mathcal{I}^{-1}$ internally maintain $\widetilde{P}_1, \ldots, \widetilde{P}_{d-1}$ and $\widetilde{P}_{2d}, \ldots, \widetilde{P}_{3d-2}$, generate "dummy" internal variable $S_i^{[1..2d-2]}$, and return it to $\mathcal{A}$ after making all the q queries but before it outputs 0/1. More

precisely, $S_i^1, \ldots, S_i^{d-1}$ are generated by random tweakable permutations $\widetilde{P}_1, \ldots, \widetilde{P}_{d-1}$, and $S_i^d, \ldots, S_i^{2d-2}$ are generated by $\widetilde{P}_{2d}^{-1}, \ldots, \widetilde{P}_{3d-2}^{-1}$.

The adversary $\mathcal{A}$ is deterministic and makes q queries to its oracles, and it also receives $S_i^{[1..2d-2]}$ for $i \in [1..q]$. Therefore, these queries and responses are summarized in a transcript

$$\theta = \{(M_i^1, \ldots, M_i^d, C_i^1, \ldots, C_i^d, S_i^1, \ldots, S_i^{2d-2}) \mid i = 1, \ldots, q\}.$$

Since $\mathcal{A}$ does not repeat a query, $M_i^{[1..d]} \neq M_j^{[1..d]}$ and $C_i^{[1..d]} \neq C_j^{[1..d]}$ hold for any $1 \leq j < i \leq q$.

Bad Transcript. In the real world, for $x \in [1..3d-2]$, each encryption round $\varepsilon[\widetilde{P}_x]$ is a permutation over $\{0,1\}^{dn}$. Then, each output of $\varepsilon[\widetilde{P}_x]$ is not repeated since $\mathcal{A}$ does not repeat a query. Therefore, the following $(3d-3) \times \binom{q}{2}$ collisions cannot appear in θ.

$$\mathsf{Bad}_1 \begin{cases} 1 \leq \exists j < \exists i \leq q, M_i^{[2..d]} \parallel S_i^1 = M_j^{[2..d]} \parallel S_j^1 \\ \vdots \\ 1 \leq \exists j < \exists i \leq q, M_i^d \parallel S_i^{[1..d-1]} = M_j^d \parallel S_j^{[1..d-1]} \end{cases}$$

$$\mathsf{Bad}_2 \begin{cases} 1 \leq \exists j < \exists i \leq q, S_i^{[1..d]} = S_j^{[1..d]} \\ \vdots \\ 1 \leq \exists j < \exists i \leq q, S_i^{[d-1..2d-2]} = S_j^{[d-1..2d-2]} \end{cases}$$

$$\mathsf{Bad}_3 \begin{cases} 1 \leq \exists j < \exists i \leq q, S_i^{[d..2d-2]} \parallel C_i^1 = S_j^{[d..2d-2]} \parallel C_j^1 \\ \vdots \\ 1 \leq \exists j < \exists i \leq q, S_i^{2d-2} \parallel C_i^{[1..d-1]} = S_j^{2d-2} \parallel C_j^{[1..d-1]} \end{cases}$$

Here, each of Bad_1, Bad_2, and Bad_3 is the set of $(d-1) \times \binom{q}{2}$ collisions. As an example, if $d = 3$ (see Fig. 5), they can be described as

$$\begin{aligned}
\mathsf{Bad}_1 &= \{1 \leq \exists j < \exists i \leq q,\ M_i^2 \parallel M_i^3 \parallel S_i^1 = M_j^2 \parallel M_j^3 \parallel S_j^1\} \\
&\quad \cup \{1 \leq \exists j < \exists i \leq q,\ M_i^3 \parallel S_i^1 \parallel S_i^2 = M_j^3 \parallel S_j^1 \parallel S_j^2\}, \\
\mathsf{Bad}_2 &= \{1 \leq \exists j < \exists i \leq q,\ S_i^1 \parallel S_i^2 \parallel S_i^3 = S_j^1 \parallel S_j^2 \parallel S_j^3\} \\
&\quad \cup \{1 \leq \exists j < \exists i \leq q,\ S_i^2 \parallel S_i^3 \parallel S_i^4 = S_j^2 \parallel S_j^3 \parallel S_j^4\}, \\
\mathsf{Bad}_3 &= \{1 \leq \exists j < \exists i \leq q,\ S_i^3 \parallel S_i^4 \parallel C_i^1 = S_j^3 \parallel S_j^4 \parallel C_j^1\} \\
&\quad \cup \{1 \leq \exists j < \exists i \leq q,\ S_i^4 \parallel C_i^1 \parallel C_i^2 = S_j^4 \parallel C_j^1 \parallel C_j^2\}.
\end{aligned}$$

Since one encryption round is a permutation over $\{0,1\}^{dn}$ and $\mathcal{A}$ does not repeat a query, the six internal states $(M_i^2 \parallel M_i^3 \parallel S_i^1)$, $(M_i^3 \parallel S_i^1 \parallel S_i^2)$, $(S_i^1 \parallel S_i^2 \parallel S_i^3)$, $(S_i^2 \parallel S_i^3 \parallel S_i^4)$, $(S_i^3 \parallel S_i^4 \parallel C_i^1)$, and $(S_i^4 \parallel C_i^1 \parallel C_i^2)$ are not repeated. This means that no collision in $\mathsf{Bad}_1 \cup \mathsf{Bad}_2 \cup \mathsf{Bad}_3$ can happen in the real world.

On the other hand, in the ideal world, $S_i^1, \ldots, S_i^{d-1}$ are generated to avoid collisions in Bad_1, and $S_i^d, \ldots, S_i^{2d-2}$ are generated to avoid collisions in Bad_3 in both query directions. Only collisions in Bad_2 can happen in both query directions. We define the set of bad transcripts as

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \text{a collision in } \mathsf{Bad}_2 \text{ occurs}\}.$$

Note that Bad_1 and Bad_3 cannot happen in both worlds.

We now prove the following lemma.

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

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

Figure 4: Oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$. After q queries, S is given to $\mathcal{A}$.

