Beyond-birthday-bound Security Based on Tweakable Block Cipher

Kazuhiko Minematsu

NEC Corporation, 1753 Shimonumabe, Nakahara-Ku, Kawasaki, Japan,
k-minematsu@ah.jp.nec.com

Abstract. This paper studies how to build a $2n$-bit block cipher which is hard to distinguish from a truly random permutation against attacks with $q \approx 2^{n/2}$ queries, i.e., birthday attacks. Unlike previous approaches using pseudorandom functions, we present a simple and efficient proposal using a tweakable block cipher as an internal module. Our proposal is provably secure against birthday attacks, if underlying tweakable block cipher is also secure against birthday attacks. We also study how to build such tweakable block ciphers from ordinary block ciphers, which may be of independent interest. **keywords**: Block Cipher Mode, Birthday Bound, Tweakable Block Cipher.

1 Introduction

A double-block-length cipher (DBLC), i.e. a $2n$-bit block cipher made from n-bit block components, has been one of the main research topics in the symmetric cryptography. In particular, a seminal work of Luby and Rackoff [17] proved that a 4-round Feistel permutation is computationally hard to distinguish from a truly random permutation if each round function is an n-bit pseudorandom function [11]. The proof of [17] is valid for chosen-ciphertext attacks (CCAs) using $q \ll 2^{n/2}$ queries, and is called a proof of $O(2^{n/2})$-security. As $2^{n/2}$ is related to the birthday paradox for n-bit variables, it is also called the security up to the birthday bound (for n). Then, building a DBLC having beyond-birthday-bound security, i.e., $O(2^{\omega+n/2})$-security for some $\omega > 0$, is an interesting research topic from theoretical and practical aspects. In particular, such a DBLC can improve the security of any block cipher mode that has $O(2^{n/2})$-security with an n-bit block cipher[1]. However, achieving $O(2^{\omega+n/2})$-security is generally difficult, even for a small ω. We have very few known DBLC proposals having this property. All of them were based on Feistel permutations using pseudorandom functions [22][18][20]. Although these studies indicated the great potential of Feistel permutation, we wondered if using Feistel was the only solution.

In this paper, we demonstrate how this problem can be solved using a tweakable block cipher, defined by Liskov et al.[16]. In particular, we present how to build a DBLC based on a tweakable block cipher $\widetilde{E}$ with n-bit block and m-bit

[1] For some specific applications, such as stateful encryption and stateful authentication, block cipher modes with beyond-birthday-bound security are known [15][5].

tweak for any $1 \leq m \leq n$, and prove $O(2^{(n+m)/2})$-security against CCAs. One significant fact is that it is *optimally efficient*, as it requires only two $\widehat{E}$ calls (independently of m) and some universal hash functions. Thus, assuming very fast universal hash functions (e.g., [25]), our DBLC will have almost the same throughput as that of a tweakable block cipher. This means that, the task of building a secure $2n$-bit block cipher can be efficiently reduced to that of building a secure n-bit block tweakable block cipher. We think this is an interesting application of tweakable block cipher, that has not been mentioned before. As a by-product, we provide some variants such as a pseudorandom function with $2n$-bit input and n-bit output. All variants are optimally efficient in the sense defined above.

We have to emphasize that the birthday bound here is with respect to n, and not to $n+m$. The security of our scheme is still up to the birthday bound of *input length* of the cryptographic primitive (as with Yasuda [28]). Although this makes the problem much easier in general, our result is still non-trivial and highly optimized as a solution to beyond-birthday-bound security for n.

As our DBLC requires a tweakable block cipher with beyond-birthday-bound security, we also discuss how to realize it. Specifically, we focus on constructions using n-bit block ciphers. Although known constructions [16][24] are only $O(2^{n/2})$-secure, we provide a simple solution using tweak-dependent key changes with a concrete security proof. Unfortunately, this scheme is only the first step: it can be very slow and has some severe theoretical limitations, thus is far from being perfect. Building a better scheme remains an interesting future direction of research.

2 Preliminaries

2.1 Basic Notations

A random variable will be written in capital letters and its sampled value will be written in the corresponding small letters. Let Σ^n denote $\{0,1\}^n$. The bit length of a binary sequence x is denoted by $|x|$, and $x_{[i,j]}$ denotes a subsequence of x from i-th to j-th bit, for $1 \leq i < j \leq |x|$. A uniform random function (URF) with n-bit input and ℓ-bit output, denoted by $\mathsf{R}_{n,\ell}$, is a random variable uniformly distributed over $\{f : \Sigma^n \to \Sigma^\ell\}$. Similarly, a random variable uniformly distributed over all n-bit permutations is an n-bit block uniform random permutation (URP) and is denoted by P_n. If $F_K : \mathcal{X} \to \mathcal{Y}$ is a keyed function, then F_K is a random variable (not necessarily uniformly) distributed over $\{f : \mathcal{X} \to \mathcal{Y}\}$. If F_K is a keyed permutation, F_K^{-1} will denote its inversion. We will omit K and write $F : \mathcal{X} \to \mathcal{Y}$, when K is clear from the context.

A tweakable block cipher [16] is a keyed permutation with auxiliary input called tweak. Formally, a ciphertext of a tweakable blockcipher, $\widetilde{E} : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$, is $C = \widetilde{E}(M,T)$, where $M \in \mathcal{M}$ is a plaintext and $T \in \mathcal{T}$ is the tweak. The encryption, $\widetilde{E}$, must be a keyed permutation over $\mathcal{M}$ for every $T \in \mathcal{T}$, and the decryption is defined as $\widetilde{E}^{-1}(C,T) = M$ with $\widetilde{E}^{-1} : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$. If $\widetilde{E}$ has n-bit

block and m-bit tweak, we say it is an (n, m)-bit tweakable cipher. An (n, m)-bit tweakable URP is the set of 2^m independent URPs (i.e., an n-bit URP is used for each m-bit tweak) and is denoted by $\widetilde{\mathsf{P}}_{n,m}$. We write $\widetilde{\mathsf{P}}_n$ if m is clear from the context.

2.2 Security Notion

Consider the game in which we want to distinguish two keyed functions, G and G', using a black-box access to them. We define classes of attacks: chosen-plaintext attack (CPA), and chosen-ciphertext attack (CCA), and their tweaked versions, i.e., a tweak and a plaintext (or ciphertext) can be arbitrarily chosen. Here, (tweaked) CCA can be defined when G and G' are (tweakable) permutations. Let $\mathtt{atk} \in \{\mathtt{cpa}, \mathtt{cca}, \widetilde{\mathtt{cpa}}, \widetilde{\mathtt{cca}}\}$, where $\widetilde{\mathtt{cpa}}$ ($\widetilde{\mathtt{cca}}$) denotes tweaked CPA (CCA). The maximum advantage of adversary using $\mathtt{atk}$ in distinguishing G and G' is:

$$\mathbf{Adv}^{\mathtt{atk}}_{G,G'}(\theta) \stackrel{\text{def}}{=} \max_{\mathcal{D}:\theta-\mathtt{atk}} \left| \Pr[\mathcal{D}^{G} = 1] - \Pr[\mathcal{D}^{G'} = 1] \right|, \tag{1}$$

where $\mathcal{D}^G = 1$ denotes that $\mathcal{D}$'s guess is 1, which indicates G or G'. The parameter θ denotes the attack resource, such as the number of queries, q, and time complexity [11], τ. If θ does not contain τ, the adversary has no computational restriction. The maximum is taken for all $\mathtt{atk}$-adversaries having θ. For $G : \Sigma^n \to \Sigma^m$, we have

$$\mathbf{Adv}^{\mathtt{prf}}_{G}(\theta) \stackrel{\text{def}}{=} \mathbf{Adv}^{\mathtt{cpa}}_{G,\mathsf{R}_{n,m}}(\theta),\ \mathbf{Adv}^{\mathtt{sprp}}_{G}(\theta) \stackrel{\text{def}}{=} \mathbf{Adv}^{\mathtt{cca}}_{G,\mathsf{P}_n}(\theta),\ \mathbf{Adv}^{\mathtt{prp}}_{G}(\theta) \stackrel{\text{def}}{=} \mathbf{Adv}^{\mathtt{cpa}}_{G,\mathsf{P}_n}(\theta),$$

where the last two equations are defined if G is an n-bit permutation, Moreover, if G is an (n, m)-bit tweakable cipher, we define

$$\mathbf{Adv}^{\widetilde{\mathtt{sprp}}}_{G}(\theta) \stackrel{\text{def}}{=} \mathbf{Adv}^{\widetilde{\mathtt{cca}}}_{G,\widetilde{\mathsf{P}}_{n,m}}(\theta), \text{ and } \mathbf{Adv}^{\widetilde{\mathtt{prp}}}_{G}(\theta) \stackrel{\text{def}}{=} \mathbf{Adv}^{\widetilde{\mathtt{cpa}}}_{G,\widetilde{\mathsf{P}}_{n,m}}(\theta).$$

If $\mathbf{Adv}^{\mathtt{prf}}_{G}(\theta)$ is negligibly small for all practical θ (the definition of "practical θ" depends on users.), G is a pseudorandom function (PRF)[11]. If G is invertible, it is also called a pseudorandom permutation (PRP). In addition, if $\mathbf{Adv}^{\mathtt{sprp}}_{G}(\theta)$ is negligibly small, G is a strong pseudorandom permutation (SPRP). If G is a tweakable cipher, tweakable SPRP and PRP are similarly defined using $\mathbf{Adv}^{\widetilde{\mathtt{sprp}}}_{G}(\theta)$ and $\mathbf{Adv}^{\widetilde{\mathtt{prp}}}_{G}(\theta)$. Generally, we say G is secure if $\mathbf{Adv}^{\widetilde{\mathtt{sprp}}}_{G}(\theta)$ is negligibly small.

