Hybrid Symmetric Encryption Using Known-Plaintext Attack-Secure Components

Kazuhiko Minematsu and Yukiyasu Tsunoo

NEC Corporation, 1753 Shimonumabe, Nakahara-Ku,
Kawasaki 211-8666, Japan
k-minematsu@ah.jp.nec.com

Abstract. This paper describes a hybrid symmetric cipher that combines a strongly-secure function, e.g., a pseudorandom function (PRF), which is secure against any Chosen-Plaintext Attack, and a weak PRF, which is only secure against any Known-Plaintext Attack. Although this kind of composition is potentially faster than the modes of PRFs, it has not been extensively studied. Our main contribution is in proposing a new block cipher scheme that is suitable for hybrid composition. We describe efficient hybrid constructions of pseudorandom permutation and strong pseudorandom permutation for an arbitrarily large block size using our new scheme.

1 Introduction

In 1988, Luby and Rackoff [13] began studying the secure composition of cryptographic components. They showed that only a few iterations of a Feistel round could be secure against any Chosen-Plaintext Attack (CPA) or Chosen-Ciphertext Attack (CCA), if the underlying round functions were pseudorandom functions [8] (PRFs), i.e., secure against any CPA. Following Luby and Rackoff's work, many researchers have studied the compositions of various cryptographic systems.

In this paper, we discuss hybrid[1] symmetric encryptions combining a component secure against any Known-Plaintext Attack (KPA), which is called a weak PRF (WPRF), and a stronger component such as PRF. WPRFs were studied by many researchers [1, 6, 23, 24] and widely accepted as one of the weak cryptographic primitives. Since KPA is weaker attack than CPA, a WPRF is reasonably assumed to be faster than a PRF. For example, it was pointed out [6] that the WPRF based on the Decisional Diffie-Hellman (DDH) assumption could be more efficient than the DDH-based PRF proposed by Naor and Reingold [22]. Consider a mode that invokes a PRF. If almost all invocations of the PRF can be securely substituted with those of a WPRF, then the resulting mode would be much faster than the original mode based only on PRF. In practice, such hybrid modes can be seen as modes of operation for multiple cryptographic components that have different security-levels, such as a strongly secure block cipher and its reduced-round version, or a (strong) block cipher and a (weak) stream cipher.

[1] In this paper, "hybrid" means combining strong and weak primitives.

D. Won and S. Kim (Eds.): ICISC 2005, LNCS 3935, pp. 242–260, 2006.

Although the idea of using multiple components can be seen in previous studies, for instance Bear and Lion [2], none of them used WPRFs as their components.

The basic idea is that the cascade of a PRF and a WPRF is PRF. This is intuitively correct, since outputs of a PRF, which correspond to the WPRF's inputs, should be close to random in terms of computational indistinguishability. We first prove that this idea actually holds true, and propose a hybrid construction of a PRF with large output (and small input) based on this idea. Such a PRF can be used as a stream cipher accepting an initial vector (IV).

These results are also beneficial to hybrid block ciphers. We propose a new scheme for block ciphers that slightly differs from Feistel. It provides a pseudorandom permutation (PRP) that has double length (i.e., a $2n$-bit block cipher composed of n-bit block components) using one invocation of a PRP and a WPRF, and universal hash function [32] (UH)-based mixing. As it might be impossible to build a double length PRP using two WPRF invocations, our construction is optimal (in terms of the number of n-bit PRP invocation). Moreover, we show that such a hybrid composition is, in a sense, difficult with the original Feistel. Double length PRP has been extensively studied and many schemes have been proposed [13, 25, 27, 12, 19, 28]. However, to our knowledge, our scheme is the first construction that does not need two invocations of a PRF (or PRP).

In addition, our scheme is useful for building a large block cipher. Using our hybrid block cipher scheme combined with our hybrid large output PRF, we build an mn-bit strong PRP (SPRP), which is secure against any combination of CPA and Chosen-Ciphertext Attack (CCA). A large block SPRP has desirable properties for storage encryption [35]. Our construction requires two invocations of an n-bit SPRP, $(m-2)$ invocations of an n-bit WPRF, and two Feistel rounds with UHs, for all $m > 2$. Therefore, its throughput will be close to that of the WPRF we intend to use, and the underlying n-bit SPRP's throughput will not be a problem with a large block size. For a comparison, NR mode [25], which is a highly sophisticated mode to provide a large block SPRP, requires m invocations of an n-bit SPRP and two mixing layers to provide a mn-bit block SPRP. These examples illustrate that our hybrid block cipher construction is highly optimized for both small and large block sizes.

All our security analyses are based on the standard security notions of symmetric cryptography introduced by Bellare et al. [3] and a natural extension of this to deal with KPA, which is the same as the previous studies [1, 6, 22]. We also use a framework that was proposed by Maurer [17] to perform a rigorous security analysis.

2 Preliminaries

2.1 Random Functions and Their Composition

Definition 1. *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Random function (RF) $\mathbf{F} : \mathcal{X} \to \mathcal{Y}$ is a random variable distributed over all functions $\mathcal{X}$ to $\mathcal{Y}$*[2]*. If $\mathbf{F}$ is distributed*

[2] If $\mathbf{F}$ has key K, uniformly distributed over $\mathcal{K}$, then there is function $f : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ such that $\mathbf{F}(x) = f(K, x)$ and $\Pr[\mathbf{F}(x) = y] = |\{k \in \mathcal{K} : f(k, x) = y\}|/|\mathcal{K}|$.

over all permutations on $\mathcal{X}$, it is called a random permutation (RP) on $\mathcal{X}$. A uniform random function (URF) : $\{0,1\}^n \rightarrow \{0,1\}^m$ is an RF with uniform distribution on all functions $\{0,1\}^n$ to $\{0,1\}^m$ and denoted by $\mathbf{R}_{n,m}$. A uniform random permutation (URP) on $\{0,1\}^n$ is an RP with uniform distribution on all n-bit permutations and denoted by $\mathbf{P}_n$.

Note that, in this paper, the word "random" does not imply uniformity. It only means it is probabilistic. We used bold symbols for RFs. When $\mathbf{F}$ and $\mathbf{G}$ are two RFs that have the same input/output space, we say they are *compatible.*

For simplicity, most of our results deal with cases when n-bit block components are used. We will use the following composition operators.

Definition 2. *Let $\mathbf{F} : \mathcal{X} \rightarrow \mathcal{Y}$, and $\mathbf{G} : \mathcal{Y} \rightarrow \mathcal{Z}$. Let $\mathbf{F} \circ \mathbf{G} : \mathcal{X} \rightarrow \mathcal{Z}$ such that $\mathbf{F} \circ \mathbf{G}(x) = \mathbf{G}(\mathbf{F}(x))$*[3] *, and let $\mathbf{F} \lhd \mathbf{G} : \mathcal{X} \rightarrow \mathcal{Y} \times \mathcal{Z}$ such that $\mathbf{F} \lhd \mathbf{G}(x) = (\mathbf{F}(x), \mathbf{G}(\mathbf{F}(x)))$ for all $x \in \mathcal{X}$.*