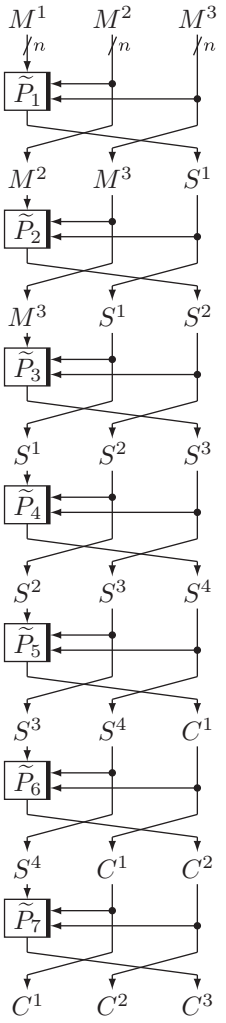


Figure 5: $\mathcal{E}_{3d-2}$ with $d = 3$

Algorithm 3: 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. $S_i^1 \leftarrow \widetilde{P}_1(M_i^1, M_i^{[2..d]})$
3. **for** $x = 2, \ldots, d-1$ **do**
   $S_i^x \leftarrow \widetilde{P}_x(M_i^x, M_i^{[x+1..d]} \,\|\, S_i^{[1..x-1]})$
4. $(S_i^{2d-1}, \ldots, S_i^{3d-2}) \leftarrow (C_i^1, \ldots, C_i^d)$
5. **for** $x = 3d-2, \ldots, 2d$ **do**
   $S_i^{x-d} \leftarrow \widetilde{P}_x^{-1}(S_i^x, S_i^{[x-d+1..x-1]})$
6. **return** $C_i^{[1..d]}$
7. $\mathsf{S} \leftarrow \mathsf{S} \,\|\, S_i^{[1..2d-2]}$

Algorithm 4: 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. $S_i^1 \leftarrow \widetilde{P}_1(M_i^1, M_i^{[2..d]})$
3. **for** $x = 2, \ldots, d-1$ **do**
   $S_i^x \leftarrow \widetilde{P}_x(M_i^x, M_i^{[x+1..d]} \,\|\, S_i^{[1..x-1]})$
4. $(S_i^{2d-1}, \ldots, S_i^{3d-2}) \leftarrow (C_i^1, \ldots, C_i^d)$
5. **for** $x = 3d-2, \ldots, 2d$ **do**
   $S_i^{x-d} \leftarrow \widetilde{P}_x^{-1}(S_i^x, S_i^{[x-d+1..x-1]})$
6. **return** $M_i^{[1..d]}$
7. $\mathsf{S} \leftarrow \mathsf{S} \,\|\, S_i^{[1..2d-2]}$

Figure 6: Oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$. After q queries, S is given to $\mathcal{A}$.

Lemma 2. $\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \le \dfrac{0.5(d-1)q^2}{2^{dn}}$.

Proof. We consider $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. For $x \in [1..d-1]$ and $1 \le j < i \le q$, we have

$$\Pr[S_i^{[x..x+d-1]} = S_j^{[x..x+d-1]}] \le \Pr[S_i^x = S_j^x] \cdots \Pr[S_i^{x+d-1} = S_j^{x+d-1}] \le \frac{1}{2^n} \cdots \frac{1}{2^n} = \frac{1}{2^{dn}}\,.$$

Note that $S_1^{[1..2d-2]}, \ldots, S_q^{[1..2d-2]}$ are given to $\mathcal{A}$ simultaneously after making all the q queries, and hence for any $x \in [1..2d-2]$, S_i^x is a random variable from the randomness of $\widetilde{P}_1, \ldots, \widetilde{P}_{d-1}$ and $\widetilde{P}_{2d}, \ldots, \widetilde{P}_{3d-2}$, and from the fact that they take distinct inputs during the computation. That is, if the i-th query and j-th query have the same tweak, then we have $\Pr[S_i^x = S_j^x] = 0$, and $\Pr[S_i^x = S_j^x] = 1/2^n$ when the tweaks are different.

Therefore, we have

$$\begin{aligned}\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &\le \sum_{x \in [1..d-1]} \sum_{i \in [2..q]} \sum_{j \in [1..i-1]} \Pr[S_i^{[x..x+d-1]} = S_j^{[x..x+d-1]}] \\ &\le \sum_{i \in [2..q]} \frac{(d-1)(i-1)}{2^{dn}} \\ &\le \frac{0.5(d-1)q^2}{2^{dn}}\,.\end{aligned}$$

□

$\Pr[\Theta_{\mathcal{R}} = \theta] / \Pr[\Theta_{\mathcal{I}} = \theta]$. We consider $\theta \in \mathsf{T}_{\mathrm{good}}$. In the real world, for $1 \le x \le 3d-2$, we define $\mathcal{T}_1^x = \emptyset$ and for $2 \le i \le q$,

$$\mathcal{T}_i^x = \{j \mid j < i \text{ and } (i\text{-th tweak of } \widetilde{P}_x) = (j\text{-th tweak of } \widetilde{P}_x)\}\,.$$

$\mathcal{T}_i^x$ is the set of all indices $1 \le j < i$ such that the i-th tweak of $\widetilde{P}_x$ is the same as the j-th tweak of $\widetilde{P}_x$.

Then we have

$$\Pr[\Theta_{\mathcal{R}} = \theta] = \prod_{x\in[1..3d-2]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \geq \frac{1}{2^{dnq}} \cdot \left(\prod_{x\in[1..d-1]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \right) \cdot \left(\prod_{x\in[2d..3d-2]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \right).$$

In the ideal world, for $1 \leq x \leq d-1$ and $2d \leq x \leq 3d-2$ and for $1 \leq i \leq q$, we define $\mathcal{T}_i^x$ as in the real world. Then we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \left(\prod_{i\in[1..q]} \frac{1}{2^{dn} - (i-1)} \right) \cdot \left(\prod_{x\in[1..d-1]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \right) \cdot \left(\prod_{x\in[2d..3d-2]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \right).$$

Then, from $q \leq 2^{dn/2}$, we have

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

From Lemma 1 and Lemma 2, we have Theorem 1. □

We note that the tightness of the security bound of Theorem 1 is left as an open question. We also note that if we use a tweakable strong pseudorandom permutation (TSPRP) [LRW02, LRW11] as the underlying TBC, then the corresponding computational security bound is obtained as in [Min15].

6 Security of $\mathcal{E}_{d+1}, \ldots, \mathcal{E}_{2d-1}$ for $q \leq 2^n$

In this section, we prove that the dn-bit BC $\mathcal{E}_{d+\ell}$ for $1 \leq \ell \leq d-1$ is BBB secure under the assumption of $q \leq 2^n$.