CCA-CPA conversion. In our security proof, it is convenient to use a conversion from a $\mathtt{cca}$-advantage into a $\mathtt{cpa}$-advantage. For this purpose, we introduce a subclass of $\mathtt{cpa}$ called $\mathtt{cpa}'$, which is as follows. First, for any keyed permutation G over $\mathcal{M}$, let $\langle G \rangle : \mathcal{M} \times \Sigma \to \mathcal{M}$ be the equivalent representation of G, where $\langle G \rangle(x, 0) = G(x)$ and $\langle G \rangle(x, 1) = G^{-1}(x)$. This expression also holds true for tweakable permutations, i.e., for any tweakable permutation $\widetilde{G}$ with message space $\mathcal{M}$ and tweak space $\mathcal{T}$, $\langle \widetilde{G} \rangle$ is an equivalent keyed function $: \mathcal{M} \times \mathcal{T} \times \Sigma \to \mathcal{M}$. The LSB of a query to $\langle G \rangle$ is called a operation indicator. Consider $F : \mathcal{M} \times \Sigma \to \mathcal{M}$ and a $\mathtt{cpa}$-adversary $\mathcal{D}$ interacting with F. Let

$X_i = (M_i, W_i) \in \mathcal{M} \times \Sigma$ be the i-th query of $\mathcal{D}$ and let $Y_i \in \mathcal{M}$ be the i-th answer. For any $\mathcal{D}$, we assume $M_i \neq M_j$ always holds when $W_i = W_j$ with $i < j$. Moreover, if $Y_i \neq M_j$ holds whenever $W_i \neq W_j$ holds with $i < j$, $\mathcal{D}$ is said to follow the *invertibility condition*. A cpa-adversary following the invertibility condition is called a cpa′-adversary. If F corresponds to $\langle G \rangle$ for a keyed permutation G, violating the invertibility condition is clearly pointless, as outputs are predictable. Thus any cca-adversary avoiding useless queries for G can be simulated by a cpa′-adversary interacting with $\langle G \rangle$. In other words, for any keyed permutations, E and G, we have

$$\mathtt{Adv}^{\mathtt{cca}}_{E,G}(q,\tau) = \mathtt{Adv}^{\mathtt{cpa}}_{\langle E\rangle,\langle G\rangle}(q,\tau) = \mathtt{Adv}^{\mathtt{cpa}'}_{\langle E\rangle,\langle G\rangle}(q,\tau). \tag{2}$$

In general, cpa′ is weaker than cpa when at least one of two target functions is not invertible. Note that, following the invertibility condition does not exclude all collisions that can not be happened for permutations. For example, if a cpa′-adversary is interacting with $F = \langle G \rangle$ for some keyed permutation G, $M_i \neq Y_j$ holds true for all $i < j$ with $W_i \neq W_j$ (in addition to $Y_i \neq M_j$, which is guaranteed from the invertibility condition). However $M_i = Y_j$ can happen when (e.g.) F is a URF, as Y_j is uniform and independent of X_i for all $i < j$.

2.3 Maurer's Methodology

Our security proof will be based on a methodology developed by Maurer [19]. Here, we briefly describe it. See Maurer [19] for a more detailed description. Consider a binary random variable A_i as a (non-deterministic) function of i input/output pairs (and internal variables) of a keyed function. We denote the event $A_i = 1$ by a_i, and denote $A_i = 0$ by $\overline{a_i}$. We assume a_i is monotone; i.e., a_i never occurs if $\overline{a_{i-1}}$ occurs. For instance, a_i is monotone if it indicates that all i outputs are distinct. An infinite sequence $\mathcal{A} = a_0 a_1 \dots$ is called a *monotone event sequence* (MES). Here, a_0 is some tautological event (i.e. $A_0 = 1$ with probability 1). Note that $\mathcal{A} \wedge \mathcal{B} = (a_0 \wedge b_0)(a_1 \wedge b_1) \dots$ is an MES if $\mathcal{A} = a_0 a_1 \dots$ and $\mathcal{B} = b_0 b_1 \dots$ are both MESs. For any sequence of random variables, $X_1, X_2, \dots$, let X^i denote $(X_1, \dots, X_i)$. Let MESs $\mathcal{A}$ and $\mathcal{B}$ be defined for two keyed functions, $F : \mathcal{X} \to \mathcal{Y}$ and $G : \mathcal{X} \to \mathcal{Y}$, respectively. Let $X_i \in \mathcal{X}$ and $Y_i \in \mathcal{Y}$ be the i-th input and output. Let P^F be the probability space defined by F. For example, $P^F_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ means $\Pr[Y_i = y_i | X^i = x^i, Y^{i-1} = y^{i-1}]$ where $Y_j = F(X_j)$ for $j \geq 1$. If $P^F_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1}) = P^G_{Y_i|X^iY^{i-1}}(y_i, x^i, y^{i-1})$ for all possible (x^i, y^{i-1}), then we write $P^F_{Y_i|X^iY^{i-1}} = P^G_{Y_i|X^iY^{i-1}}$ and denote it by $F \equiv G$. Here, note that the definitions of $\mathcal{X}$ and $\mathcal{Y}$, and the set of possible (x^i, y^{i-1}) may depend on the target attack class. Inequalities such as $P^F_{Y_i|X^iY^{i-1}} \leq P^G_{Y_i|X^iY^{i-1}}$ are similarly defined.

Definition 1. *We write* $F^{\mathcal{A}} \equiv G^{\mathcal{B}}$ *if* $P^F_{Y_i a_i | X^i Y^{i-1} a_{i-1}} = P^G_{Y_i b_i | X^i Y^{i-1} b_{i-1}}$ *holds*[2] *for all* $i \geq 1$. *Moreover, we write* $F|\mathcal{A} \equiv G|\mathcal{B}$ *if* $P^F_{Y_i | X^i Y^{i-1} a_i} = P^G_{Y_i | X^i Y^{i-1} b_i}$ *holds for all* $i \geq 1$.

Definition 2. *For MES* $\mathcal{A}$ *defined for* F, $\nu_{\mathtt{atk}}(F, \overline{a_q})$ *denotes*[3] *the maximal probability of* $\overline{a_q}$ *for any* atk*-adversary using* q *queries (and infinite computational power) that interacts with* F.

The equivalences defined by Definition 1 are crucial to information-theoretic security proofs. For example, the following theorem holds true.

Theorem 1. *(Theorem* 1 (i) *of [19]) If* $F^{\mathcal{A}} \equiv G^{\mathcal{B}}$ *or* $F|\mathcal{A} \equiv G$ *holds for an attack class* atk*, then* $\mathtt{Adv}^{\mathtt{atk}}_{F,G}(q) \leq \nu_{\mathtt{atk}}(F, \overline{a_q})$.

We will use some of Maurer's results including Theorem 1 to make simple and intuitive proofs . For completeness, these results are cited in Appendix A.

3 Previous Constructions of DBLC

There are many $O(2^{n/2})$-secure DBLC proposals. Luby and Rackoff proved that the 4-round random Feistel cipher (denoted by ψ_4) is $O(2^{n/2})$-secure. Here, "random" means that each round function is an independent n-bit block PRFs. Later, Naor and Reingold [22] proved that the first and last round functions of ψ_4 need not necessarily be pseudorandom, but only required to be ϵ-almost XOR uniform (ϵ-AXU) for sufficiently small ϵ. Here, if H is a keyed function being ϵ-AXU, we have $\Pr[H(x) \oplus H(x') = \delta] \leq \epsilon$ for any $x \neq x$ and δ. The result of [22] stimulated many related works, e.g., [23][13][26], to name a few. Above all, what inspired us was another proposal of Naor and Reingold [22], which is so-called NR mode. Basically it is an mn-bit block cipher for arbitrarily large m, using n-bit block cipher, E. When $m = 2$, NR mode encrypts a plaintext $M \in \Sigma^{2n}$ as:

$$C = G_2^{-1} \circ \mathrm{ECB}[E] \circ G_1(M), \tag{3}$$

where $\mathrm{ECB}[E]$ is the $2n$-bit permutation from ECB mode of E. G_1 and G_2 are keyed permutations called pairwise independent permutations [22]. That is, $\Pr[G_i(x) = y, G_i(x') = y'] = 1/(2^n \cdot (2^n - 1))$ for any $x \neq x'$ and $y \neq y'$, where probability is defined by the distribution of G_i's key for $i = 1, 2$.

Compared to the vast amount of $O(2^{n/2})$-secure proposals, we have very few schemes achieving better security. A scheme of Aiello and Venkatesan [1] has some beyond-birthday-bound security but not invertible. A proposal of [22] was based on unbalanced Feistel round, where each round function has inputs longer than n-bit. The $O(2^{n/2})$-security of ψ_6 was proved by Patarin [18] and another proof of ψ_r for $r \to \infty$ was given by Maurer and Pietrzak [20], though we omit the details here.

[2] As a_i denotes $A_i = 1$, this equality means $P^F_{Y_i A_i | X^i Y^{i-1} A_{i-1}}(y_i, 1, x^i, y^{i-1}, 1)$ equals to $P^G_{Y_i B_i | X^i Y^{i-1} B_{i-1}}(y_i, 1, x^i, y^{i-1}, 1)$ for all (x^i, y^{i-1}) such that both $P^F_{A_{i-1} X^i Y^{i-1}}(1, x^i, y^{i-1})$ and $P^G_{B_{i-1} X^i Y^{i-1}}(1, x^i, y^{i-1})$ are positive.