2.2 Security Measures and Their Properties

We breifly describe our security measures in a standard framework introduced by Bellare et al.[3]. Let $\mathbf{F}, \mathbf{G}$ be two compatible RFs. Let $\mathbf{D}$ be an attacker that can access the encryption oracle (EO). Here, EO has implemented $\mathbf{H}$, which is equivalent to either $\mathbf{F}$ or $\mathbf{G}$. $\mathbf{D}$ determines whether $\mathbf{H}$ is $\mathbf{F}$ or $\mathbf{G}$ after a predetermined number of queries and answers. The advantage of $\mathbf{D}$ is defined as

$$V(\mathbf{F},\mathbf{G}|\mathbf{D}) \overset{\text{def}}{=} |\Pr[\mathbf{D}\text{'s guess is } \mathbf{F}|\mathbf{H}=\mathbf{F}] - \Pr[\mathbf{D}\text{'s guess is } \mathbf{F}|\mathbf{H}=\mathbf{G}]|. \quad (1)$$

Definition 3. *The CPA-advantage (KPA-advantage) is defined as the maximal advantage of all attackers using CPA (KPA). That is,*

$$\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{G}}(q,\tau) \overset{\text{def}}{=} \max_{\mathbf{D}:(q,\tau)\text{-}CPA} V(\mathbf{F},\mathbf{G}|\mathbf{D}),\ \mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{G}}(q,\tau) \overset{\text{def}}{=} \max_{\mathbf{D}:(q,\tau)\text{-}KPA} V(\mathbf{F},\mathbf{G}|\mathbf{D}).$$

Here, (q,τ)-CPA denotes a CPA that uses q queries with time complexity τ[4]*. Similarly, (q,τ)-KPA denotes a KPA that uses q independent and uniformly random queries with time complexity τ. Especially, let $\mathbf{R}$ be a URF compatible to $\mathbf{F}$. Then, $\mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}}(q,\tau) \overset{\text{def}}{=} \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{R}}(q,\tau)$ and $\mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau) \overset{\text{def}}{=} \mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{R}}(q,\tau)$. If $\mathbf{F}$ is an RP, we have $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{F}}(q,\tau) \overset{\text{def}}{=} \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{P}}(q,\tau)$ where $\mathbf{P}$ is the URP.*

Finally, we will define the CCA-advantage. This provides the security against an attacker who can adaptively choose a plaintext (a ciphertext) and receive the ciphertext (the plaintext). It can be defined as a variant of the CPA-advantage.

Definition 4. *Let $\mathbf{F}$ and $\mathbf{G}$ be two RPs on $\mathcal{X}$. The inverse of $\mathbf{F}$ is denoted by $\mathbf{F}^{-1}$. Let $\langle\mathbf{F}\rangle$ be the RF:$\mathcal{X} \times \{0,1\} \rightarrow \mathcal{X}$ such that $\langle\mathbf{F}\rangle(x_i,d_i) = \mathbf{F}(x_i)$ if*

[3] Note that the definition of $\circ$ is different from the standard one.

[4] The time complexity includes the worst case execution time and the program size, in some fixed RAM computation model.

$d_i = 0$ and $\mathbf{F}^{-1}(x_i)$ if $d_i = 1$. The CCA-advantage is defined as $\mathrm{Adv}^{\mathrm{cca}}_{\mathbf{F},\mathbf{G}}(q,\tau) \overset{\mathrm{def}}{=} \mathrm{Adv}^{\mathrm{cpa}}_{\langle\mathbf{F}\rangle,\langle\mathbf{G}\rangle}(q,\tau)$ *and we have* $\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{F}}(q,\tau) \overset{\mathrm{def}}{=} \mathrm{Adv}^{\mathrm{cca}}_{\mathbf{F},\mathbf{P}}(q,\tau)$*.*

If $\mathbf{F}$ has a small CPA-advantage for some sufficiently large q and τ in distinguishing $\mathbf{F}$ from URF, it is called a pseudorandom function (PRF). In addition, if $\mathbf{F}$ is invertible, it is called a pseudorandom permutation (PRP). Similarly, if $\mathbf{F}$ has a small KPA-advantage, it is called a weak PRF [24] (WPRF), and if $\mathbf{F}$ is an RP and has a small CCA-advantage, it is called a strong PRP (SPRP).

It is well known that triangle inequality holds for the CPA, KPA, and CCA-advantages. More precisely, we have $\mathrm{Adv}^{***}_{\mathbf{F},\mathbf{H}}(q,\tau) \le \mathrm{Adv}^{***}_{\mathbf{F},\mathbf{G}}(q,\tau) + \mathrm{Adv}^{***}_{\mathbf{G},\mathbf{H}}(q,\tau)$ for $*** \in \{\mathrm{cpa}, \mathrm{kpa}, \mathrm{cca}\}$.

Let $\mathbf{F}, \mathbf{G}$ be compatible RFs with n-bit input, and let $\mathbf{R}$ be the URF with n-bit output. The following equation plays an important role in our analysis.

$$\mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{G}}(q,\tau) = \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{R}\triangleleft\mathbf{F},\mathbf{R}\triangleleft\mathbf{G}}(q,\tau'), \text{ where } \tau = \tau + O(nq). \tag{2}$$

This is natural, since all adaptive attacks are useless in distinguishing $\mathbf{R}\triangleleft\mathbf{F}$ from $\mathbf{R}\triangleleft\mathbf{G}$. Actually, the difference between $\mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{G}}(q,\tau)$ and $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{R}\triangleleft\mathbf{F},\mathbf{R}\triangleleft\mathbf{G}}(q,\tau)$ only depends on the time for generating uniformly random plaintexts (for $\mathbf{F}$ and $\mathbf{G}$). We assume that the time for generating q uniformly random plaintexts needs $O(nq)$ time. Hereafter, $\mathcal{X}$ denotes $\{0,1\}^n$ and τ' denotes $\tau + O(nq)$.

Lemma 1. *For any* $\mathbf{F}$ *and* $\mathbf{G}$ *,* $\mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{G}}(q,\tau) \le \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{G}}(q,\tau)$*. Moreover, let* $\mathbf{E}$ *be an RF that can be cascaded to* $\mathbf{F}$ *and* $\mathbf{G}$*, and* $\mathbf{R}$ *be the URF compatible with* $\mathbf{E}$*. Then,* $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{E}\triangleleft\mathbf{F},\mathbf{E}\triangleleft\mathbf{G}}(q,\tau) \le 2\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{E},\mathbf{R}}(q,\tau) + \mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{F},\mathbf{G}}(q,\tau')$*.*

Proof. The first claim is obvious. For the second, we have

$$\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{E}\triangleleft\mathbf{F},\mathbf{E}\triangleleft\mathbf{G}}(q,\tau) \le \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{E}\triangleleft\mathbf{F},\mathbf{R}\triangleleft\mathbf{F}}(q,\tau) + \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{R}\triangleleft\mathbf{F},\mathbf{R}\triangleleft\mathbf{G}}(q,\tau) + \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{R}\triangleleft\mathbf{G},\mathbf{E}\triangleleft\mathbf{G}}(q,\tau).$$

Combining the above inequality with Eq. (2) proves the second claim.

2.3 Monotone Event Sequence and Conditional Equivalences

We will use a methodology developed by Maurer [17, 18] to analyze information-theoretic security, i.e., the maximum advantage without computational restrictions. Here, let us briefly describe his notations. Consider event a_i defined for i input/output pairs of $\mathbf{F}$. Let $\overline{a_i}$ be the negation of a_i. We assumed a_i was monotone, i.e., a_i never occurred if $\overline{a_{i-1}}$ occurred. For instance, a_i is monotone if this indicates that all i outputs are distinct. An infinite sequence of monotone events $\mathcal{A} = a_0 a_1 \ldots$ is called a monotone event sequence (MES). Here, a_0 denotes some tautological event. Note that $\mathcal{A} \wedge \mathcal{B} = (a_0 \wedge b_0)(a_1 \wedge b_1)\ldots$ is an MES if $\mathcal{A} = a_0 a_1 \ldots$ and $\mathcal{B} = b_0 b_1 \ldots$ are both MESs. For any sequence of random variables, $X_1, X_2, \ldots$, let X^i denote $(X_1, \ldots, X_i)$. After this, $\mathrm{dist}(X^i)$ will denote an event where $X_1, X_2, \ldots, X_i$ are distinct.