Theorem 2. *Fix $d \geq 2$ and $\ell \in [1..d-1]$. For $x \in [1..d+\ell]$, let $\widetilde{P}_x : \{0,1\}^n \times \{0,1\}^{(d-1)n} \to \{0,1\}^n$ be a random tweakable permutation, and consider $\mathcal{E}_{d+\ell} = \mathcal{E}_{d+\ell}[\widetilde{P}_1, \ldots, \widetilde{P}_{d+\ell}]$. Then for any $\mathcal{A}$ that makes at most $q \leq 2^n$ queries, it holds that*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathcal{E}_{d+\ell}}(\mathcal{A}) \leq \frac{dq^2}{2^{(1+\ell)n}}.$$

Proof. We assume without loss of generality that $\mathcal{A}$ is deterministic, makes exactly q queries, does not repeat a query, and does not make a redundant query. We first define the oracles $(\mathcal{R}, \mathcal{R}^{-1})$ and $(\mathcal{I}, \mathcal{I}^{-1})$.

Procedures of the Oracles. The oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$ represent the real world and implement $\mathcal{E}_{d+\ell}$ and $\mathcal{E}_{d+\ell}^{-1}$, and the oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$ represent the ideal world and implement π and π^{-1}.

In the real world, the definitions of $\mathcal{R}$ and $\mathcal{R}^{-1}$ are in Algorithms 5 and 6 in Fig. 7. For the i-th query $M_i^{[1..d]} \in \{0,1\}^{dn}$ to $\mathcal{R}$, we compute $C_i^{[1..d]} \in \{0,1\}^{dn}$ by following the definition of $\mathcal{E}_{d+\ell}$, and return it to $\mathcal{A}$. We also compute $S_i^{[1..\ell]} \in \{0,1\}^{\ell n}$, which is the ℓ output bit strings of internal random tweakable permutations in $\mathcal{R}$, and return it to

$\mathcal{A}$. If $d = 3$, then this corresponds to S_i^1 in Fig. 9. $\mathcal{R}^{-1}$ is similarly defined, and for a decryption query $C_i^{[1..d]}$, $\mathcal{A}$ obtains $M_i^{[1..d]}$ and $S_i^{[1..\ell]}$ during the interaction. Note that this is different from the proof of Theorem 1, where the additional information is given to the adversary after making all the queries but before it outputs the decision bit.

In the ideal world, we define $\mathcal{I}$ and $\mathcal{I}^{-1}$ as in Algorithms 7 and 8 in Fig. 8. For each query, $\mathcal{I}$ and $\mathcal{I}^{-1}$ generate "dummy" internal variables $S_i^{[1..\ell]}$, and give them to $\mathcal{A}$. Intuitively, if the i-th query is an encryption query, then we generate S_i^x for $x \in [1..\ell]$ by simulating $\widetilde{P}_x$. We use $\mathcal{S}_i^x$ as the record of the output values that share the same tweak in the first $i-1$ queries. If the i-th query is a decryption query, then we use $\widetilde{P}_{d+x}^{-1}$ instead of $\widetilde{P}_x$.

We remark that we used dummy permutations in Algorithms 3 and 4 in Fig. 6, while we use the so-called lazy-sampling in Algorithms 7 and 8 in Fig. 8. This is because in the latter case, the randomness to generate certain S_i^x changes depending on the direction of the query. For instance, S_1 in Fig. 9, when interpreted in the ideal world, is generated with $\widetilde{P}_1$ in encryption, but this is generated with $\widetilde{P}_4$ in decryption. This type of switching does not happen in Algorithms 3 and 4, and hence lazy-sampling is not necessary and dummy permutations work fine.

We see that as long as $\mathcal{I}$ and $\mathcal{I}^{-1}$ simulate $\widetilde{P}_x$ and $\widetilde{P}_{d+x}^{-1}$ as in Algorithms 7 and 8 in Fig. 8 (that is, if $\theta \notin \mathsf{T}_{\mathrm{bad}}$ holds defined below), the probability distribution of $S_1^{[1..\ell]}, \ldots, S_q^{[1..\ell]}$ is equal to the one in the real world.

The adversary $\mathcal{A}$ is deterministic and makes q queries to its oracles, and it also receives $S_i^{[1..\ell]}$ for $i \in [1..q]$. These queries and responses are summarized in a transcript

$$\theta = \{(M_i^1, \ldots, M_i^d, C_i^1, \ldots, C_i^d, S_i^1, \ldots, S_i^\ell) \mid i = 1, \ldots, q\}.$$

Since $\mathcal{A}$ does not repeat any query, $M_i^{[1..d]} \neq M_j^{[1..d]}$ and $C_i^{[1..d]} \neq C_j^{[1..d]}$ hold for any $1 \le j < i \le q$.

Bad Transcript. In the real world, for $x \in [1..d+\ell]$, each encryption round $\varepsilon[\widetilde{P}_x]$ is a permutation over $\{0,1\}^{dn}$, and hence each output of $\varepsilon[\widetilde{P}_x]$ is not repeated as we assume that $\mathcal{A}$ does not repeat a query. It follows that the following $(d+\ell-1) \times \binom{q}{2}$ collisions cannot appear in θ.

$$\mathsf{Bad}_1 \begin{cases} 1 \le \exists j < \exists i \le q, M_i^{[2..d]} \,\|\, S_i^1 = M_j^{[2..d]} \,\|\, S_j^1 \\ \vdots \\ 1 \le \exists j < \exists i \le q, M_i^{[\ell+1..d]} \,\|\, S_i^{[1..\ell]} = M_j^{[\ell+1..d]} \,\|\, S_j^{[1..\ell]} \end{cases}$$

$$\mathsf{Bad}_2 \begin{cases} 1 \le \exists j < \exists i \le q, M_i^{[\ell+2..d]} \,\|\, S_i^{[1..\ell]} \,\|\, C_i^1 = M_j^{[\ell+2..d]} \,\|\, S_j^{[1..\ell]} \,\|\, C_j^1 \\ \vdots \\ 1 \le \exists j < \exists i \le q, M_i^d \,\|\, S_i^{[1..\ell]} \,\|\, C_i^{[1..d-\ell-1]} = M_j^d \,\|\, S_j^{[1..\ell]} \,\|\, C_j^{[1..d-\ell-1]} \end{cases}$$

$$\mathsf{Bad}_3 \begin{cases} 1 \le \exists j < \exists i \le q, S_i^{[1..\ell]} \,\|\, C_i^{[1..d-\ell]} = S_j^{[1..\ell]} \,\|\, C_j^{[1..d-\ell]} \\ \vdots \\ 1 \le \exists j < \exists i \le q, S_i^\ell \,\|\, C_i^{[1..d-1]} = S_j^\ell \,\|\, C_j^{[1..d-1]} \end{cases}$$