[3] The original definition does not contain atk; this is for readability.

4 Building a DBLC with Beyond-birthday-bound Security

4.1 Extending Naor-Reingold Approach

Our goal is to build a $O(2^{\omega+n/2})$-secure DBLC, i.e., an $2n$-bit keyed permutation which is hard to be distinguished from P_{2n} against any practical CCA using $q \ll 2^{\omega+n/2}$ queries for some $\omega > 0$ (a large ω indicates a strong security). Our initial question is if we can adopt a Mix-Encrypt-Mix structure[4] similar to Eq. (3). In the following, we provide a novel solution using tweakable block ciphers. The scheme has Mix-Encrypt-Mix structure similar to NR mode, thus we call our scheme Extended Naor-Reingold (ENR)[5]. It has a parameter $m \in \{1, \ldots, n\}$, and we will prove $O(2^{(n+m)/2})$-security.

For convenience, for any random variable X, we abbreviate $X_{[1,m]}$ to $\widehat{X}$ (i.e., $\widehat{X}$ is the first m-bit of X). If $|X| = m$, we have $\widehat{X} = X$. Let $\widetilde{E}$ be an (n, m)-bit tweakable cipher, and let $\widetilde{E}_L$ and $\widetilde{E}_R$ denote two independently-keyed instances of $\widetilde{E}$. ENR consists of $\widetilde{E}_L$, $\widetilde{E}_R$, and a $2n$-bit keyed permutation, G. For plaintext $(M_l, M_r) \in \Sigma^n \times \Sigma^n$ and ciphertext $(C_l, C_r) \in \Sigma^n \times \Sigma^n$, the encryption and decryption of ENR are defined as Fig. 1.

Algorithm 4.1: $\mathrm{ENR}[G, \widetilde{E}](M_l, M_r)$

$(S, T) \leftarrow G(M_l, M_r)$
$U \leftarrow \widetilde{E}_L(S, \widehat{T}), \quad V \leftarrow \widetilde{E}_R(T, \widehat{U})$
$(C_l, C_r) \leftarrow G^{-1}_{\mathtt{rev}}(U, V)$
return $((C_l, C_r))$

Algorithm 4.2: $\mathrm{ENR}[G, \widetilde{E}]^{-1}(C_l, C_r)$

$(U, V) \leftarrow G_{\mathtt{rev}}(C_l, C_r)$
$T \leftarrow \widetilde{E}_R^{-1}(V, \widehat{U}), \quad S \leftarrow \widetilde{E}_L^{-1}(U, \widehat{T})$
$(M_l, M_r) \leftarrow G^{-1}(S, T)$
return $((M_l, M_r))$

Fig. 1. Encryption (left) and decryption (right) procedures of ENR.

Here, $G_{\mathtt{rev}}$ denotes the mirrored image of G, i.e., $G_{\mathtt{rev}}(x) = \mathtt{rev}(G(\mathtt{rev}(x)))$ with $\mathtt{rev}(x_1, \ldots, x_{2n}) = (x_{2n}, \ldots, x_1)$. We assume $G_{\mathtt{rev}}$ and G use the same key. Basically, we can prove the security of ENR for a more general setting where the second mixing layer is not restricted to $G_{\mathtt{rev}}$. We here focus on the use of $G_{\mathtt{rev}}$ because it allows us to reuse the key and implementation of G.

[4] Naor and Reingold's unbalanced Feistel cipher is based on Mix-Encrypt-Mix structure and achieves $O(2^{\omega+n/2})$-security. However, as it uses PRFs with input longer than n-bit, it is not comparable to ours. Moreover, an important difference is that the number of round of their scheme is depending on the security parameter (for higher security more rounds are needed), while that of ours is constant.

[5] If our scheme is realized with non-tweakable permutation (by setting $m = 0$), it will be very close to NR mode.

4.2 Security Proof of ENR

To prove the security of ENR$[G, \widetilde{E}]$, we first introduce a condition for G.

Definition 3. *Let G be a $2n$-bit keyed permutation. Let $m \in \{1, \ldots, n\}$ be a parameter. If G is (ϵ, γ, ρ)-almost uniform ((ϵ, γ, ρ)-AU), we have*

$$\Pr[G(x)_{[1,n+m]} = G(x')_{[1,n+m]}] \le \epsilon, \text{ and}$$
$$\Pr[G(x)_{[n+1,2n]} = G(x')_{[n+1,2n]}] \le \gamma, \text{ and}$$
$$\Pr[G(x)_{[n+1,n+m]} = G(x')_{[n+1,n+m]}] \le \rho, \text{ for any distinct } x, x' \in \Sigma^{2n}.$$

A $2n$-bit pairwise independent permutation is $(2^{-(n+m)}, 2^{-n}, 2^{-m})$-AU. Even a more efficient construction is possible by using Feistel permutation (see Corollaries 1 and 2). The security proof of general ENR is as follows.

Theorem 2. *If G is (ϵ, γ, ρ)-AU for $m \in \{1, \ldots, n\}$ and $\widetilde{E}$ is an (n, m)-bit tweakable cipher, we have*

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{ENR}[G,\widetilde{E}]}(q, \tau)$$
$$\le 2\mathtt{Adv}^{\widetilde{\mathtt{sprp}}}_{\widetilde{E}}(q, \tau + O(q)) + q^2 \left(3\epsilon + \frac{2\gamma}{2^m} + \frac{\rho}{2^n} + \max\left\{\frac{\gamma}{2^m}, \frac{\rho}{2^n}\right\} + \frac{1}{2^{n+m}}\right).$$

We also provide two instantiations of ENR with Feistel-based implementations of G.

Corollary 1. *Let $m = n$ and $\psi[H]$ be a balanced $2n$-bit (left-to-right, see the left of Fig. 2) Feistel using a round function $H : \Sigma^n \to \Sigma^n$. H is defined as $H(x) = K \cdot x$, where multiplication is defined over* GF(2^n) *and key K is uniformly random over* GF(2^n)*. Then we have*

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{ENR}[\psi[H],\widetilde{E}]}(q, \tau) \le 2\mathtt{Adv}^{\widetilde{\mathtt{sprp}}}_{\widetilde{E}}(q, \tau + O(q)) + \frac{5q^2}{2^{2n}}.$$

Proof. When $m = n$, every $2n$-bit keyed permutation is $(0, \gamma, \rho)$-AU for some $\gamma = \rho$. The probability of $\psi[H](x)_{[n+1,\ldots,2n]} = \psi[H](x')_{[n+1,\ldots,2n]}$ is at most γ for any $x \neq x'$, if H is γ-AXU. Here, our H is 2^{-n}-AXU, thus $\psi[H]$ is $(0, 2^{-n}, 2^{-n})$-AU. Combining this fact and Theorem 2 proves the corollary.

Corollary 2. *Let $m < n$, and K_1, K_2, and K_3 be independent and uniform over* GF(2^n) *(represented as n-bit values). We define $H_1 : \Sigma^n \to \Sigma^n$ as $H_1(x) = K_1 \cdot x$, and define $H_2 : \Sigma^{n-m} \to \Sigma^{n+m}$ as $H_2(x) = (K_2 \cdot \acute{x} \| K_3 \cdot \acute{x})_{[1,\ldots,n+m]}$, where $\acute{x} = x \| 0^m$. Then,*

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{ENR}[\psi[H_1,H_2],\widetilde{E}]}(q, \tau) \le 2\mathtt{Adv}^{\widetilde{\mathtt{sprp}}}_{\widetilde{E}}(q, \tau + O(q)) + q^2 \left(\frac{8}{2^{n+m}} + \frac{2}{2^{2n}}\right),$$

where $\psi[H_1, H_2]$ is a 2-round Feistel permutation with i-th round function H_i (the first round is balanced and the second is unbalanced, see the right of Fig. 2).

Proof. We show that $\psi[H_1, H_2]$ is (ϵ, γ, ρ)-AU with $\epsilon = 2^{-(n+m)}$, $\gamma = 2^{-n}$, and $\rho = 2^{-n} + 2^{-m}$. The proofs for ϵ and γ are easy, as H_2 is $2^{-(n+m)}$-AXU and H_1 is 2^{-n}-AXU. To prove ρ, let $\mathcal{E}_1$ denote the collision event on $\psi[H_1](x)_{[1,\ldots,n]}$ and let $\mathcal{E}_2$ denote the collision event on $\psi[H_1, H_2](x)_{[n+1,\ldots,n+m]}$. Here, ρ is obtained by bounding $\Pr(\mathcal{E}_2)$ for any two distinct inputs to $\psi[H_1, H_2]$, which is as follows.

$$\Pr(\mathcal{E}_2) = \Pr(\mathcal{E}_1)\cdot\Pr(\mathcal{E}_2|\mathcal{E}_1)+\Pr(\overline{\mathcal{E}_1})\cdot\Pr(\mathcal{E}_2|\overline{\mathcal{E}_1}) \le \Pr(\mathcal{E}_1)+\Pr(\mathcal{E}_2|\overline{\mathcal{E}_1}) \le 2^{-n}+2^{-m},$$

where the last inequality follows from that H_1 is 2^{-n}-AXU and $H_2(x)_{[n+1,\ldots,n+m]}$ is 2^{-m}-AXU. Combining this observation and Theorem 2, the proof is completed.