Let MESs $\mathcal{A}$ and $\mathcal{B}$ be defined for $\mathbf{F} : \mathcal{X} \to \mathcal{Y}$ and $\mathbf{G} : \mathcal{X} \to \mathcal{Y}$, respectively. Let $X_i \in \mathcal{X}$ and $Y_i \in \mathcal{Y}$ be the i-th input and output. Let $P^{\mathbf{F}}$ be the probability space defined by $\mathbf{F}$. For example, $P^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y^i, x^i)$ means $\Pr[Y_i = y_i | X^i = x^i, Y^{i-1} = y^{i-1}]$ where $Y_j = \mathbf{F}(X_j)$ for $j = 1, \ldots$.

Definition 5. *Let us say* $\mathbf{F}$ *and* $\mathbf{G}$ *are equivalent and write* $\mathbf{F} \equiv \mathbf{G}$ *if* $P^{\mathbf{F}}_{Y_i|X^iY^{i-1}} = P^{\mathbf{G}}_{Y_i|X^iY^{i-1}}$*, which means* $P^{\mathbf{F}}_{Y_i|X^iY^{i-1}}(y^i, x^i) = P^{\mathbf{G}}_{Y_i|X^iY^{i-1}}(y^i, x^i)$ *for all* $x^i \in \mathcal{X}^i$*,* $y^i \in \mathcal{Y}^i$ *and for all* $i \geq 1$*.*

Definition 6. *We write* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$ *if* $P^{\mathbf{F}}_{Y_ia_i|X^iY^{i-1}a_{i-1}} = P^{\mathbf{G}}_{Y_ib_i|X^iY^{i-1}b_{i-1}}$[5] *holds, which means* $P^{\mathbf{F}}_{Y_ia_i|X^iY^{i-1}a_{i-1}}(y^i, x^i) = P^{\mathbf{G}}_{Y_ib_i|X^iY^{i-1}b_{i-1}}(y^i, x^i)$ *holds for all* (y^i, x^i) *such that both* $P^{\mathbf{F}}_{a_{i-1}|X^{i-1}Y^{i-1}}(y^{i-1}, x^{i-1})$ *and* $P^{\mathbf{G}}_{b_{i-1}|X^{i-1}Y^{i-1}}(y^{i-1}, x^{i-1})$ *are positive for all* $i \geq 1$*.*

Definition 7. *We write* $\mathbf{F}|\mathcal{A} \equiv \mathbf{G}|\mathcal{B}$ *if* $P^{\mathbf{F}}_{Y_i|X^iY^{i-1}a_i} = P^{\mathbf{G}}_{Y_i|X^iY^{i-1}b_i}$ *holds. Moreover, let* $\mathcal{C} = c_0c_1\ldots$ *be an MES defined for* $\mathbf{F}$*. We write* $\mathbf{F}^{\mathcal{A}}|\mathcal{C} \equiv \mathbf{G}^{\mathcal{B}}$ *if* $P^{\mathbf{F}}_{Y_ia_i|X^iY^{i-1}a_{i-1}c_i} = P^{\mathbf{G}}_{Y_ib_i|X^iY^{i-1}b_{i-1}}$ *holds.*

Note that if $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$, then $\mathbf{F}|\mathcal{A} \equiv \mathbf{G}|\mathcal{B}$ (but not vice versa).

Definition 8. *For* $\mathcal{A}$ *defined for* $\mathbf{F}$*,* $\nu(\mathbf{F}, \overline{a_q})$ *denotes the maximal probability of* $\overline{a_q}$ *for any* (q, ∞)*-CPA that interacts with* $\mathbf{F}$*. Similarly,* $\mu(\mathbf{F}, \overline{a_q})$ *denotes the maximal probability of* $\overline{a_q}$ *for any non-adaptive* (q, ∞)*-CPA.*

Clearly, $\mu(\mathbf{F}, \overline{a_q}) \leq \nu(\mathbf{F}, \overline{a_q})$ holds. In addition, $\mu(\mathbf{F}, \overline{a_q})$ equals $\max_{x^q \in \mathcal{X}^q} P^{\mathbf{F}}_{\overline{a_q}|X^q}$, which often makes the analysis of $\mu(\mathbf{F}, \overline{a_q})$ much easier than that of $\nu(\mathbf{F}, \overline{a_q})$.

These equivalences are crucial to the proof of information-theoretic security. For example, if $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$, then $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{G}}(q, \infty) \leq \nu(\mathbf{F}, \overline{a_q})$ (Theorem 6 in Appendix A). Moreover, one can turn the analysis of adaptive attacks (i.e., $\nu(*, *)$) into that of non-adaptive attacks (i.e., $\mu(*, *)$) under some additional conditions. We will use a number of Maurer's results including Theorem 6, as these often provide a rigorous security proof, which can not be obtained with other methods[6]. For completeness, these results are cited in Appendix A.

Caveat. Maurer's methodology [17] can only be applied to an information-theoretic setting. In most cases information-theoretic proofs can be easily converted into computational ones, but this is not always the case [18, 21]. However, we do not encounter such difficulties in this paper. His methodology can also be applied to *random systems*, i.e., stateful random functions. We will use some random systems in our proofs for convenience, but in practice, none of our hybrid modes require underlying components to be stateful.

2.4 Why We Should Care About Hybrid Modes?

As we mentioned, the focus of this paper is modes for a PRF combined with a WPRF. However, why do we need such hybrid modes as we already have PRFs? The main advantage of hybrid modes is throughput, since a WPRF is

[5] Here, $P^{\mathbf{F}}_{Y_ia_i|X^iY^{i-1}a_{i-1}}(y^i, x^i)$ is $\Pr[Y_i = y_i, a_i|a_{i-1}, X^{i-1} = x^{i-1}, Y^{i-1} = y^{i-1}]$.

[6] For example, let $\mathbf{C}$ be a $2n$-bit 3-round Feistel with PRFs. Classical analysis requires $q^2/2^{2n}$ as a term appearing in the upper bound of $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{C}}(q, \tau)$, while Maurer [17] showed this was redundant.

naturally assumed to be faster than a compatible PRF. The following examples demonstrate that this assumption actually holds true in some cases.

Example 1. Let $\mathbf{M}[\mathbf{F}_1, \mathbf{F}_2]$ denote a $2n$-bit 2-round Feistel, where $\mathbf{F}_i$ is the i-th round function:$\mathcal{X} \to \mathcal{X}$ for $i = 1, 2$ (recall that $\mathcal{X}$ denotes $\{0,1\}^n$). The first round of $\mathbf{M}[\mathbf{F}_1, \mathbf{F}_2]$ is left-to-right. That is, the input to $\mathbf{F}_1$ is the left half of the input to $\mathbf{M}[\mathbf{F}_1, \mathbf{F}_2]$. It is well known that the 3-round Feistel where each round function is an independent PRF is PRP. However, the following lemma shows that the 2-round Feistel, which can never be a PRP, can be KPA-secure.