Here, each of Bad_1 and Bad_3 is the set of $\ell \times \binom{q}{2}$ collisions and Bad_2 is the set of $(d-\ell-1) \times \binom{q}{2}$ collisions. As an example, if $d = 3$ and $\ell = 1$ (see Fig. 9), they can be described as

$$\mathsf{Bad}_1 = \{1 \le \exists j < \exists i \le q,\ M_i^2 \,\|\, M_i^3 \,\|\, S_i^1 = M_j^2 \,\|\, M_j^3 \,\|\, S_j^1\},$$

Algorithm 5: Procedure of $\mathcal{R}$ for the i-th query

Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $(C_i^{[1..d]}, S_i^{[1..\ell]}) \in \{0,1\}^{dn+\ell n}$

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

Algorithm 6: Procedure of $\mathcal{R}^{-1}$ for the i-th query

Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $(M_i^{[1..d]}, S_i^{[1..\ell]}) \in \{0,1\}^{dn+\ell n}$

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

Figure 7: Oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$

Algorithm 7: Procedure of $\mathcal{I}$ for the i-th query

Input: $M_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $(C_i^{[1..d]}, S_i^{[1..\ell]}) \in \{0,1\}^{dn+\ell n}$

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

Algorithm 8: Procedure of $\mathcal{I}^{-1}$ for the i-th query

Input: $C_i^{[1..d]} \in \{0,1\}^{dn}$
Output: $(M_i^{[1..d]}, S_i^{[1..\ell]}) \in \{0,1\}^{dn+\ell n}$

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

Figure 8: Oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$

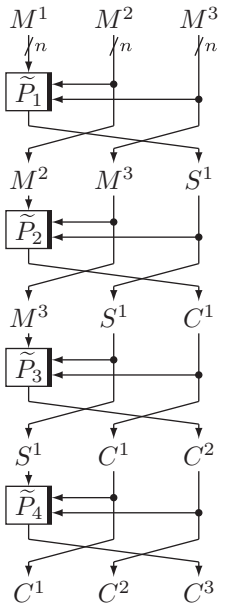


Figure 9: $3n$-bit construction with 4 rounds

$$\mathsf{Bad}_2 = \{1 \le \exists j < \exists i \le q,\ M_i^3 \,\|\, S_i^1 \,\|\, C_i^1 = M_j^3 \,\|\, S_j^1 \,\|\, C_j^1\}\,,$$
$$\mathsf{Bad}_3 = \{1 \le \exists j < \exists i \le q,\ S_i^1 \,\|\, C_i^1 \,\|\, C_i^2 = S_j^1 \,\|\, C_j^1 \,\|\, C_j^2\}\,.$$

Since one encryption round is a permutation over $\{0,1\}^{dn}$ and $\mathcal{A}$ does not repeat a query, the three internal states $(M_i^2 \,\|\, M_i^3 \,\|\, S_i^1)$, $(M_i^3 \,\|\, S_i^1 \,\|\, C_i^1)$, and $(S_i^1 \,\|\, C_i^1 \,\|\, C_i^2)$ are not repeated. This means that no collisions in $\mathsf{Bad}_1 \cup \mathsf{Bad}_2 \cup \mathsf{Bad}_3$ can happen in the real world.

On the other hand, in the ideal world, $S_i^1, \ldots, S_i^\ell$ are generated to avoid collisions in Bad_1 when $\mathcal{A}$'s i-th query is an encryption query and collisions in Bad_3 when $\mathcal{A}$'s i-th query is a decryption query. However, collisions in Bad_1 can happen when $\mathcal{A}$'s i-th query is a decryption query, and collisions in Bad_3 can happen when $\mathcal{A}$'s i-th query is an encryption query. Collisions in Bad_2 can happen if $d \ge 3$ and $1 \le \ell \le d-2$, in both query directions. We define the set of bad transcripts as

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \text{a collision in } \mathsf{Bad}_1 \cup \mathsf{Bad}_2 \cup \mathsf{Bad}_3 \text{ occurs}\}\,.$$

We now prove the following lemma.

Lemma 3. $\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \le \dfrac{(d-1)q^2}{2^{(\ell+1)n}}$.

Proof. We consider $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. Let p_i^1 be the probability that adversary $\mathcal{A}$'s i-th query causes one of the collisions in Bad_1 for the first time (Therefore, for all $1 \le j \le i-1$, the j-th query does not cause any collisions in $\mathsf{Bad}_1 \cup \mathsf{Bad}_2 \cup \mathsf{Bad}_3$). Let p_i^2 and p_i^3 be the probabilities analogously defined for Bad_2 and Bad_3. Then we have $\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \le \sum_{i \in [2..q]} (p_i^1 + p_i^2 + p_i^3)$.

First, let us assume that $\mathcal{A}$'s i-th query is a decryption query, in which case we have $p_i^3 = 0$.

With respect to p_i^1, $M_i^1, \ldots, M_i^d$ are generated by the random permutation, and this implies that we have

$$\begin{aligned} p_i^1 &\leq \sum_{x\in[1..\ell]} \sum_{j\in[1..i-1]} \Pr[M_i^{[x+1..d]} \parallel S_i^{[1..x]} = M_j^{[x+1..d]} \parallel S_j^{[1..x]}] \\ &\leq \sum_{x\in[1..\ell]} \sum_{j\in[1..i-1]} \Pr[M_i^{[x+1..d]} = M_j^{[x+1..d]}] \cdot \Pr[S_i^{[1..x]} = S_j^{[1..x]}] \\ &\leq \sum_{x\in[1..\ell]} \left(\left(\sum_{j\in[1..i-1]} \Pr[S_i^{[1..x]} = S_j^{[1..x]}] \right) \cdot \frac{2^{xn}}{2^{dn} - (i-1)} \right). \end{aligned}$$

Note that $S_j^{[1..\ell]}$ is given to $\mathcal{A}$ along with $M_j^{[1..d]}$ as the reply to the query $C_j^{[1..d]}$, so $S_1^{[1..\ell]}, \ldots, S_{i-1}^{[1..\ell]}$ are fixed strings. From Algorithms 7 and 8, $S_i^{[1..x]}$ is chosen uniformly at random from the set of size exactly $\prod_{y\in[1..x]}(2^n - |\mathcal{S}_i^y|)$. Therefore, we have

$$\Pr[S_i^{[1..x]} = S_j^{[1..x]}] \leq \frac{1}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)}.$$