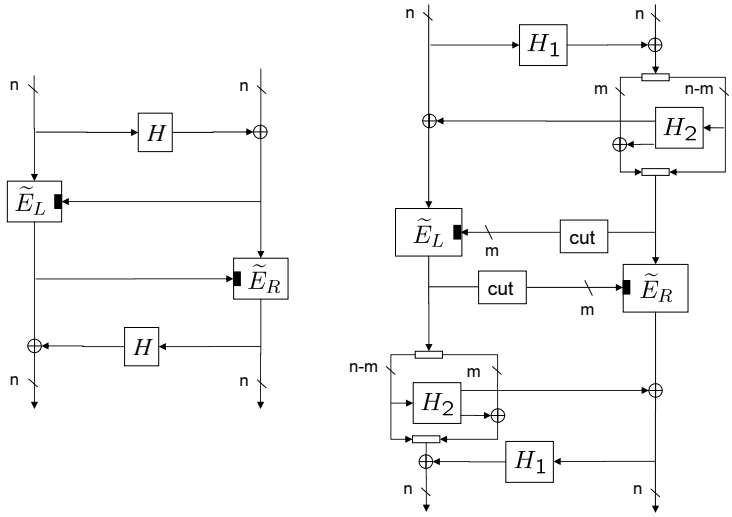

Fig. 2. Encryption of ENR. Left: the case $m = n$. Right: the case $m < n$.

4.3 Proof of Theorem 2

Setup. Let us abbreviate $\mathrm{ENR}[G, \widetilde{\mathsf{P}}_{n,m}]$ to ENR^*, where G is (ϵ, γ, ρ)-AU. We only present the information-theoretic part, that is, the indistinguishability of ENR^* from P_{2n} against any computationally unbounded $\mathtt{cca}$-adversary. The computational part is easy from the standard technique (see e.g., [2]). For convenience, we introduce some notations. For any $F : \mathcal{M} \times \Sigma \to \mathcal{M}$ with a set $\mathcal{M}$, $F[i] : \mathcal{M} \to \mathcal{M}$ is defined as $F[i](x) = F(x, i)$ for $i \in \Sigma$. For $F : \Sigma^{2n} \times \Sigma \to \Sigma^{2n}$, we define $\mathbb{G}F : \Sigma^{2n} \times \Sigma \to \Sigma^{2n}$ as

$$\mathbb{G}F(x, 0) = G^{-1}_{\mathtt{rev}} \circ F[0] \circ G(x), \quad \text{and } \mathbb{G}F(x, 1) = G^{-1} \circ F[1] \circ G_{\mathtt{rev}}(x). \quad (4)$$

Then, $\mathsf{DR} : \Sigma^{2n} \times \Sigma \to \Sigma^{2n}$ is defined as

$$\begin{aligned}\mathsf{DR}((x_l, x_r), 0) =& (U, \mathsf{R}_R(x_r, \widehat{U}, 0)), \text{ where } U = \mathsf{R}_L(x_l, \widehat{x_r}, 0),\\ \mathsf{DR}((x_l, x_r), 1) =& (\mathsf{R}_R(x_l, \widehat{T}, 1), T), \text{ where } T = \mathsf{R}_L(x_r, \widehat{x_l}, 1),\end{aligned} \tag{5}$$

using two independent URFs, R_L, $\mathsf{R}_R : \Sigma^n \times \Sigma^m \times \Sigma \to \Sigma^n$. Let $\widetilde{\mathsf{P}}_L$ and $\widetilde{\mathsf{P}}_R$ denote two independent instances of $\widetilde{\mathsf{P}}_{n,m}$. Using them, we also define $\mathsf{DP} : \Sigma^{2n} \times \Sigma \to \Sigma^{2n}$ in the same way as DR but R_R and R_L are substituted with $\langle \widetilde{\mathsf{P}}_R \rangle$ and $\langle \widetilde{\mathsf{P}}_L \rangle$, respectively. Here, note that $\mathbb{G}\mathsf{DP}$ is equivalent to $\langle \mathrm{ENR}^* \rangle$.

The proof outline is as follows. We analyze $\mathtt{cpa}'$-advantage between $\mathbb{G}\mathsf{DP}$ and $\langle \mathsf{P}_{2n} \rangle$, which corresponds to what we want from Eq. (2). Then, using the triangle inequality, we move as $\mathbb{G}\mathsf{DP} \Rightarrow \mathbb{G}\mathsf{DR} \Rightarrow \mathsf{R}_{2n+1,2n} \Rightarrow \langle \mathsf{P}_{2n} \rangle$, that is, we evaluate the maximum $\mathtt{cpa}'$-advantages for the game with $\mathbb{G}\mathsf{DP}$ and $\mathbb{G}\mathsf{DR}$ (Game 1), and the game with $\mathbb{G}\mathsf{DR}$ and $\mathsf{R}_{2n+1,2n}$ (Game 2), and the game with $\mathsf{R}_{2n+1,2n}$ and $\langle \mathsf{P}_{2n} \rangle$ (Game 3). Formally, we have

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{ENR}^*}(q) = \mathtt{Adv}^{\mathtt{cca}}_{\mathrm{ENR}^*, \mathsf{P}_{2n}}(q) = \mathtt{Adv}^{\mathtt{cpa}'}_{\langle \mathrm{ENR}^* \rangle, \langle \mathsf{P}_{2n} \rangle} = \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DP}, \langle \mathsf{P}_{2n} \rangle} \tag{6}$$

$$\leq \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DP}, \mathbb{G}\mathsf{DR}}(q) + \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DR}, \mathsf{R}_{2n+1,2n}}(q) + \mathtt{Adv}^{\mathtt{cpa}'}_{\mathsf{R}_{2n+1,2n}, \langle \mathsf{P}_{2n} \rangle}(q). \tag{7}$$

Analysis of Game 3. By extending the well-known PRP-PRF switching lemma (e.g., Lemma 1 of [4]), we easily get

$$\mathtt{Adv}^{\mathtt{cpa}'}_{\mathsf{R}_{2n+1,2n}, \langle \mathsf{P}_{2n} \rangle}(q) \leq \binom{q}{2} \cdot \frac{1}{2^{2n}}. \tag{8}$$

Analysis of Game 2. We first observe that

$$\mathbb{G}\mathsf{R}_{2n+1,2n} \equiv \mathsf{R}_{2n+1,2n}, \text{ and thus } \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DR}, \mathsf{R}_{2n+1,2n}}(q) = \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DR}, \mathbb{G}\mathsf{R}_{2n+1,2n}}(q), \tag{9}$$

since pre- and post-processing added by $\mathbb{G}$ are permutations. We consider an adversary, $\mathcal{D}$, accessing to F which is DR or $\mathsf{R}_{2n+1,2n}$. For each time period $i = 1, \ldots, q$, $\mathcal{D}$ can choose whether $F[0]$ or $F[1]$ is queried. This information is denoted by $W_i \in \Sigma$, and if $W_i = 0$, the input to $F[0]$ is denoted by $(SE_i, TE_i) \in \Sigma^n \times \Sigma^n$ (if $W_i = 1$, (SE_i, TE_i) is undefined), and the corresponding output is denoted by $(UE_i, VE_i) \in \Sigma^n \times \Sigma^n$. Similarly, if $W_i = 1$, the input to $F[1]$ and the output from $F[1]$ are denoted by (UD_i, VD_i) and (SD_i, TD_i), respectively (see Fig. 3). These notations will also be used for adversaries accessing to $\mathbb{G}F$. We define an MES $\mathcal{E} = e_0 e_1 \ldots$, where e_q denotes the event that

$$(SE_i, \widehat{TE_i}) \neq (SE_j, \widehat{TE_j}) \text{ and } (\widehat{UE_i}, TE_i) \neq (\widehat{UE_j}, VE_j), \text{and} \tag{10}$$

$$(UD_i, \widehat{TD_i}) \neq (UD_j, \widehat{TD_j}) \text{ and } (\widehat{UD_i}, VD_i) \neq (\widehat{UD_j}, VD_j), \tag{11}$$

holds for all possible $i \neq j$, $i, j \in \{1, \ldots, q\}$, e.g., Eq. (10) for $i \neq j$ with $W_i = W_j = 0$. Then, we obtain the following equivalence. Its proof is in Appendix B.

$$\mathsf{DR}^{\mathcal{E}} \equiv \mathsf{R}^{\mathcal{E}}_{2n+1,2n}. \tag{12}$$

From Eq. (12) and Lemma 2, we have

$$\mathbb{G}\mathsf{DR}^{\mathcal{E}} \equiv \mathbb{G}\mathsf{R}^{\mathcal{E}}_{2n+1,2n}. \tag{13}$$

Using Eqs. (9) and (13) and Theorem 1, we obtain

$$\mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DR},\mathsf{R}_{2n+1,2n}}(q) = \mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DR},\mathbb{G}\mathsf{R}_{2n+1,2n}}(q) \le \nu_{\mathtt{cpa}'}(\mathbb{G}\mathsf{R}_{2n+1,2n}, \overline{e_q}). \tag{14}$$

We leave the analysis of the last term of Eq. (14) for now.