Lemma 2. $\mathrm{Adv}^{\mathrm{kpa}}_{\mathbf{M}[\mathbf{F}_1,\mathbf{F}_2],\mathbf{P}_{2n}}(q, \tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}_1}(q, \tau) + \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}_2}(q, \tau) + \frac{q^2}{2^n}$.

This lemma is proved by a simple non-adaptive analysis similar to Maurer [15].

Actually, a similar result can be obtained for a generalized Feistel. For example, the type I transformation [33] on mn-bit block input requires $2m - 1$ rounds to achieve $2^{n/2}$-bit CPA-security [20] (i.e., the CPA-advantage is negligibly small if $q \ll 2^{n/2}$), whereas m rounds are sufficient to attain $2^{n/2}$-bit KPA-security. However, we omitted the formal descriptions of these results here.

As another example, it was pointed out [6] that the WPRF based on the DDH assumption could be more efficient than the DDH-based PRF construction proposed by Naor and Reingold [22]. These examples illustrate that well-designed hybrid modes can be faster than modes that only use PRFs.

Basically, we can only use WPRFs as building blocks. A mode proposed by Damgård and Nielsen [6] can convert any WPRF into a pseudorandom generator (PRG), which implies that any WPRF can be converted into a PRF using the PRG-to-PRF conversion [7]. However, this takes too much computation time and hence is rather impractical. Still, our proposals can be seen as modes of WPRF if this KPA-to-CPA conversion is incorporated into them[7].

3 Hybrid Construction of Large Output PRF

The basic idea behind hybrid modes is that the cascade of a PRF and a WPRF is a PRF. If the WPRF has large output, then the cascade would have almost the same throughput as that of the WPRF. This idea is intuitively correct. Actually, a similar idea was originally proposed by Aiello, Rajagopalan, and Venkatesan[1], without complete security proof (in fact, they only proved Lemma 3). In this section, we will describe our hybrid construction of a large output PRF called ARV[8], and prove it is secure.

Definition 9. *Let* $\mathbf{F}_1 : \mathcal{X} \to \mathcal{X}$ *be a PRF and* $\mathbf{F}_2 : \mathcal{X} \to \mathcal{X}$ *be a WRPF.* ARV *is defined as* $\mathrm{ARV}_m[\mathbf{F}_1, \mathbf{F}_2] \overset{\mathrm{def}}{=} \mathbf{F}_1 \circ L_{\mathbf{F}_2,m}$ *(see Def.2 for the def. of* $\circ$*) , where* $L_{\mathbf{F}_2,m} : \mathcal{X} \to \mathcal{X}^m$ *is* $L_{\mathbf{F}_2,m}(x) = (\mathbf{F}_{2,1}(x), \mathbf{F}_{2,2}(x), \ldots, \mathbf{F}_{2,m}(x))$ *for any* $x \in \mathcal{X}$*. Here,* $\mathbf{F}_{2,1}, \ldots, \mathbf{F}_{2,m}$ *are independently-keyed* m *RFs that are equivalent to* $\mathbf{F}_2$*.*

[7] The term "KPA-to-CPA" conversion was also used in [6]. However, it was not intended as a conversion of WPRF into PRF.

[8] Even though Aiello et al.'s proposal was slightly different from ours, we still called it ARV.

Before analyzing ARV, we have to formally prove that the cascade of PRF and WPRF is PRF.

Theorem 1. *Let* $\mathbf{G} = \mathbf{C} \circ \mathbf{F}$ *and* $\mathbf{G}' = \mathbf{C} \lhd \mathbf{F}$*, where* $\mathbf{C} : \mathcal{X} \to \mathcal{X}$*, and* $\mathbf{F} : \mathcal{X} \to \mathcal{X}^m$*. Then,*

$$\mathrm{Adv}^{\mathrm{prf}}_{\mathbf{G}}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{G}'}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{C}}(q,\tau) + \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau') + \frac{q^2}{2^{n+1}}. \quad (3)$$

Proof. The first inequality is obvious. For the second inequality, let $\mathbf{H}_1$ and $\mathbf{H}_2$ be $\mathbf{R}_{n,n} \lhd \mathbf{F}$, and $\mathbf{R}_{n,n} \lhd \mathbf{R}_{n,mn}$, respectively. We then obtain $\mathrm{Adv}^{\mathrm{prf}}_{\mathbf{G}'}(q,\tau) \le \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G}',\mathbf{H}_1}(q,\tau) + \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{H}_1,\mathbf{H}_2}(q,\tau) + \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{H}_2}(q,\tau)$. It is easy to see that $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G}',\mathbf{H}_1}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{C}}(q,\tau)$ and $\mathrm{Adv}^{\mathrm{prf}}_{\mathbf{H}_2}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{H}_2}(q,\infty) < \frac{q^2}{2^{n+1}}$. Finally, $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{H}_1,\mathbf{H}_2}(q,\tau) \le \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau')$ follows from Eq. (2).

Now, the remaining task is to show the KPA-advantage of $L_{\mathbf{F}_2,m}$. This is easily derived from triangle inequality.

Lemma 3. *(in [1, 6]) Let* $\mathbf{F} : \mathcal{X} \to \mathcal{X}$*. Then,* $\mathrm{Adv}^{\mathrm{wprf}}_{L_{\mathbf{F},m}}(q,\tau) \le m \cdot \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau)$*.*

From Theorem 1 and Lemma 3, it is obvious that using $\mathbf{F}_1(x_i)$ as part of the i-th output does not compromise the security of ARV. That is, we can use $\lhd$ instead of $\circ$. We thus have the following corollary.

Corollary 1. *Let* $\mathrm{ARV}^+_m[\mathbf{F}_1,\mathbf{F}_2] \overset{\mathrm{def}}{=} \mathbf{F}_1 \lhd L_{\mathbf{F}_2,m}$*. Then,* $\mathrm{Adv}^{\mathrm{prf}}_{\mathrm{ARV}_m[\mathbf{F}_1,\mathbf{F}_2]}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathrm{ARV}^+_m[\mathbf{F}_1,\mathbf{F}_2]}(q,\tau) \le \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}_1}(q,\tau) + m \cdot \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}_2}(q,\tau') + \frac{q^2}{2^{n+1}}$.

An advantage of ARV^+ over ARV is that the former guarantees an improved throughput for any small m whenever $\mathbf{F}_2$ is faster than $\mathbf{F}_1$.

Smaller key size. Althought the key size of $L_{\mathbf{F},m}$ is large (i.e., m keys), a mode of WPRF proposed by Damgård and Nielsen [6] reduces the key size to $2\log_2 m$. However, we will not discuss the key scheduling issue in this paper.

4 Hybrid Construction of PRP

4.1 Hybrid Double Length PRP is Difficult Within 3-Round Feistel

In this section, we deal with the hybrid construction of a PRP. Our first target is a double length PRP (DLPRP). More specifically, we want to build a PRP on $\mathcal{X}^2$ using a PRF: $\mathcal{X} \to \mathcal{X}$ and a WPRF: $\mathcal{X} \to \mathcal{X}$. It is well known that the cascade of a light-weight mixing and two Feistel rounds where round functions are two independent PRFs is a DLPRP (this was first pointed out by Lucks [14]). To implement the light-weight mixing, no cryptographic functions are needed: one Feistel round using ϵ-AXU [25] with an adequately small ϵ is enough. Here, ϵ-AXU is defined as follows. There have been many proposals for practical and efficient ϵ-AXUs, for instance MMH [9].