If $S_j^y \in \mathcal{S}_i^y$ for some $j \in [1..i-1]$ and $y \in [1..x]$, then $S_i^y \neq S_j^y$ holds. This implies that $\Pr[S_i^{[1..x]} = S_j^{[1..x]}] = 0$. Furthermore, for every $z \in [y+1..x]$, we see that $S_j^z \notin \mathcal{S}_i^z$ holds. In other words, if the tweaks of the j-th and i-th queries for $\widetilde{P}_{d+y}$ are the same, then the j-th and i-th tweaks of $\widetilde{P}_{d+y+1}, \ldots, \widetilde{P}_{d+x}$ are all distinct. Since this holds true for all $y \in [1..x]$, the sets $\{j \mid S_j^1 \in \mathcal{S}_i^1\}, \ldots, \{j \mid S_j^x \in \mathcal{S}_i^x\}$ do not contain common elements. It follows that the number of j satisfying $\Pr[S_i^{[1..x]} = S_j^{[1..x]}] = 0$ is at least $\sum_{y\in[1..x]} |\{j \mid S_j^y \in \mathcal{S}_i^y\}| = \sum_{y\in[1..x]} |\mathcal{S}_i^y|$. Therefore, we have

$$\sum_{j\in[1..i-1]} \Pr[S_i^{[1..x]} = S_j^{[1..x]}] \leq \frac{(i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y| \right)}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)}.$$

Also, we can prove the following inequality by using the assumption of $q \leq 2^n$. The proof is elementary, and is presented in Appendix A.[2]

$$\frac{(i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y| \right)}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)} \cdot \frac{1}{2^{dn} - (i-1)} \leq \frac{2(i-1)}{2^{(d+x)n}}. \tag{1}$$

Then, for $q \leq 2^n$, we have

$$\begin{aligned} p_i^1 &\leq \sum_{x\in[1..\ell]} \left(\left(\sum_{j\in[1..i-1]} \Pr[S_i^{[1..x]} = S_j^{[1..x]}] \right) \cdot \frac{2^{xn}}{2^{dn} - (i-1)} \right) \\ &\leq \sum_{x\in[1..\ell]} \left(\frac{(i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y| \right)}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)} \cdot \frac{2^{xn}}{2^{dn} - (i-1)} \right) \end{aligned}$$

[2] This is the only case where we rely on the assumption of $q \leq 2^n$.

$$\leq \sum_{x\in[1..\ell]} \frac{2(i-1)}{2^{(d+x)n}} \cdot 2^{xn} = \frac{2\ell(i-1)}{2^{dn}} .$$

We next consider p_i^2. For $\ell = d-1$, we have $p_i^2 = 0$. For $1 \leq \ell \leq d-2$, $C_i^{[1..d-\ell-1]}$ is chosen by $\mathcal{A}$. Then, we have

$$\begin{aligned} p_i^2 &\leq \sum_{j\in[1..i-1]} \Pr[M_i^d \parallel S_i^{[1..\ell]} = M_j^d \parallel S_j^{[1..\ell]}] \\ &\leq \sum_{j\in[1..i-1]} (\Pr[M_i^d = M_j^d] \cdot \Pr[(S_i^{[1..\ell]} = S_j^{[1..\ell]}]) \\ &\leq \frac{(i-1) - \left(\sum_{x\in[1..\ell]} |\mathcal{S}_i^x|\right)}{\prod_{x\in[1..\ell]} (2^n - |\mathcal{S}_i^x|)} \cdot \frac{2^{(d-1)n}}{2^{dn} - (i-1)} \\ &\leq \frac{2(i-1)}{2^{(d+\ell)n}} \cdot 2^{(d-1)n} = \frac{2(i-1)}{2^{(\ell+1)n}} . \end{aligned}$$

By following the same analysis, when $\mathcal{A}$'s i-th query is an encryption query, we have $p_i^1 = 0$, $p_i^2 \leq \frac{2(i-1)}{2^{(\ell+1)n}}$ for $1 \leq \ell \leq d-2$, $p_i^2 = 0$ for $\ell = d-1$, and $p_i^3 \leq \frac{2\ell(i-1)}{2^{dn}}$.

Then, regardless of the direction of the i-th query, we have

$$\begin{aligned} p_i^1 + p_i^2 + p_i^3 &\leq \begin{cases} \dfrac{2(i-1)}{2^{(\ell+1)n}} + \dfrac{2\ell(i-1)}{2^{dn}} & \text{for } 1 \leq \ell \leq d-2 \\ \dfrac{2(d-1)(i-1)}{2^{dn}} & \text{for } \ell = d-1 \end{cases} \\ &\leq \frac{2(d-1)(i-1)}{2^{(\ell+1)n}} \quad \text{for } 1 \leq \ell \leq d-1 . \end{aligned}$$

Therefore, we have

$$\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \sum_{i\in[2..q]} (p_i^1 + p_i^2 + p_i^3) \leq \sum_{i\in[2..q]} \frac{2(d-1)(i-1)}{2^{(\ell+1)n}} \leq \frac{(d-1)q^2}{2^{(\ell+1)n}} . \qquad \square$$

$\Pr[\Theta_{\mathcal{R}} = \theta] / \Pr[\Theta_{\mathcal{I}} = \theta]$. We next consider $\theta \in \mathsf{T}_{\mathrm{good}}$. In the real world, for all $1 \leq j < i \leq q$ and $1 \leq x \leq d+\ell$, we define

$$\mathcal{T}_i^x = \{j\text{-th output of } \widetilde{P}_x \mid (i\text{-th tweak of } \widetilde{P}_x) = (j\text{-th tweak of } \widetilde{P}_x)\} .$$

We also define $\mathcal{T}_1^x = \emptyset$ for all x. Then we have

$$\Pr[\Theta_{\mathcal{R}} = \theta] = \prod_{x\in[1..d+\ell]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} .$$

We have $\mathcal{S}_i^x = \mathcal{T}_i^x$ for all $1 \leq x \leq \ell$ when $\mathcal{A}$'s i-th query is an encryption query, and $\mathcal{S}_i^x = \mathcal{T}_i^{d+x}$ for all $1 \leq x \leq \ell$ when $\mathcal{A}$'s i-th query is a decryption query. Therefore, we have

$$\Pr[\Theta_{\mathcal{R}} = \theta] = \prod_{x\in[1..d+\ell]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \geq \frac{1}{2^{dnq}} \cdot \left(\prod_{x\in[1..\ell]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{S}_i^x|} \right) .$$

In the ideal world, we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \left(\prod_{i\in[1..q]} \frac{1}{2^{dn} - (i-1)}\right) \cdot \left(\prod_{x\in[1..\ell]} \prod_{i\in[1..q]} \frac{1}{2^n - |\mathcal{S}_i^x|}\right).$$

Then, for $q \le 2^{dn/2}$, which is true from the assumption, we have

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

From Lemma 1 and Lemma 3, we have Theorem 2. □

The tightness of the security bound of Theorem 2 is not known and is left as an open question. The computational security bound where we use a TSPRP [LRW02, LRW11] as the underlying TBC can be obtained as in [Min15].