Analysis of Game 1. We consider the indistinguishability between $\langle\widetilde{\mathsf{P}}_{n,m}\rangle$ and $\mathsf{R}_{n+m+1,n}$. We first focus on the input/output collision for the same tweak value. More precisely, let $(X_i, T_i, W_i) \in \Sigma^n \times \Sigma^m \times \Sigma$ denote the i-th input to $\langle\widetilde{\mathsf{P}}_{n,m}\rangle$ or $\mathsf{R}_{n+m+1,n}$, and let $Y_i \in \Sigma^n$ be the i-th output. For $b \in \Sigma$ and $t \in \Sigma^m$, let $\mathcal{X}^t_b = \{X_i : i \in \{1,\ldots,q\}, T_i = t, W_i = b\}$ and $\mathcal{Y}^t_b = \{Y_i : i \in \{1,\ldots,q\}, T_i = t, W_i = b\}$. Then, a_q denotes the event that

$$[\mathcal{X}^t_0 \cap \mathcal{Y}^t_1 = \emptyset] \wedge [\mathcal{X}^t_1 \cap \mathcal{Y}^t_0 = \emptyset] \text{ for all } t \in \Sigma^m.$$

The corresponding MES, $\mathcal{A} = a_0 a_1 \ldots$, is called the generalized collision-freeness (GCF). Then, we have

$$\langle\widetilde{\mathsf{P}}_{n,m}\rangle^{\mathcal{A}\wedge\mathcal{C}} \equiv \mathsf{R}^{\mathcal{A}}_{n+m+1,n}, \text{ for some MES } \mathcal{C}. \tag{15}$$

The proof of Eq.(15) is written in Appendix C. As mentioned, if we substitute R_L and R_R with $\langle\widetilde{\mathsf{P}}_L\rangle$ and $\langle\widetilde{\mathsf{P}}_R\rangle$, we will obtain DP. Thus, from Eq. (15), we get

$$\mathsf{DP}^{\mathcal{AL}\wedge\mathcal{CL}\wedge\mathcal{AR}\wedge\mathcal{CR}} \equiv \mathsf{DR}^{\mathcal{AL}\wedge\mathcal{AR}}, \text{ and } \mathbb{G}\mathsf{DP}^{\mathcal{AL}\wedge\mathcal{CL}\wedge\mathcal{AR}\wedge\mathcal{CR}} \equiv \mathbb{G}\mathsf{DR}^{\mathcal{AL}\wedge\mathcal{AR}}, \tag{16}$$

where $\mathcal{AL} = al_0 al_1 \ldots$ denotes the GCF for $\langle\widetilde{\mathsf{P}}_L\rangle$ or R_L, and $\mathcal{AR} = ar_0 ar_1 \ldots$ denotes the GCF for $\langle\widetilde{\mathsf{P}}_R\rangle$ or R_R, and $\mathcal{CL}$ and $\mathcal{CR}$ are some MESs (implied by Eq. (15)). The second equivalence follows from Lemma 2. Thus, using Theorem 1 we obtain

$$\mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DP},\mathbb{G}\mathsf{DR}}(q) \le \nu_{\mathtt{cpa}'}(\mathbb{G}\mathsf{DR}, \overline{al_q \wedge ar_q}). \tag{17}$$

For DR and $\mathsf{R}_{2n+1,2n}$, the occurrence of $al_q \wedge ar_q$ can be completely determined by the q inputs and outputs. From this fact and Lemma 5, we can *adjoin* $\mathcal{AL}\wedge\mathcal{AR}$ to the both sides of Eq. (12) and obtain

$$\mathsf{DR}^{\mathcal{E}\wedge\mathcal{AL}\wedge\mathcal{AR}} \equiv \mathsf{R}^{\mathcal{E}\wedge\mathcal{AL}\wedge\mathcal{AR}}_{2n+1,2n}. \tag{18}$$

Moreover, it is easy to see that $\mathcal{E} \wedge \mathcal{AL} \wedge \mathcal{AR} \equiv \mathcal{AL} \wedge \mathcal{AR}$ holds for DR and $\mathsf{R}_{2n+1,2n}$. Combining this observation, Eq. (18), and Lemmas 2 and 3, we have

$$\begin{aligned}
&\mathbb{G}\mathsf{DR}^{\mathcal{AL}\wedge\mathcal{AR}} \equiv \mathbb{G}\mathsf{R}^{\mathcal{AL}\wedge\mathcal{AR}}_{2n+1,2n}, \text{ and} \\
&\mathtt{Adv}^{\mathtt{cpa}'}_{\mathbb{G}\mathsf{DP},\mathbb{G}\mathsf{DR}}(q) \le \nu_{\mathtt{cpa}'}(\mathbb{G}\mathsf{DR}, \overline{al_q \wedge ar_q}) = \nu_{\mathtt{cpa}'}(\mathbb{G}\mathsf{R}_{2n+1,2n}, \overline{al_q \wedge ar_q}).
\end{aligned} \tag{19}$$

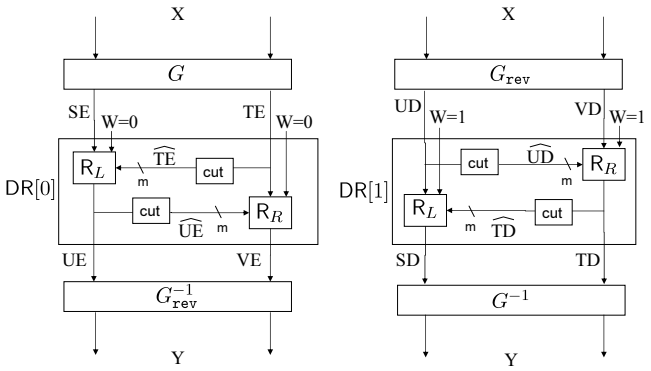

Fig. 3. $\mathbb{G}\mathsf{DR}$ function.

Collision probability analysis. Combining Eqs. (7), (8), (14), and (19), and Lemma 4, we have

$$\mathtt{Adv}^{\mathtt{sprp}}_{\mathrm{ENR}^*}(q) \le \binom{q}{2}\frac{1}{2^{2n}} + \sum_{\mathbf{ev}=\overline{e_q},\overline{al_q},\overline{ar_q}} \nu_{\mathtt{cpa}'}(\mathbb{G}\mathsf{R}_{2n+1,2n}, \mathbf{ev}). \tag{20}$$

We need to bound $\nu_{\mathtt{cpa}'}$ terms of Eq. (20). First, the maximum probabilities of $\overline{al_q}$ and $\overline{ar_q}$ (under $\mathbb{G}\mathsf{R}_{2n+1,2n}$) are the same because of the symmetry from Eq. (4) and that $G_{\mathtt{rev}}$ is a mirrored image of G. Thus we only need to evaluate the maximum probabilities of $\overline{al_q}$ and $\overline{e_q}$.

As shown by Eqs. (10) and (11), $\overline{e_q}$ consists of collision events such as

$$\begin{aligned}
&\mathrm{type}[\mathbf{e}_1] : (SE_i, \widehat{TE_i}) = (SE_j, \widehat{TE_j}), \qquad \mathrm{type}[\mathbf{e}_2] : (\widehat{UE_i}, TE_i) = (\widehat{UE_j}, TE_j)\\
&\mathrm{type}[\mathbf{e}_3] : (\widehat{UD_i}, VD_i) = (\widehat{UD_j}, VD_j), \quad \mathrm{type}[\mathbf{e}_4] : (UD_i, \widehat{TD_i}) = (UD_j, \widehat{TD_j})
\end{aligned}$$

for all possible $i \neq j$, $i, j \in \{1, \ldots, q\}$. Moreover, $\overline{al_q}$ consists of collision events such as

$$\begin{aligned}
&\mathrm{type}[\mathbf{a}_1] : (SE_i, \widehat{TE_i}) = (SE_j, \widehat{TE_j}), \qquad \mathrm{type}[\mathbf{a}_2] : (UE_i, \widehat{TE_i}) = (UE_j, \widehat{TE_j})\\
&\mathrm{type}[\mathbf{a}_3] : (UD_i, \widehat{TD_i}) = (UD_j, \widehat{TD_j}), \qquad \mathrm{type}[\mathbf{a}_4] : (SD_i, \widehat{TD_i}) = (SD_j, \widehat{TD_j})\\
&\mathrm{type}[\mathbf{a}_5] : (SE_i, \widehat{TE_i}) = (SD_j, \widehat{TD_j}), \qquad \mathrm{type}[\mathbf{a}_6] : (UE_i, \widehat{TE_i}) = (UD_j, \widehat{TD_j}).
\end{aligned}$$

Note that $\mathrm{type}[\mathbf{a}_1]$ and $\mathrm{type}[\mathbf{a}_3]$ are the same as $\mathrm{type}[\mathbf{e}_1]$ and $\mathrm{type}[\mathbf{e}_4]$, respectively. Let $\Pr[\mathbf{x}]$ be the maximum probability of $\mathrm{type}[\mathbf{x}]$-collision for $\mathbf{x} \in \{\mathbf{e}_1, \ldots, \mathbf{e}_4, \mathbf{a}_1, \ldots, \mathbf{a}_6\}$ under $\mathbb{G}\mathsf{R}_{2n+1,2n}$, where the maximum is taken for all q-$\mathtt{cpa}'$ (possibly adaptive) adversaries and for all $i, j \in \{1, \ldots, q\}$ with $i \neq j$. Using the union bound and the symmetry of $\mathbb{G}\mathsf{R}_{2n+1,2n}[0]$ and $\mathbb{G}\mathsf{R}_{2n+1,2n}[1]$, the

R.H.S. of Eq. (20) is at most

$$\binom{q}{2}\left(\frac{1}{2^{2n}}+\sum_{\mathrm{i}=1,\ldots 4}\Pr[\mathbf{e}_{\mathrm{i}}]+2\sum_{\mathrm{j}=1,\ldots 6}\Pr[\mathbf{a}_{\mathrm{j}}]\right). \tag{21}$$

From Eq. (9), the adversary's choice must be independent of (the key of) G and $G_{\mathtt{rev}}$. With this fact, each collision probability of Eq. (21) can be easily bounded for any $\mathtt{cpa}'$-adversary if G is (ϵ,γ,ρ)-AU[6]. The full description of our analysis is rather long[7], thus we here describe some typical examples. Other collision probabilities can be analyzed in a similar way. Let XE_i and YE_i be the i-th $2n$-bit input and output of $\mathbb{GR}_{2n+1,2n}$ with $W_i=0$ (they are undefined for i satisfying $W_i=1$). Similarly, XD_i and YD_i denote the i-th input and output with $W_i=1$.