Definition 10. *Let* $\mathbf{F} : \mathcal{X} \to \mathcal{Y}$*. If* $\mathbf{F}$ *is* ϵ*-almost XOR universal (*ϵ*-AXU), then* $\Pr\{\mathbf{F}(x) \oplus \mathbf{F}(x') = y\} \leq \epsilon$ *for all* $(x, x') \in \mathcal{X}^2$ *such that* $x \neq x'$ *and all* $y \in \mathcal{Y}$*.*

Can we substitute one of two PRFs (in DLPRP described above) with some WPRF and maintain the cipher's security? If the answer is yes, we can build a hybrid DLPRP using one invocation of a PRF and a WPRF, and a light-weight mixing round[9].

Unfortunately, the answer is not that clear. At least we found that, some special WPRF could be used as the last round function. The following theorem has a typical example.

Theorem 2. *Let* $\mathbf{G}$ *be* $\mathbf{E} \circ \mathbf{M}[\mathbf{F}_1, \mathbf{F}_2]$*, where* $\mathbf{E}$ *is a* $2n$*-bit RP and* $\mathbf{M}[\mathbf{F}_1, \mathbf{F}_2]$ *is a* 2*-round Feistel (see Ex. 1). Let* S_i *be the i-th input to* $\mathbf{F}_1$ *and let* a_i *be* $\mathrm{dist}(S^i)$*. Note that* S_i *is also the left half of the i-th output of* $\mathbf{E}$*. Let us assume that* $\mathbf{F}_2(x) = \mathbf{H}(\hat{x})$ *holds for all* x*, where* $\mathbf{H} : \{0,1\}^{n-1} \to \mathcal{X}$*, and* $\hat{x}$ *is the first* $n-1$ *bits of* x*. Then,* $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q, \tau)$ *is at most* $\mu(\mathbf{E}, \overline{a_q}) + \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}_1}(q, \tau) + \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{H}}(q, \tau) + q^2/2^n$*. If* $\mathbf{E}$ *is one right-to-left Feistel round with* ϵ*-AXU, then* $\mu(\mathbf{E}, \overline{a_q}) \leq \epsilon q^2/2$*.*

Proof. The proof is an extension of 3-round Feistel's proof. See Appendix B.

If $\mathbf{H}$ is a PRF, then $\mathbf{F}_2$ is obviously a WPRF, but not a PRF[10]. However, we could not find a way of evaluating the CPA-advantage of the cipher unless $\mathbf{F}_2$ was such a special WPRF (or a PRF). The reason is, roughly saying, that the information of S_i, which is a key to find a collision among S^{i+1}, may not be sufficiently hidden unless $\mathbf{F}_2$ is a PRF or a special WPRF described above. Moreover, the construction in Theorem 2 is not a hybrid one, but only a mode of two PRFs. For now, we think a general security proof based only on the CPA-advantage of $\mathbf{F}_1$ and KPA-advantage of $\mathbf{F}_2$ is intractable.

4.2 New Scheme Providing Hybrid DLPRP

Here, we propose a new block cipher scheme that slightly differs from Feistel.

Definition 11. *For an RP on* $\mathcal{X}$*,* $\mathbf{C}$*, and* $\mathbf{F} : \mathcal{X} \to \mathcal{X}^{m-1}$*, let* $\mathbf{N}_m[\mathbf{C}, \mathbf{F}]$ *be an RP on* $\mathcal{X}^m$ *defined as* $\mathbf{N}_m[\mathbf{C}, \mathbf{F}](x_l, x_r) = (\mathbf{C}(x_l), \mathbf{F}(\mathbf{C}(x_l)) \oplus x_r)$*, where* $x_l \in \mathcal{X}$ *and* $x_r \in \mathcal{X}^{m-1}$*.*

Here, $\mathbf{N}_m[\mathbf{C}, \mathbf{F}]$ is clearly invertible if $\mathbf{C}$ is invertible. Note that $\mathbf{N}_m[*, *]$ is unbalanced (i.e., a message is divided into two submessages of unequal lengths) for all $m > 2$. Let us say $\mathbf{N}_m[*, *]$ is $(n, (m-1)n)$ unbalanced. Now, let us show that the double length scheme, $\mathbf{N}_2[*, *]$, has quite a unique property: it provides an efficient hybrid DLPRP that accepts *any* WPRF. The first step in proving this is in analyzing an ideal setting (i.e., when $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$ is used).

[9] Building a DLPRP using two WPRF calls seems impossible, though we have not formally proved this so far.

[10] Interestingly, this kind of WPRF was proposed in Lucks's "Faster Luby-Rackoff Cipher" [14], although he only proved its non-adaptive CPA-security.

Theorem 3. *Let* $\mathbf{G}$ *be* $\mathbf{E}\circ\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$*, where* $\mathbf{E}$ *is an RP on* $\mathcal{X}^2$*. Let* S_i *denote the i-th input to* $\mathbf{P}_n$*, which corresponds to the left half of the i-th output of* $\mathbf{E}$*. We then obtain*

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q,\infty) \le \mu(\mathbf{E}, \overline{a_q}) + \frac{q^2}{2^{n+2}}, \quad \text{where } a_q \text{ denotes } \mathrm{dist}(S^q). \tag{4}$$

Moreover, if $\mathbf{E}$ *is one right-to-left Feistel round with* ϵ*-AXU,* $\mathbf{H}: \mathcal{X} \to \mathcal{X}$ *(see left of Fig. 1), then* $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q,\infty)$ *is at most* $\frac{q^2}{2}\left(\epsilon + \frac{1}{2^{n+1}}\right)$*.*

Proof. The core of the proof is in the following lemma. This is proved in Appendix C.

Lemma 4. *For any RF:*$\mathcal{X}^2 \to \mathcal{X}^2$*, let* (S_i, T_i) *be the i-th input, where* $S_i, T_i \in \mathcal{X}$*. Similarly,* (U_i, V_i) *denotes the i-th output, where* $U_i, V_i \in \mathcal{X}$*. For the case of* $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$*,* $U_i = \mathbf{P}_n(S_i)$ *and* $V_i = \mathbf{R}_{n,n}(\mathbf{P}_n(S_i)) \oplus T_i$*. Let* a_i *and* b_i *be* $\mathrm{dist}(S^i)$ *and* $\mathrm{dist}(U^i)$*, respectively. For two MESs,* $\mathcal{A} = a_0 a_1 \ldots$ *and* $\mathcal{B} = b_0 b_1 \ldots$*,*

$$\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \equiv \mathbf{P}_{2n}^{\mathcal{A}\wedge\mathcal{B}} \tag{5}$$

holds for some MES $\mathcal{C} = c_0 c_1 \ldots$ *defined for* $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$*.*

Let us abbreviate $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$ to $\mathbf{N}_2^*$. Using Lemmas 4 and 5, we obtain

$$(\mathbf{E}\circ\mathbf{N}_2^*)^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \equiv (\mathbf{E}\circ\mathbf{P}_{2n})^{\mathcal{A}\wedge\mathcal{B}}, \tag{6}$$

where MESs are defined for $\mathbf{N}_2^*$ and $\mathbf{P}_{2n}$ (see the left of Fig. 1). Let $\widehat{\mathbf{P}}_{2n}$ be a random system compatible to $\mathbf{P}_{2n}$, which always behaves as if some distinct inputs are given to $\mathbf{P}_{2n}$, no matter what the actual inputs are. We then have

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{E}\circ\mathbf{N}_2^*}(q,\infty) \le \nu(\mathbf{E}\circ\mathbf{P}_{2n}, \overline{a_q} \vee \overline{b_q}) \le \mu(\mathbf{E}, \overline{a_q}) + \mu(\widehat{\mathbf{P}}_{2n}, \overline{b_q}). \tag{7}$$