7 Security of $\mathcal{E}_d$ for $q \le 2^{n/2}$

In this section, we prove that the dn-bit BC $\mathcal{E}_d$ is birthday-bound secure. This implies that the security bound $O(q^2/2^{(\ell+1)n})$ of the BC $\mathcal{E}_{d+\ell}$ in Sect. 6 also holds for the case $\ell = 0$. We describe the tightness of this security bound in Sect. 8.

Theorem 3. *Fix $d \ge 2$. For $x \in [1..d]$, let $\widetilde{P}_x : \{0,1\}^n \times \{0,1\}^{(d-1)n} \to \{0,1\}^n$ be a random tweakable permutation, and consider $\mathcal{E}_d = \mathcal{E}_d[\widetilde{P}_1, \ldots, \widetilde{P}_d]$. Then for any $\mathcal{A}$ that makes at most $q \le 2^{n/2}$ queries, it holds that*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathcal{E}_d}(\mathcal{A}) \le \frac{dq^2}{2^n}.$$

Proof. As in the previous cases, we assume that $\mathcal{A}$ is deterministic, makes exactly q queries, does not repeat a query, and does not make a redundant query.

Procedures of the Oracles. The oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$ are for the real world to implement $\mathcal{E}_d$ and $\mathcal{E}_d^{-1}$, and the oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$ are for the ideal world to implement π and π^{-1}. In the real world, we define $\mathcal{R}$ and $\mathcal{R}^{-1}$ as in Algorithms 9 and 10 in Fig. 10. In the ideal world, we define $\mathcal{I}$ and $\mathcal{I}^{-1}$ as in Algorithms 11 and 12 in Fig. 11.

A transcript is defined as

$$\theta = \{(M_i^1, \ldots, M_i^d, C_i^1, \ldots, C_i^d) \mid i = 1, \ldots, q\}.$$

Since $\mathcal{A}$ does not repeat a query, $M_i^{[1..d]} \ne M_j^{[1..d]}$ and $C_i^{[1..d]} \ne C_j^{[1..d]}$ hold for any $1 \le j < i \le q$.

Bad Transcript. In the real world, we see that the following $(d-1) \times \binom{q}{2}$ collisions cannot appear in θ.

$$\mathsf{Bad} \quad \begin{cases} M_i^{[2..d]} \,\|\, C_i^1 = M_j^{[2..d]} \,\|\, C_j^1 \\ \vdots \\ M_i^d \,\|\, C_i^{[1..d-1]} = M_j^d \,\|\, C_j^{[1..d-1]} \end{cases}$$

Here, Bad is the set of $(d-1) \times \binom{q}{2}$ collisions. Since one encryption round is a permutation over $\{0,1\}^{dn}$ and $\mathcal{A}$ does not repeat a query, no collision in Bad can happen in the real world.

Algorithm 9: 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. $C_i^1 \leftarrow \widetilde{P}_1(M_i^1, M_i^{[2..d]})$
2. **for** $x = 2, \ldots, d-1$ **do**
   $C_i^x \leftarrow \widetilde{P}_x(M_i^x, M_i^{[x+1..d]} \,\|\, C_i^{[1..x-1]})$
3. $C_i^d \leftarrow \widetilde{P}_d(M_i^d, C_i^{[1..d-1]})$
4. **return** $C_i^{[1..d]}$

Algorithm 10: 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. $M_i^d \leftarrow \widetilde{P}_d^{-1}(C_i^d, C_i^{[1..d-1]})$
2. **for** $x = d-1, \ldots, 2$ **do**
   $M_i^x \leftarrow \widetilde{P}_x^{-1}(C_i^x, M_i^{[x+1..d]} \,\|\, C_i^{[1..x-1]})$
3. $M_i^1 \leftarrow \widetilde{P}_1^{-1}(C_i^1, M_i^{[2..d]})$
4. **return** $M_i^{[1..d]}$

Figure 10: Oracles $\mathcal{R}$ and $\mathcal{R}^{-1}$

Algorithm 11: 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. **return** $C_i^{[1..d]}$

Algorithm 12: 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. **return** $M_i^{[1..d]}$

Figure 11: Oracles $\mathcal{I}$ and $\mathcal{I}^{-1}$

On the other hand, collisions in Bad can happen in the ideal world. We define the set of bad transcripts as

$$\mathsf{T}_{\mathrm{bad}} = \{\theta \mid \text{a collision in } \mathsf{Bad} \text{ occurs}\}.$$

Then we prove the following lemma.

Lemma 4. $\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] \leq \dfrac{q^2}{2^n}$.

Proof. We consider $\theta \in \mathsf{T}_{\mathrm{bad}}$ in the ideal world. When $\mathcal{A}$'s i-th query is an encryption query, $M_i^{[1..d]}$ are chosen by $\mathcal{A}$ and $\Pr[C_i^1 = C_j^1] \leq \frac{2^{(d-1)n}}{2^{dn}-(i-1)}$. When $\mathcal{A}$'s i-th query is a decryption query, $C_i^{[1..d]}$ are chosen by $\mathcal{A}$ and $\Pr[M_i^d = M_j^d] \leq \frac{2^{(d-1)n}}{2^{dn}-(i-1)}$. Therefore, for $q \leq 2^{n/2}$, we have

$$\begin{aligned}
\Pr[\Theta_{\mathcal{I}} \in \mathsf{T}_{\mathrm{bad}}] &\leq \prod_{i\in[2..q]} \prod_{j\in[1..i-1]} \frac{2^{(d-1)n}}{2^{dn}-(i-1)} \\
&\leq \prod_{i\in[2..q]} \frac{(i-1)\cdot 2^{(d-1)n}}{2^{dn}-(i-1)} \\
&\leq \prod_{i\in[2..q]} \frac{2(i-1)}{2^n} \leq \frac{q^2}{2^n}.
\end{aligned}$$

□

$\Pr[\Theta_{\mathcal{R}} = \theta] / \Pr[\Theta_{\mathcal{I}} = \theta]$. We consider $\theta \in \mathsf{T}_{\mathrm{good}}$. In the real world, for all $1 \le j < i \le q$ and $1 \le x \le d$, we define

$$\mathcal{T}_i^x = \{j\text{-th output of } \widetilde{P}_x \mid (i\text{-th tweak of } \widetilde{P}_x) = (j\text{-th tweak of } \widetilde{P}_x)\}$$

as before. We also define $\mathcal{T}_1^x = \emptyset$ for all x. Then we have

$$\Pr[\Theta_{\mathcal{R}} = \theta] = \prod_{x \in [1..d]} \prod_{i \in [1..q]} \frac{1}{2^n - |\mathcal{T}_i^x|} \ge \prod_{x \in [1..d]} \prod_{i \in [1..q]} \frac{1}{2^n} = \prod_{i \in [1..q]} \frac{1}{2^{dn}}\,.$$

In the ideal world, we have

$$\Pr[\Theta_{\mathcal{I}} = \theta] = \prod_{i \in [1..q]} \frac{1}{2^{dn} - (i-1)}\,.$$

Then we have

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

From Lemma 1 and Lemma 4, we have Theorem 3. □

The computational security bound with TSPRPs [LRW02, LRW11] instead of random tweakable permutations can be obtained as in [Min15].