- type[$\mathbf{e}_1$]. Here, a collision means $G(XE_i)_{[1,\ldots,n+m]}=G(XE_j)_{[1,\ldots,n+m]}$ for $XE_i\neq XE_j$. Moreover, XE_i and XE_j are independent of G's key. Thus we have $\Pr[\mathbf{e}_1]\leq\epsilon$ as G is assumed to be (ϵ,γ,ρ)-AU.
- type[$\mathbf{e}_2$]. Without loss of generality, we assume $i<j$. The probability of $TE_i=TE_j$ is at most γ, as G is (ϵ,γ,ρ)-AU. Since G is invertible, the inputs to $\mathsf{R}_{2n+1,2n}[0]$ are always distinct. This implies that $\widehat{UE}_j$ is independent of previous variables (including $\widehat{UE}_i$, TE_i and TE_j) and uniform, even conditioned by the event $TE_i=TE_j$. Thus we get

$$\Pr[\mathbf{e}_2]=\max_{i\neq j}\Pr[\widehat{UE}_i=\widehat{UE}_j|TE_i=TE_j]\cdot\Pr[TE_i=TE_j]\leq 2^{-m}\gamma. \tag{22}$$

- type[$\mathbf{a}_5$]. When $i<j$, $(SD_j,\widehat{TD}_j)$ is uniform and independent of $(SE_i,\widehat{TE}_i)$, thus collision probability is exactly $2^{-(n+m)}$. When $j<i$, $XE_i\neq YD_j$ must hold as we consider $\mathtt{cpa}'$-adversary (i.e., $XE_i=YD_j$ for $j<i$ means an intentional invertibility check). Hence

$$\begin{aligned}&\Pr[(SE_i,\widehat{TE}_i)=(SD_j,\widehat{TD}_j)]\\&=\Pr[G(XE_i)_{[1,\ldots,n+m]}=G(YD_j)_{[1,\ldots,n+m]}]\leq\epsilon.\end{aligned} \tag{23}$$

  Thus we have $\Pr[\mathbf{a}_5]\leq\max\{2^{-(n+m)},\epsilon\}$. Here, $\epsilon\geq 2^{-(n+m)}$ as it is the collision probability over $(n+m)$ bits.

In summary, we obtain all maximum collision probabilities:

$$\begin{aligned}&\Pr[\mathbf{e}_1]\leq\epsilon,\quad\Pr[\mathbf{e}_2]\leq 2^{-m}\gamma,\quad\Pr[\mathbf{e}_3]\leq\epsilon,\quad\Pr[\mathbf{e}_4]\leq 2^{-m}\gamma,\\&\Pr[\mathbf{a}_1]\leq\epsilon,\quad\Pr[\mathbf{a}_2]\leq 2^{-n}\rho,\quad\Pr[\mathbf{a}_3]\leq 2^{-m}\gamma,\\&\Pr[\mathbf{a}_4]\leq 2^{-(n+m)},\quad\Pr[\mathbf{a}_5]\leq\epsilon,\quad\Pr[\mathbf{a}_6]\leq\max\{2^{-m}\gamma,2^{-n}\rho\}.\end{aligned} \tag{24}$$

Combining Eqs. (24) and (21) proves the theorem.

[6] Note that if G is (ϵ,γ,ρ)-AU, the mirrored image of $G_{\mathtt{rev}}$ is also (ϵ,γ,ρ)-AU.

[7] This is mainly because we have to think of the cases when the adversary's choice is adaptive, even though it is independent of G.

4.4 PRP and PRF Versions of ENR

Although our primary target is a DBLC secure against CCA, a slight simplification of our proposal yields a CPA-secure variant of ENR. It saves some operations from the original ENR at the cost of a weaker attack class.

Definition 4. *The simplified* ENR *(*sENR*) is defined as* ENR *with* $G_{\mathtt{rev}}$ *being omitted (or, substituted with the identity function).*

Corollary 3. *Let* G *be* (ϵ, γ, ρ)*-AU. Then, the* cpa*-security of* $\mathrm{sENR}[G, \widetilde{E}]$ *is:*

$$\mathtt{Adv}^{\mathtt{prp}}_{\mathrm{sENR}[G,\widetilde{E}]}(q,\tau) \leq 2\mathtt{Adv}^{\widetilde{\mathtt{prp}}}_{\widetilde{E}}(q,\tau + O(q)) + q^2\left(\epsilon + \frac{\gamma}{2^m} + \frac{\rho}{2^{n+1}} + \frac{1}{2^{n+m}}\right).$$

The proof is similar to that of Theorem 2, thus is omitted here. The reason why $G_{\mathtt{rev}}$ can be omitted is that, we do not have to consider some bad events (e.g., the collision of $(\widehat{UD}, VD)$) that have to be avoided by $G_{\mathtt{rev}}$ when decryption query is possible. Moreover, by truncating the rightmost n-bit output, we obtain a PRF : $\Sigma^{2n} \to \Sigma^n$ which is $O(2^{(n+m)/2})$-secure for any $m = 1, \ldots, n$ (the proof is trivial from Corollary 3). We emphasize that ENR, and the simplified ENR, and its truncated-output version are optimally efficient, for they need exactly c calls of $\widetilde{E}$ when the output is cn bits, for $c = 1, 2$.

5 A Simple Construction of Tweakable Block Cipher with Beyond-birthday-bound Security

Our proposal requires a tweakable block cipher with beyond-birthday-bound security. Then, one may naturally ask how to realize it. A straightforward approach is building from scratch, e.g., Mercy [9] and HPC [8]. Recent studies [10][21] demonstrated that adding a tweak to some internal variables of a (generalized) Feistel cipher could yield a secure tweakable block cipher. This technique, called direct tweaking, may well be applied to a concrete tweakable cipher using (e.g.) S-box and linear diffusion. Another approach, which we focus on, is building from ordinary block ciphers. There are several schemes [16][24] that turn an n-bit block cipher into an (n, n)-bit tweakable cipher. However, they only have $O(2^{n/2})$-security[8]. Building a tweakable block cipher with better security has been considered as rather difficult (Liskov et al. mentioned it as an open problem [16]).

Our solution is simple and intuitive: changing keys depending on tweaks. This idea was possibly in mind of [16]. However, to our knowledge it has not been seriously investigated[9]. Although our scheme is simple, its security proof needs some cares. Throughout this section, we occasionally write E_K instead of E, if we need to specify the key we use.

[8] In [10], tweakable ciphers having "security against exponential attacks" are proposed. They correspond to $(2n, m)$-bit tweakable ciphers with $O(2^n)$-security, thus their security is up to the birthday bound of the block size.

[9] Liskov et al., said that a change of a tweak should be faster than a change of a key. This requirement is certainly desirable, however not mandatory one.

Definition 5. *For $E_K : \Sigma^n \to \Sigma^n$ with key $K \in \mathcal{K}$ and $F_{MK} : \Sigma^m \to \mathcal{K}$ with key $MK \in \mathcal{K}'$, Tweak-dependent Rekeying (TDR) is an (n, m)-bit tweakable cipher, where its encryption is $\mathrm{TDR}[E, F](x, t) = E_{F_{MK}(t)}(x)$, and decryption is $\mathrm{TDR}[E, F]^{-1}(y, t) = E^{-1}_{F_{MK}(t)}(y)$. Here, the key of $\mathrm{TDR}[E, F]$ is F's key, MK.*

Theorem 3. $\widetilde{\mathtt{Adv}^{\mathtt{sprp}}}_{\mathrm{TDR}[E,F]}(q, \tau) \le \mathtt{Adv}^{\mathtt{prf}}_F(\eta, \tau + O(q)) + \eta \mathtt{Adv}^{\mathtt{sprp}}_E(q, \tau + O(q))$, *where* $\eta \stackrel{\mathrm{def}}{=} \min\{q, 2^m\}$.

Proof. Let $\mathsf{R} : \Sigma^m \to \mathcal{K}$ be the URF. We have

$$\widetilde{\mathtt{Adv}^{\mathtt{sprp}}}_{\mathrm{TDR}[E,F]}(q, \tau) \le \widetilde{\mathtt{Adv}^{\mathtt{cca}}}_{\mathrm{TDR}[E,F],\mathrm{TDR}[E,\mathsf{R}]}(q, \tau) + \widetilde{\mathtt{Adv}^{\mathtt{sprp}}}_{\mathrm{TDR}[E,\mathsf{R}]}(q, \tau). \tag{25}$$

The first term of R.H.S. for Eq. (25) is clearly at most $\mathtt{Adv}^{\mathtt{prf}}_F(\eta, \tau + O(q))$, as we can evaluate F or R on at most η points. For the second term, the adversary can produce at most η instances of E, and their keys are independent and uniform (as keys are generated from URF). For each sampled key, the adversary can query at most q times[10]. Thus, the second term is at most $\eta \mathtt{Adv}^{\mathtt{sprp}}_E(q, \tau + O(q))$ from the triangle inequality.