In Eq. (7), the first inequality follows from the equivalence $\mathbf{E}\circ\mathbf{P}_{2n} \equiv \mathbf{P}_{2n}$, and Lemma 4, and Theorem 6. For the last inequality, note that $\mathbf{P}_{2n}^{\mathcal{B}}|\mathcal{A} \equiv \widehat{\mathbf{P}}_{2n}^{\mathcal{B}}$ holds, since $\mathcal{A}$ indicates that inputs to $\mathbf{P}_{2n}$ are distinct and $\mathcal{B}$ is defined for outputs. Applying $\mathbf{P}_{2n}^{\mathcal{B}}|\mathcal{A} \equiv \widehat{\mathbf{P}}_{2n}^{\mathcal{B}}$ to Lemma 10 proves the last inequality. Let us analyze $\mu(\widehat{\mathbf{P}}_{2n}, \overline{b_q})$, which corresponds to the probability of a collision occurring in the left halves of $\widehat{\mathbf{P}}_{2n}$'s outputs. For any $i \ne j$, we obtain

$$\begin{aligned} P^{\widehat{\mathbf{P}}_{2n}}(U_i = U_j) &= \sum_{u, v_i, v_j \in \mathcal{X}, v_i \ne v_j} P^{\widehat{\mathbf{P}}_{2n}}(U_i = U_j = u, V_i = v_i, V_j = v_j) \\ &= \sum_{u, v_i, v_j \in \mathcal{X}, v_i \ne v_j} \frac{1}{2^{2n}} \cdot \frac{1}{2^{2n}-1} = 2^n \cdot \frac{2^n(2^n-1)}{2 \cdot 2^{2n} \cdot 2^{2n}-1} < \frac{1}{2^{n+1}}. \end{aligned}$$

This means $\mu(\widehat{\mathbf{P}}_{2n}, \overline{b_q})$ is less than $\binom{q}{2}\frac{1}{2^{n+1}} < \frac{q^2}{2^{n+2}}$. Substituting $\mu(\widehat{\mathbf{P}}_{2n}, \overline{b_q})$ with $\frac{q^2}{2^{n+2}}$ in Eq. (7) proves the first claim. As the proof of the second claim is easily derived by the first claim and a trivial collision analysis of $\mathbf{E}$, we omitted it.

The CPA-security of $\mathbf{E} \circ \mathbf{N}_2[\mathbf{C}, \mathbf{F}]$ is easy to prove, when both $\mathbf{C}$ and $\mathbf{F}$ are CPA-secure. Here, we will present a stronger result: we only need the KPA-security of $\mathbf{F}$ and CPA-security of $\mathbf{C}$.

Theorem 4. *Let $\mathbf{G} = \mathbf{E} \circ \mathbf{N}_2[\mathbf{C}, \mathbf{F}]$, where $\mathbf{E}$ is an RP on $\mathcal{X}^2$, $\mathbf{C}$ is an RP on $\mathcal{X}$, and $\mathbf{F} : \mathcal{X} \to \mathcal{X}$. Then,*

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q,\tau) \leq \mu(\mathbf{E}, \overline{a_q}) + \mathrm{Adv}^{\mathrm{prp}}_{\mathbf{C}}(q,\tau) + \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau') + \frac{5q^2}{2^{n+2}}, \qquad (8)$$

where a_q denotes an event where q inputs to $\mathbf{C}$ are distinct.

Proof. Using triangle inequality, $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q,\tau)$ is no more than $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G},\mathbf{G}'}(q,\tau) + \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G}',\mathbf{G}^*}(q,\tau) + \mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}^*}(q,\tau)$, where $\mathbf{G}'$ and $\mathbf{G}^*$ denote $\mathbf{E} \circ \mathbf{N}_2[\mathbf{P}_n, \mathbf{F}]$ and $\mathbf{E} \circ \mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$, respectively. Note that $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G}',\mathbf{G}^*}(q,\tau) \leq \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{P}_n \lhd \mathbf{F}, \mathbf{P}_n \lhd \mathbf{R}_{n,n}}(q,\tau)$ and thus we can use Lemma 1. This observation and Theorem 3 complete the proof.

As Theorem 4 shows, if $\mathbf{C}$ is a PRP and $\mathbf{F}$ is a WPRF, the cascade of lightweight mixing and $\mathbf{N}_2[\mathbf{C}, \mathbf{F}]$ is a DLPRP. Unlike a 3-round Feistel, no additional conditions are needed for $\mathbf{F}$.

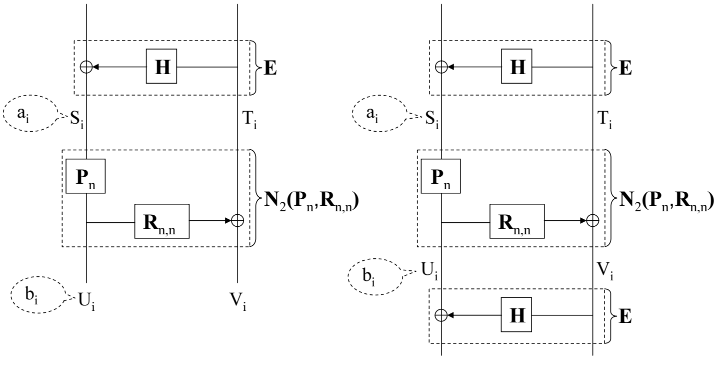

Fig. 1. Our Double Length PRP (left) and Double Length SPRP (right)

4.3 Achieving Large Block Size

One notable property of our scheme is that it offers a very efficient way of extending block size. We can use $\mathbf{N}_m[*, *]$ to build an mn-bit block cipher. Here, we need a WPRF:$\mathcal{X} \to \mathcal{X}^{m-1}$ for the second argument of $\mathbf{N}_m[*, *]$. Such an RF can be composed from any WPRF:$\mathcal{X} \to \mathcal{X}$, as shown in Lemma 3.

Corollary 2. *Let $\mathbf{C}$ be an RP on $\mathcal{X}$, and let $\mathbf{F}$ be an RF: $\mathcal{X} \to \mathcal{X}$. Moreover, let $\mathbf{E}$ be a right-to-left, $(n, (m-1)n)$ unbalanced Feistel round with ϵ-AXU. Then,*

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{E} \circ \mathbf{N}_m[\mathbf{C}, L_{\mathbf{F},m-1}]}(q,\tau) \leq \mathrm{Adv}^{\mathrm{prp}}_{\mathbf{C}}(q,\tau) + (m-1) \cdot \mathrm{Adv}^{\mathrm{wprf}}_{\mathbf{F}}(q,\tau') + q^2 \left(\frac{\epsilon}{2} + \frac{5}{2^{n+2}} \right).$$

Proof. The logic of the proof is the same as with DLPRP. Consider $\mathbf{E} \circ \mathbf{G}$, where $\mathbf{G}$ is an mn-bit RP. Assume S_i is the leftmost n-bit of the i-th input to $\mathbf{G}$, and U_i is the leftmost n-bit of the i-th output of $\mathbf{G}$. Let a_i and b_i denote $\mathrm{dist}(S^i)$ and $\mathrm{dist}(U^i)$. We can then prove that $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{E} \circ \mathbf{N}_m[\mathbf{P}_n, \mathbf{R}_{n,(m-1)n}]}(q, \infty)$ is at most $\mu(\mathbf{E}, \overline{a_q}) + q^2/2^{n+2}$ in almost the same way as with the proof of Theorem 3. From this and Theorem 4,

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{E} \circ \mathbf{N}_m[\mathbf{C}, L_{\mathbf{F},m-1}]}(q, \tau) \leq \mu(\mathbf{E}, \overline{a_q}) + \mathrm{Adv}^{\mathrm{prp}}_{\mathbf{C}}(q, \tau) + \mathrm{Adv}^{\mathrm{wprf}}_{L_{\mathbf{F},m-1}}(q, \tau') + \frac{5q^2}{2^{n+2}} \tag{9}$$

is obtained. Here, $\mu(\mathbf{E}, \overline{a_q}) \leq \epsilon q^2/2$ holds, if $\mathbf{E}$ is an unbalanced Feistel with ϵ-AXU. From this observation, and Eq. (9), and Lemma 3, Corollary 2 is proved.