8 An Attack against $\mathcal{E}_d$

In this section, we show an attack against $\mathcal{E}_d$ with $q = O(2^{n/2})$ queries. This means that our security bound in Theorem 3 is tight.

Let $\widetilde{P}_1, \ldots, \widetilde{P}_d$ be $(n, (d-1)n)$-bit random tweakable permutations and we consider $\mathcal{E}_d[\widetilde{P}_1, \ldots, \widetilde{P}_d]$. Our attack is a chosen plaintext attack, so the adversary can choose any plaintexts $M_i^{[1..d]} \in \{0,1\}^{dn}$ for $i = 1, \ldots, q$ and send them to oracle $\mathcal{O} \in \{\mathcal{E}_d, \pi\}$, and it is given q ciphertexts $C_i^{[1..d]} \in \{0,1\}^{dn}$ encrypted by $\mathcal{O}$.

The adversary fixes $M^{[2..d]}$ during its attack (i.e., $M_1^{[2..d]} = \cdots = M_q^{[2..d]}$), and chooses distinct M^1 (that is $M_1^1, \ldots, M_q^1$ are different from each other). If $\mathcal{O} = \mathcal{E}_d$, then $C_i^1 = \widetilde{P}_1(M_i^1, M_i^{[2..d]})$ for $1 \le i \le q$ are also different from each other since $\widetilde{P}_1(\cdot, T)$ is a permutation on $\{0,1\}^n$ when T is fixed. Otherwise, if $\mathcal{O} = \pi$, then there is a possibility that $C_i^1 = C_j^1$ holds for some $1 \le j < i \le q$. Therefore, the adversary looks for one of the collisions $C_i^1 = C_j^1$ for some $1 \le j < i \le q$ after its interaction with $\mathcal{O}$. If the adversary finds a collision, it guesses $\mathcal{O} = \pi$ and else, it guesses $\mathcal{O} = \mathcal{E}_d$. When $\mathcal{O} = \mathcal{E}_d$ the guess is correct with probability 1 and it is wrong if and only if $\mathcal{O} = \pi$ and the collision $C_i^1 = C_j^1$ does not happen for all $1 \le j < i \le q$. From the birthday bound, the attack succeeds with an overwhelming probability.

9 Conclusions

In this paper, we analyzed the iterative construction of a block cipher that is constructed from a TBC that have long tweaks. In particular, we showed the relationship between the number rounds of Minematsu's dn-bit block cipher [Min15] and its security. We showed that with $3d - 2$ rounds, it achieves BBB security $O(q^2/2^{dn})$, saving two rounds. Also, we proved that if $q \le 2^n$, then $d + \ell$ rounds for $1 \le \ell \le d - 1$ achieve BBB security

$O(q^2/2^{(1+\ell)n})$. We also considered the d round version, which is tightly birthday-bound secure.

There are various interesting open questions. The first question is whether the security bounds can be improved. In particular, we do not know if the assumption of $q \leq 2^n$ can be removed from Theorem 2, and tightness of the security bounds in Theorems 1 and 2 are left as an open question. Generalization to enciphering schemes [CLMP17, CMN18] is an interesting question, and the analysis in the indifferentiability framework to obtain a public random permutation, following [GL15], is also left as an interesting open question.

Acknowledgments

The authors thank the anonymous reviewers of FSE 2020 for valuable comments that helped improving this paper.

References

[Ava17] Roberto Avanzi. The QARMA Block Cipher Family. Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes. *IACR Trans. Symmetric Cryptol.*, 2017(1):4–44, 2017.

[BGIM19] Zhenzhen Bao, Jian Guo, Tetsu Iwata, and Kazuhiko Minematsu. ZOCB and ZOTR: Tweakable Blockcipher Modes for Authenticated Encryption with Full Absorption. *IACR Trans. Symmetric Cryptol.*, 2019(2):1–54, 2019.

[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.

[BLMR19] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks. *IACR Trans. Symmetric Cryptol.*, 2019(1):5–45, 2019.

[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.

[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.

[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.

[CLS17] Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New Constructions of MACs from (Tweakable) Block Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(2):27–58, 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. 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.

[CS06b] 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.

[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.

[GL15] Chun Guo and Dongdai Lin. Improved domain extender for the ideal cipher. *Cryptography and Communications*, 7(4):509–533, 2015.

[GLN19] Tony Grochow, Eik List, and Mridul Nandi. DoveMAC: A TBC-based PRF with Smaller State, Full Security, and High Rate. *IACR Trans. Symmetric Cryptol.*, 2019(3):43–80, 2019.

[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.

[Hal07] Shai Halevi. Invertible Universal Hashing and the TET Encryption Mode. 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 412–429. Springer, 2007.

[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.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 34–65. Springer, 2017.

[JNP14a] Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. Deoxys v1. CAESAR submission, 2014.

[JNP14b] Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. KIASU v1. CAESAR submission, 2014.

[JNP14c] 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.

[LN17] Eik List and Mridul Nandi. ZMAC+ - An Efficient Variable-output-length Variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.

[LR88] Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[LRW02] Moses 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 Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. *J. Cryptology*, 24(3):588–613, 2011.

[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.

[MI15] Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. In Jens Groth, editor, *Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings*, volume 9496 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 2015.

[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.

[Min14] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. 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 275–292. Springer, 2014.

[Min15] Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. *Des. Codes Cryptography*, 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.

[MRS09] Ben Morris, Phillip Rogaway, and Till Stegers. How to Encipher Messages on a Small Domain. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 286–302. Springer, 2009.

[Nai15] Yusuke Naito. Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher. In Man Ho Au and Atsuko Miyaji, editors, *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*, volume 9451 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2015.

[NIS] NIST Lightweight Cryptography. https://csrc.nist.gov/projects/lightweight-cryptography.