At first glance, TDR seems to provide a desirable security, since it simulates the tweakable URP in an intuitive way. However, this is not always the case. For example, when $\mathcal{K} = \Sigma^n$ and $m = n$, a simple attack using about $2^{n/2}$ queries can easily distinguish TDR from $\widetilde{\mathsf{P}}_{n,n}$: we first query a fixed plaintext with many distinct tweaks, and if a ciphertext collision is found for tweak t and t', then query a new plaintext with tweaks t and t' and see if the new ciphertexts collide again[11].

Nevertheless, this scheme can have beyond-birthday-bound security if tweak length is not longer than the half of block length:

Corollary 4. *Let E_K be an n-bit block cipher with key $K \in \Sigma^n$. For $m < n/2$, let $E^{\shortparallel} : \Sigma^m \to \Sigma^n$ be defined as $E^{\shortparallel}(x) = E(x \| 0^{n-m})$. Then $\widetilde{\mathtt{Adv}^{\mathtt{sprp}}}_{\mathrm{TDR}[E,E^{\shortparallel}]}(q, \tau)$ is at most $(\eta + 1)\mathtt{Adv}^{\mathtt{sprp}}_E(q, \tau + O(q)) + \eta^2/2^{n+1}$, where $\eta = \min\{q, 2^m\}$.*

Here, $\mathrm{TDR}[E, E^{\shortparallel}]$ is secure if $2^{-(n-2m)}$ is sufficiently small and E is computationally secure, where "secure" means $\mathtt{cca}$-advantage being much smaller than 2^{-m}. Unfortunately, Corollary 4 does not tell us how large q is admissible by itself, since the first term of the bound would not be negligible if q is large. Nonetheless, as the first term is at least $\eta\tau + O(q)/2^n \approx q/2^{n-m}$ when $q \ge 2^m$ (achieved by the exhaustive key search, see [3]), we expect that $\mathrm{TDR}[E, E^{\shortparallel}]$ is computationally secure against attacks with $q \ll 2^{n-m}$ queries, if E is sufficiently secure.

[10] A more elaborate analysis can significantly improve the second term of the bound. However, it requires some additional parameters to describe the adversary's strategy and thus the result would look rather complicated. We here make it simple.

[11] This does not contradict with Theorem 3: the second term of the bound is at least $\eta(\tau + O(q))/|\mathcal{K}|$, which is about $q^2/2^n$ when $|\mathcal{K}| = 2^n$, as pointed out by Bellare et al. [3].

Practically, the big problem of TDR is the frequent key scheduling of E, as it may be much slower than encryption. Still, the negative impact on speed could be alleviated when on-the-fly key scheduling is possible.

Combining ENR and TDR. A combination of ENR and TDR provides a DBLC using an n-bit block cipher E. Let us consider combining the schemes from Corollaries 2 and 4. The resulting DBLC needs 4 calls of E and two key schedulings of E. By assuming $\mathtt{Adv}^{\mathtt{sprp}}_{E}(q,\tau) \approx q/2^n$, the security bound of this DBLC is about $2q/2^{n-m} + 8q^2/2^{(n+m)/2} + 2q^2/2^{2n} + 1/2^{n-2m}$. Then the choice $m \approx n/3$ achieves the security against $q \ll 2^{2n/3}$ queries for fixed n, which is the best possible for this combination. For example, if we use AES (i.e., $n = 128$) and set $m = 42$, the combined scheme's security is about 83.5-bit, assuming AES's security. Compared to the previous DBLCs having 64-bit security, the gain is not that large, but non-negligible. Of course, the security and efficiency of the resulting ENR would be greatly improved by using a better AES-based tweakable block cipher.

6 Conclusion

We described the extended Naor-Reingold (ENR), which converts an n-bit block tweakable block cipher into a $2n$-bit block cipher. ENR has the beyond-birthday-bound security (for n) if underlying tweakable block cipher does, and has almost the same throughput as that of the tweakable block cipher. Hence, we have shown that a good (i.e., fast and secure) tweakable cipher implies a good double-block-length cipher. We also described a way to convert an n-bit block cipher into tweakable one and achieves beyond-birthday-bound security based on the computational indistinguishability of the underlying block cipher. Unfortunately, this scheme has both theoretical and practical drawbacks due to its frequent rekeying. Thus, finding an efficient scheme without rekeying would be an important open problem.

Future directions. It would be interesting to extend ENR to mn-bit block cipher for $m > 2$ and make ENR tweakable, keeping beyond-birthday-bound security for n. Both problems can be basically solved by using ENR as a module of some known block cipher modes (e.g., CMC mode [12]) as they have $O(2^n)$-security with $2n$-bit pseudorandom permutation. However, more efficient constructions may well be possible.

Acknowledgments

We would like to thank Thomas Ristenpart, Tetsu Iwata, and the anonymous referees for very helpful comments and suggestions. We also thank Debra L. Cook for suggesting references.

References

1. W. Aiello and R. Venkatesan. "Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel." *Advances in Cryptology*- EUROCRYPT '96, LNCS 1070, pp. 307-320, 1996.
2. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. " A Concrete Security Treatment of Symmetric Encryption." *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, FOCS '97, pp. 394-403, 1997.
3. M. Bellare, T. Krovetz, and P. Rogaway. "Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible." *Advances in Cryptology*- EUROCRYPT '98, LNCS 1403, pp. 266- 280, 1998.
4. M. Bellare and P. Rogaway. "The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs." *Advances in Cryptology*- EUROCRYPT '06, LNCS 4004, pp. 409-426, 2006.
5. D. J. Bernstein. "Stronger Security Bounds for Wegman-Carter-Shoup Authenticators." *Advances in Cryptology*- EUROCRYPT '05, LNCS 3494, pp. 164-180, 2005.
6. G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti, and S. Marchesin. "Efficient Software Implementation of AES on 32-Bit Platforms." *Cryptographic Hardware and Embedded Systems*- CHES'02, LNCS 2523, pp. 129-142, 2003.
7. L. Carter and M. Wegman. "Universal Classes of Hash Functions." *Journal of Computer and System Science*, Vol. 18, pp. 143-154, 1979.
8. R. Schroeppel. "Hasty Pudding Cipher." `http://www.cs.arizona.edu/rcs/hpc`, 1998.
9. P. Crowley. "Mercy: A Fast Large Block Cipher for Disk Sector Encryption." *Fast Software Encryption*- FSE'00, LNCS 1978, pp. 49-63, 2000.
10. D. Goldenberg, S. Hohenberger, M. Liskov, E. C. Schwartz, and H. Seyalioglu. "On Tweaking Luby-Rackoff Blockciphers." *Advances in Cryptology*-ASIACRYPT'07, LNCS 4833, pp. 342-356, 2007.
11. O. Goldreich. "Modern Cryptography, Probabilistic Proofs and Pseudorandomness." Springer-Verlag, Algorithms and Combinatorics, Vol. 17, 1998.
12. S. Halevi and P. Rogaway. "A Tweakable Enciphering Mode." *Advances in Cryptology*-CRYPTO '03, LNCS 2729, pp. 482-499, 2003.
13. T. Iwata, T. Yagi, and K. Kurosawa. "On the Pseudorandomness of KASUMI Type Permutations." *Information Security and Privacy* -ACISP'03, Vol. 2727, 2003.
14. T. Iwata and K. Kurosawa. "OMAC: One-Key CBC MAC." *Fast Software Encryption*- FSE'03, LNCS 2887, pp. 129-153, 2003.
15. T. Iwata. "New Blockcipher Modes of Operation with Beyond the Birthday Bound Security." *Fast Software Encryption*- FSE'06, LNCS 4047, pp. 310-327, 2006.
16. M. Liskov, R. L. Rivest, and D. Wagner. "Tweakable Block Ciphers." *Advances in Cryptology*- CRYPTO'02, LNCS 2442, pp. 31-46, 2002.
17. M. Luby and C. Rackoff. "How to Construct Pseudo-random Permutations from Pseudo-random functions." *SIAM J. Computing*, Vol. 17, No. 2, pp. 373-386, 1988.
18. J. Patarin. "Security of Random Feistel Schemes with 5 or More Rounds." *Advances in Cryptology*- CRYPTO'04, LNCS 3152, pp. 106-122, 2004.
19. U. Maurer. "Indistinguishability of Random Systems." *Advances in Cryptology*- EUROCRYPT'02, LNCS 2332, pp. 110-132, 2002.
20. U. Maurer and K. Pietrzak. "The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations." *Advances in Cryptology* - EUROCRYPT'03, LNCS 2656, pp. 544-561, 2003.

21. A. Mitsuda and T. Iwata. "Tweakable Pseudorandom Permutation from Generalized Feistel Structure." *Provable Security* - ProvSec'08, LNCS 5324, 2008.
22. M. Naor and O. Reingold. "On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited." *Journal of Cryptology*, Vol. 12 (1), pp. 29-66, 1999.
23. S. Patel, Z. Ramzan, and G. Sundaram. "Towards Making Luby-Rackoff Ciphers Optimal and Practical." *Fast Software Encryption*, FSE'99, LNCS 1636, pp. 171-185, 1999.
24. P. Rogaway. "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC." Full version of *Advances in Cryptology*- ASIACRYPT'04. LNCS 3329, pp. 16-31, 2004, `http://www.cs.ucdavis.edu/~rogaway/papers/offsets.pdf`, Sep.24, 2006.
25. T. Krovetz. "Message Authentication on 64-Bit Architectures." *Selected Areas in Cryptography*- SAC'06, LNCS 4356, pp. 327-341, 2007.
26. S. Vaudenay. "On the Lai-Massey scheme." *Advances in Cryptology* - ASIACRYPT'99, LNCS 1716, pp. 8-10, 1999.
27. M. Wegman and L. Carter. "New Hash Functions and Their Use in Authentication and Set Equality." *Journal of Computer and System Sciences*, Vol. 22, pp. 265-279, 1981.
28. K. Yasuda. "A One-Pass Mode of Operation for Deterministic Message Authentication- Security beyond the Birthday Barrier." *Fast Software Encryption*, FSE'08, LNCS 5086, pp. 316-333, 2008.