To implement an efficient large block cipher with our scheme, the domain of ϵ-AXU needs to be easily expanded. Most practical AXUs have this property.

5 Hybrid Construction of SPRP

Similar to the 3-round Feistel, our hybrid PRP is completely vulnerable to CCA. However, small additions to our scheme can yield an SPRP. This is a very similar approach to that presented by Naor and Reingold [25]. Our SPRP construction is based on the following theorem.

Theorem 5. *Let* $\mathbf{Q}$ *be* $\mathbf{E}_1 \circ \mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}] \circ \mathbf{E}_2^{-1}$, *where* $\mathbf{E}_1$ *and* $\mathbf{E}_2$ *are independent RPs on* $\mathcal{X}^2$. *For any* $\mathbf{E}_1 \circ \mathbf{G} \circ \mathbf{E}_2^{-1}$, *where* $\mathbf{G}$ *is an RP on* $\mathcal{X}^2$, *let* (S_i, T_i) *be the i-th input to* $\mathbf{G}$. *Similarly, let* (U_i, V_i) *be the i-th output of* $\mathbf{G}$. *Let* a_i *and* b_i *denote* $\mathrm{dist}(S^i)$ *and* $\mathrm{dist}(U^i)$, *respectively. Then,*

$$\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{Q}}(q, \infty) \leq \mu(\mathbf{E}_1, \overline{a_q}) + \mu(\mathbf{E}_2, \overline{b_q}). \tag{10}$$

In addition, let $\mathbf{Q}'$ *be* $\mathbf{E} \circ \mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}] \circ \mathbf{E}$, *where* $\mathbf{E}$ *is a* $2n$*-bit right-to-left Feistel with* ϵ*-AXU,* $\mathbf{H} : \mathcal{X} \to \mathcal{X}$ *(see the right of Fig. 1). Then* $\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{Q}'}(q, \infty) \leq \epsilon q^2$.

Proof. See Appendix D.

As well as Sect. 4.3, Theorem 5 can easily be generalized to an mn-bit block size. In this case, the second argument of $\mathbf{N}_m[*, *]$ has to be a PRF:$\mathcal{X} \to \mathcal{X}^{m-1}$.

Corollary 3. *Let* $\mathbf{G}$ *be* $\mathbf{E} \circ \mathbf{N}_m[\mathbf{C}, \mathbf{F}] \circ \mathbf{E}$, *where* $\mathbf{E}$ *is an mn-bit right-to-left* $(n, (m-1)n)$ *unbalanced Feistel with* ϵ*-AXU,* $\mathbf{H} : \mathcal{X}^{m-1} \to \mathcal{X}$, *and* $\mathbf{C}$ *is an RP on* $\mathcal{X}$ *and* $\mathbf{F} : \mathcal{X} \to \mathcal{X}^{m-1}$. *Then,*

$$\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{G}}(q, \tau) \leq \mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{C}}(q, \tau) + \mathrm{Adv}^{\mathrm{prf}}_{\mathbf{F}}(q, \tau) + \epsilon q^2. \tag{11}$$

Proof. Let $\mathbf{Q}$ be $\mathbf{E} \circ \mathbf{N}_m[\mathbf{P}_n, \mathbf{R}_{n,(m-1)n}] \circ \mathbf{E}$. Then, $\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{Q}}(q, \infty) \leq \epsilon q^2$ can be proved in the same way as with the proof of Theorem 5, as we can use the same MESs as Theorem 5 (i.e., collisions in the leftmost n-bit of $\mathbf{N}_m[\mathbf{P}_n, \mathbf{R}_{n,(m-1)n}]$'s inputs and outputs). Corollary 3 follows from this and triangle inequality.

Suppose that an SPRP on $\mathcal{X}$, $\mathbf{C}$, and a WPRF, $\mathbf{F} : \mathcal{X} \to \mathcal{X}$, are available. Here, we first generate two independent versions of $\mathbf{C}$, $\mathbf{C}_1$ and $\mathbf{C}_2$, and build an mn-bit hybrid block cipher $\mathbf{E} \circ \mathbf{N}_m[\mathbf{C}_1, \mathrm{ARV}^{+}_{m-2}[\mathbf{C}_2, \mathbf{F}]] \circ \mathbf{E}$, where $\mathbf{E}$ is an $(n, (m-1)n)$ unbalanced Feistel with ϵ-AXU (see Fig. 2 in Appendix E). From Corollaries 1 and 3, this cipher is proved to be SPRP. It only requires two invocations of SPRP, $(m-2)$ invocations of WPRF, and two invocations of ϵ-AXU:$\mathcal{X}^{m-1} \to \mathcal{X}$ for any $m > 2$.

6 Summary

For comparison, we considered the NR mode [26]. It uses m invocations of an SPRP on $\mathcal{X}$ and two mixing layers on $\mathcal{X}^m$ to provide an mn-bit block SPRP. These mixing layers are composed of independent AXUs and slightly more complicated than ours. For $m > 2$, NR mode is very close to the best if an n-bit SPRP is the only cryptographic component available (and a fast AXU is available[11]), since it would be impossible to have an m-block pseudorandom output without using m SPRP invocations. Furthermore, it is easily verified that if one mixing layer is omitted from the NR mode, the resulting mode, which is denoted by the NR$^-$ mode, is a PRP, if the underlying component is a PRP. This is a highly optimized large block PRP construction based on small PRP and AXU.

Table 1. The number of component calls for hybrid and previous modes. All components are n-bit block, except for AXU. AXU$_{\alpha,\beta}$ denotes AXU: $\{0,1\}^\alpha \to \{0,1\}^\beta$.

DLPRP	PRP	WPRF	AXU$_{2n,n}$	others
Hybrid (left of Fig.1)	1	1	1	-
3-round Feistel	2	0	1	-
mn-bit PRP ($m > 2$)	PRP	WPRF	AXU$_{n(m-1),n}$	others
Hybrid (left of Fig.2)	1	$m-1$	1	-
NR$^-$ mode	m	0	1	some additional AXU calls
mn-bit SPRP ($m > 2$)	SPRP	WPRF	AXU$_{n(m-1),n}$	others
Hybrid (right of Fig.2)	2	$m-2$	2	-
NR mode	m	0	2	some additional AXU calls

As Table 1 shows, our hybrid modes performs quite well for both small and large blocks. In addition, they have comparable parallelism to that of the NR (or NR$^-$) mode, due to the high parallelism of $L_{\mathbf{F},m}$. The implementation cost of hybrid mode is naturally higher than that of the NR mode, but the additional cost would be small, or, at least smaller than the implemention cost of another PRF, since WPRF is a "cheaper" primitive than PRF.