[NR99] Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.

[NS20] Yusuke Naito and Takeshi Sugawara. Lightweight Authenticated Encryption Mode of Operation for Tweakable Block Ciphers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(1), 2020. To appear.

[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.

[PS16] Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. 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 I*, volume 9814 of *Lecture Notes in Computer Science*, pages 33–63. Springer, 2016.

[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[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. Information Theory*, 55(10):4749–4760, 2009.

[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.

[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.

A Proof of Equation (1)

For $1 \le i \le q$ and $q \le 2^n$, we prove that

$$\frac{(i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y|\right)}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)} \cdot \frac{1}{2^{dn} - (i-1)} \le \frac{2(i-1)}{2^{(d+x)n}} .$$

Here, $d \ge 2$, $\ell \in [1..d-1]$, $x \in [1..\ell]$, and $0 \le \sum_{y\in[1..x]} |\mathcal{S}_i^y| \le i-1$.

Proof. We subtract the left hand side from the right hand side:

$$\frac{2(i-1)}{2^{(d+x)n}} - \frac{(i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y|\right)}{\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)} \cdot \frac{1}{2^{dn} - (i-1)}$$

$$= \frac{2(i-1)\cdot\left(2^{dn} - (i-1)\right)\cdot\left(\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)\right) - 2^{(d+x)n}\left((i-1) - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y|\right)\right)}{2^{(d+x)n}\left(2^{dn} - (i-1)\right)\cdot\left(\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|)\right)} .$$

Here, $\sum_{y\in[1..x]} |\mathcal{S}_i^y|$ is equal to the number of j satisfying $\Pr[S_i^{[1..x]} = S_j^{[1..x]}] = 0$, so we have $0 \le \sum_{y\in[1..x]} |\mathcal{S}_i^y| \le i-1 < 2^n$ (This is the point where we rely on the assumption of $q \le 2^n$). Therefore, the denominator is positive. We define $f(i)$ as the numerator and we prove $f(i) \ge 0$.

Since $|\mathcal{S}_i^y| \le 2^n - 1$ holds for all y, we have

$$\prod_{y\in[1..x]} (2^n - |\mathcal{S}_i^y|) \ge 2^{xn} - \left(\sum_{y\in[1..x]} |\mathcal{S}_i^y|\right)\cdot 2^{(x-1)n} .$$

Let $\mathsf{sum} = \sum_{y\in[1..x]} |\mathcal{S}_i^y|$. Then we have $0 \le \mathsf{sum} \le i-1 < 2^n$ and

$$\begin{aligned}
f(i) &\ge 2(i-1)\cdot\left(2^{dn} - (i-1)\right)\cdot\left(2^{xn} - \mathsf{sum}\cdot 2^{(x-1)n}\right) - 2^{(d+x)n}\left((i-1) - \mathsf{sum}\right) \\
&\ge 2(i-1)\cdot\left(2^{(d+x)n} - \left(\mathsf{sum}\cdot 2^{(d+x-1)n} + (i-1)\cdot 2^{xn}\right)\right) \\
&\quad - (i-1)\cdot 2^{(d+x)n} + \mathsf{sum}\cdot 2^{(d+x)n} \\
&= (i-1)\cdot\left(\left(2\cdot 2^{(d+x)n} - 2\cdot\mathsf{sum}\cdot 2^{(d+x-1)n} - 2(i-1)\cdot 2^{xn}\right) - 2^{(d+x)n}\right) \\
&\quad + \mathsf{sum}\cdot 2^{(d+x)n} \\
&= (i-1)\cdot\left(\left(2^{(d+x)n} - \mathsf{sum}\cdot 2^{(d+x-1)n}\right) - \mathsf{sum}\cdot 2^{(d+x-1)n} - 2(i-1)\cdot 2^{xn}\right) \\
&\quad + \mathsf{sum}\cdot 2^{(d+x)n}
\end{aligned}$$

$$
\begin{aligned}
&= (i-1)\cdot\left(2^{(d+x)n} - \mathsf{sum}\cdot 2^{(d+x-1)n}\right) - \mathsf{sum}\cdot(i-1)\cdot 2^{(d+x-1)n} + \mathsf{sum}\cdot 2^{(d+x)n} \\
&\quad - 2(i-1)^2\cdot 2^{xn} \\
&= (i-1)\cdot\left(2^{(d+x)n} - \mathsf{sum}\cdot 2^{(d+x-1)n}\right) + \mathsf{sum}\cdot\left(2^{(d+x)n} - (i-1)\cdot 2^{(d+x-1)n}\right) \\
&\quad - 2(i-1)^2\cdot 2^{xn} \\
&= (i-1)\cdot(2^n - \mathsf{sum})\cdot 2^{(d+x-1)n} + \mathsf{sum}\cdot(2^n-(i-1))\cdot 2^{(d+x-1)n} - 2(i-1)^2\cdot 2^{xn} \\
&\geq (i-1)\cdot(2^n - \mathsf{sum})\cdot 2^{(x+1)n} + \mathsf{sum}\cdot(2^n-(i-1))\cdot 2^{(x+1)n} - 2(i-1)^2\cdot 2^{xn} \\
&= (i-1)\cdot((2^n - \mathsf{sum})\cdot 2^n - 2(i-1))\cdot 2^{xn} + \mathsf{sum}\cdot(2^n-(i-1))\cdot 2^{(x+1)n} \\
&= g(i) + \mathsf{sum}\cdot(2^n-(i-1))\cdot 2^{(x+1)n}\,,
\end{aligned}
$$

where $g(i) = (i-1)\cdot((2^n - \mathsf{sum})\cdot 2^n - 2(i-1))\cdot 2^{xn}$.

Recall that sum satisfies $0 \leq \mathsf{sum} \leq i-1 < 2^n$. We therefore consider the following two cases depending on the value of sum.

- Case $\mathsf{sum} < 2^n - 1$. In this case, we have $g(i) \geq 0$ from $\mathsf{sum} \leq i-1 < 2^n$, and $f(i) \geq 0$ follows.
- Case $\mathsf{sum} = 2^n - 1$. In this case, $i = 2^n$ holds and we have

$$
\begin{aligned}
f(2^n) &\geq g(2^n) + (2^n-1)\cdot 2^{(x+1)n} \\
&\geq (2^n-1)\cdot(2^n - 2(2^n-1))\cdot 2^{xn} + (2^n-1)\cdot 2^{(x+1)n} \\
&\geq 2\cdot(2^n-1)\cdot 2^{xn} \geq 0\,.
\end{aligned}
$$

Therefore, we always have $f(i) \geq 0$. □