A Lemmas from Maurer's Methodology

We describe some lemmas developed by Maurer [19] that we used in this paper. We assume that F and G are two random functions with the same input/output size; we define MESs $\mathcal{A} = a_0 a_1 \dots$ and $\mathcal{B} = b_0 b_1 \dots$ for F and G. The i-th input and output are denoted by X_i and Y_i for F (or G), respectively.

Lemma 1. *(Lemma* 1 (iv) *of [19]) If* $F|\mathcal{A} \equiv G|\mathcal{B}$ *and* $P^F_{a_i|X^iY^{i-1}a_{i-1}} \leq P^G_{b_i|X^iY^{i-1}b_{i-1}}$ *holds for* $i \geq 1$*, then there exists an MES* $\mathcal{C}$ *defined for* G *such that* $F^{\mathcal{A}} \equiv G^{\mathcal{B}\wedge\mathcal{C}}$*.*

Lemma 2. *(Lemma* 4 (ii) *of [19]) Let* $\mathbb{F}$ *be the function of* F *and* G *(i.e.,* $\mathbb{F}[F]$ *is a function that internally invokes* F*, possibly multiple times, to process its inputs). Here,* $\mathbb{F}$ *can be probabilistic, and if so, we assume* $\mathbb{F}$ *is independent of* F *or* G*. If* $F^{\mathcal{A}} \equiv G^{\mathcal{B}}$ *holds,* $\mathbb{F}[F]^{\mathcal{A}'} \equiv \mathbb{F}[G]^{\mathcal{B}'}$ *also holds, where* a'_i *denotes an event that* $\mathcal{A}$*-event is satisfied for the time period* i*. For example, if* $\mathbb{F}[F]$ *always invoke* F c *times for any input, then* $a'_i = a_{ci}$*.* $\mathcal{B}'$ *is defined in the same way.*

Lemma 3. *(Lemma* 6 (ii) *of [19]) If* $F^{\mathcal{A}} \equiv G^{\mathcal{B}}$ *holds for the attack class* `atk`*, then* $\nu_{\mathtt{atk}}(F, \overline{a_q}) = \nu_{\mathtt{atk}}(G, \overline{b_q})$ *holds.*

Lemma 4. *(Lemma* 6 (iii) *of [19])* $\nu_{\mathtt{atk}}(F, \overline{a_q \wedge b_q}) \leq \nu_{\mathtt{atk}}(F, \overline{a_q}) + \nu_{\mathtt{atk}}(F, \overline{b_q})$*.*

Lemma 5. *(An extension of Lemma* 2 (ii) *of [19]) If* $F^{\mathcal{A}} \equiv G^{\mathcal{B}}$*, then* $F^{\mathcal{A}\wedge\mathcal{C}} \equiv G^{\mathcal{B}\wedge\mathcal{C}}$ *holds for any MES* $\mathcal{C}$ *defined on the inputs and/or outputs.*

B Proof of Equation (12)

We focus on the indistinguishability between $\mathsf{DR}[0]$ and $\mathsf{R}_{2n,2n}$. Let $\mathrm{dist}(X^i, Y^j)$ denote an event that there is no collision among $\{X_1, \ldots, X_i, Y_1, \ldots, Y_j\}$. Let i-th input (to $\mathsf{DR}[0]$ or $\mathsf{R}_{2n,2n}$) be $X_i \stackrel{\text{def}}{=} (SE_i, TE_i) \in \Sigma^n \times \Sigma^n$, and i-th output be $Y_i \stackrel{\text{def}}{=} (UE_i, VE_i) \in \Sigma^n \times \Sigma^n$. We define events $il_q \stackrel{\text{def}}{=} \mathrm{dist}(SE^q, \widehat{TE^q})$ and $ir_q \stackrel{\text{def}}{=} \mathrm{dist}(\widehat{UE^q}, TE^q)$ and the corresponding MESs, $\mathcal{IL}$ and $\mathcal{IR}$. For $\mathsf{DR}[0]$, let us analyze the conditional probability of $\widehat{Y_q}$ (which equals to $\widehat{UE}_q$), given $X^q = x^q$, $Y^{q-1} = y^{q-1}$ and $il_q \wedge ir_q$. Note that the inputs to $\mathsf{R}_L[0]$ are distinct from il_q, which means $\widehat{Y^q}$ are independent and uniform. However, if $te_i = te_j$ for some $i \neq j$, $ue_i \neq ue_j$ must hold from ir_q. Thus, $\widehat{Y_q}$ is uniform over $\widehat{\mathcal{Y}}^c = \{0,1\}^m \setminus \widehat{\mathcal{Y}}$, where $\widehat{\mathcal{Y}} \stackrel{\text{def}}{=} \{ue_i : te_i = te_q, i = 1, \ldots, q-1\}$. The remaining $(2n-m)$ bits of Y_q are uniform over Σ^{2n-m} from il_q and ir_q. For $\mathsf{R}_{2n,2n}$, the set $\widehat{\mathcal{Y}}$ can be defined in the same way and Y_q (given $X^q = x^q$, $Y^{q-1} = y^{q-1}$ and $il_q \wedge ir_q$) is clearly uniformly distributed over $\widehat{\mathcal{Y}}^c \times \Sigma^{2n-m}$. Thus we have

$$P^{\mathsf{DR}[0]}_{Y_q | X^q Y^{q-1} il_q ir_q} = P^{\mathsf{R}_{2n,2n}}_{Y_q | X^q Y^{q-1} il_q ir_q}. \tag{26}$$

Next, we see that

$$P^{\mathsf{DR}[0]}_{il_q ir_q | X^q Y^{q-1} il_{q-1} ir_{q-1}}(x^q, y^{q-1}) = \begin{cases} 0 & \text{if } il_q \text{ is contradicted by } x^q, \\ \frac{|\widehat{\mathcal{Y}}^c|}{2^m} & \text{otherwise.} \end{cases} \tag{27}$$

holds true, as il_q is a function of x^q and the conditional probability of ir_q given $X^q = x^q$, $Y^{q-1} = y^{q-1}$, and $il_q \wedge b_{q-1}$ is the probability of $\widehat{Y_q} \notin \widehat{\mathcal{Y}}$, where $\widehat{Y_q}$ is uniform given il_q. Therefore, the conditional probability of ir_q is $|\widehat{\mathcal{Y}}^c|/2^m$ when x^q satisfies il_q. The same analysis also holds for $\mathsf{R}_{2n,2n}$. Thus we have

$$P^{\mathsf{DR}[0]}_{il_q ir_q | X^q Y^{q-1} il_{q-1} ir_{q-1}} = P^{\mathsf{R}_{2n,2n}}_{il_q ir_q | X^q Y^{q-1} il_{q-1} ir_{q-1}} \tag{28}$$

From Eqs. (26) and (28),

$$\mathsf{DR}[0]^{\mathcal{IL} \wedge \mathcal{IR}} \equiv \mathsf{R}^{\mathcal{IL} \wedge \mathcal{IR}}_{2n,2n}, \text{ and } \mathsf{DR}[1]^{\mathcal{IL}' \wedge \mathcal{IR}'} \equiv \mathsf{R}^{\mathcal{IL}' \wedge \mathcal{IR}'}_{2n,2n} \tag{29}$$

is obtained. The latter equivalence is derived by symmetry, where $\mathcal{IL}'$ and $\mathcal{IR}'$ are defined by $il'_q \stackrel{\text{def}}{=} \mathrm{dist}(UD^q, \widehat{TD^q})$ and $ir'_q \stackrel{\text{def}}{=} \mathrm{dist}(\widehat{UD^q}, VD^q)$ (here, i-th input is $X_i = (UD_i, VD_i)$ and output is $Y_i = (SD_i, TD_i)$). From Eq. (29) and the independence of $\mathsf{DR}[0]$ and $\mathsf{DR}[1]$, the proof is completed.

C Proof of Equation (15)

We abbreviate $\mathsf{R}_{n+m+1,n}$ and $\widetilde{\mathsf{P}}_{n,m}$ to R and P, respectively. From the definition of GCF event a_q, it is easy to derive

$$\langle \widetilde{\mathsf{P}} \rangle | \mathcal{A} \equiv \mathsf{R} | \mathcal{A}. \tag{30}$$

Next, we have

$$P^{\langle\widetilde{\mathsf{P}}\rangle}_{a_q|X^qY^{q-1}a_{q-1}}(x^q, y^{q-1}) = 1, \text{ and } P^{\mathsf{R}}_{a_q|X^qY^{q-1}a_{q-1}}(x^q, y^{q-1}) = 1 - \frac{\theta}{2^n}, \quad (31)$$

for any x_q consistent with a_q (given x^{q-1} and y^{q-1}), since $\langle\widetilde{\mathsf{P}}\rangle$'s output always keeps GCF, while R's output is uniform and thus has a chance to violate GCF. From Eq. (31), we get $P^{\mathsf{R}}_{a_q|X^qY^{q-1}a_{q-1}} \leq P^{\langle\widetilde{\mathsf{P}}\rangle}_{a_q|X^qY^{q-1}a_{q-1}}$. The proof is completed by combining this inequality, and Eq. (30), and Lemma 1.