Several options can be considered to implement our proposals. A promising approach is to combine the AES and a stream cipher that accepts IVs and is

[11] If a mode without AXU is desirable, EME or CMC modes [10, 11] are used.

faster than AES. For example, some stream ciphers proposed for the recent ECRYPT project [34] have this property. Such a stream cipher can be used as $\mathbf{F}$ in the $L_{\mathbf{F},t}$ construction. We can even use it directly as a substitute for $L_{\mathbf{F},t}$. In addition, we can save the implementation cost if the stream cipher is based on AES (an example of this is LEX [4]). Of course, we have to carefully check if our stream cipher is adequately secure. In this case, stream ciphers must be secure against attacks using many random IVs and corresponding (short) keystreams. These attacks are classified as a kind of resynchronization attack [5] and well-considered stream ciphers would be immune from them.

References

1. W. Aiello, S. Rajagopalan, and R. Venkatesan. “High-Speed Pseudorandom Number Generation with Small Memory.” *Fast Software Encryption*, FSE’99, LNCS 1636, pp. 290-304, 1999.
2. R. Anderson and E. Biham. “Two Practical and Provably Secure Block Ciphers: BEAR and LION.” *Fast Software Encryption*, FSE’96, LNCS 1039, pp. 113-120, 1996.
3. 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.
4. A. Biryukov. “New 128-bit Key Stream Cipher LEX.” *ECRYPT Stream Cipher Project Report*, available from `http://www.ecrypt.eu.org/stream/`
5. J. Daemen, R. Govaerts, J. Vandewalle. “Resynchronization Weaknesses in Synchronous Stream Ciphers.” *Advances in Cryptology*- EUROCRYPT’93, LNCS 765, pp. 159-167, 1993.
6. I. Damgård and J. Nielsen. “Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security.” *Advances in Cryptology*- CRYPTO’02, LNCS 2442, pp. 449-464, 2002.
7. O. Goldreich, S. Goldwasser, and S. Micali. “How to Construct Random Functions.” *Journal of the ACM*, Vol. 33, No. 4, pp. 792-807, 1986.
8. O. Goldreich. “Modern Cryptography, Probabilistic Proofs and Pseudorandomness.” *Springer.*
9. S. Halevi and H. Krawczyk. “MMH:Software Message Authentication in the Gbit/second rates.” *Fast Software Encryption*, FSE’97, LNCS 1267, pp. 172-189, 1997.
10. S. Halevi and P. Rogaway. “A Tweakable Enciphering Mode.” *Advances in Cryptology* - CRYPTO’03, LNCS 2729, pp. 482-499, 2003.
11. S. Halevi and P. Rogaway. “A Parallelizable Enciphering Mode.” *Topics in Cryptology*- CT-RSA’04, LNCS 2964, pp. 292-304, 2004.
12. T. Iwata and K. Kurosawa. “On the Universal Hash Functions in Luby-Rackoff Cipher.” *Information Security and Cryptology*- ICISC’02, pp. 226-236, LNCS 2587, 2003.
13. 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.
14. S. Lucks. “Faster Luby-Rackoff Ciphers.” *Fast Software Encryption*, FSE’96, LNCS 1039, pp. 189-203. 1996.
15. U. Maurer. “A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generators.” *Advances in Cryptology*- EUROCRYPT’92, pp. 239-255, 1992.

16. U. Maurer and J. L. Massey. "Cascade Ciphers: The Importance of Being First." *J. Cryptology* Vol. 6, num.1, pp. 55-61, 1993.
17. U. Maurer. "Indistinguishability of Random Systems." *Advances in Cryptology-* EUROCRYPT'02, LNCS 2332, pp. 110-132, 2002.
18. U. Maurer and K. Pietrzak. "Composition of Random Systems: When Two Weak Make One Strong." *Theory of Cryptography* - TCC'04, LNCS 2951, pp. 410-427, 2004.
19. M. Minier and H. Gilbert. "New Results on the Pseudorandomness of Some Blockcipher Constructions." *Fast Software Encryption*, FSE'01, LNCS 2355, pp. 248-266, 2002.
20. S. Moriai and S. Vaudenay. "On the Pseudorandomness of Top-Level Schemes of Block Ciphers." *Advances in Cryptology* - ASIACRYPT'00, LNCS 1976, pp. 289-302, 2000.
21. S. Myers. "Black-Box Composition Does Not Imply Adaptive Security." *Advances in Cryptology-* EUROCRYPT'04, LNCS 3027, pp. 189-206, 2004.
22. M. Naor and O. Reingold. "Number-theoretic Constructions of Efficient Pseudorandom Functions." 38 *th Annual Symposium on Foundations of Computer Science*, FOCS'97, pp. 458-467, 1997.
23. M. Naor and O. Reingold. "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs (Extended Abstract)." *Advances in Cryptology* - CRYPTO'98, LNCS 1462, pp. 267-282, 1998.
24. M. Naor and O. Reingold. "Synthesizers and their application to the parallel construction of pseudo-random functions." *J. of Computer and Systems Sciences*, Vol. 58 (2), pp. 336-375, 1999.
25. M. Naor and O. Reingold. "On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited." *Journal of Cryptology*, Vol. 12 (1), pp. 29-66, 1999.
26. M. Naor and O. Reingold. "The NR Mode of Operation." *Manuscript*, available from `http://www.wisdom.weizmann.ac.il/~naor/PAPERS/nr-mode.ps`
27. 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.
28. J. Patarin. "Security of Random Feistel Schemes with 5 or More Rounds." *Advances in Cryptology* - CRYPTO'04, LNCS 3152, pp. 106-122, 2004.
29. S. Vaudenay. "Feistel Ciphers with L_2-Decorrelation." *Selected Areas in Cryptography* - SAC'98, LNCS 1556, pp. 1-14, 1998.
30. S. Vaudenay. "Provable Security for Block Ciphers by Decorrelation." *15th Annual Symposium on Theoretical Aspects of Computer Science-* STACS '98, LNCS 1373, pp. 249-275, 1998.
31. S. Vaudenay. "Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness." *Selected Areas in Cryptography* - SAC'00, LNCS 1758, pp. 49-61, 2000.
32. 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.
33. Y. Zheng, T. Matsumoto, and H. Imai. "On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses." *Advances in Cryptology* - CRYPTO'89, LNCS 435, pp. 461-480, 1990.
34. ECRYPT Stream Cipher Project. `http://www.ecrypt.eu.org/stream/`
35. Security in Storage Working Group, An IEEE Information Assurance Activity. `http://www.siswg.org`

A Theorems and Lemmas Proved by Maurer [17]

Let us now describe some of Maurer's results [17]. They were used in our analysis.

Theorem 6. *(Theorem* 1 (i) *of [17]) Let $\mathcal{A}$ and $\mathcal{B}$ be MESs defined for* $\mathbf{F}$ *and* $\mathbf{G}$*. If* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$ *or* $\mathbf{F}|\mathcal{A} \equiv \mathbf{G}$*, then* $\mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{F},\mathbf{G}}(q,\infty) \le \nu(\mathbf{F},\overline{a_q})$*.*

Theorem 7. *(Theorem* 7 *of [17]) Let* $\mathbf{G}$ *be* $\mathbf{E}\circ\mathbf{M}[\mathbf{R}^{(1)},\mathbf{R}^{(2)}]$*, where* $\mathbf{E}$ *is an RP on* $\mathcal{X}^2$*,* $\mathbf{R}^{(1)}$ *and* $\mathbf{R}^{(2)}$ *are independent URFs:*$\mathcal{X} \to \mathcal{X}$*. Here,* $\mathbf{M}[*,*]$ *is a* $2n$*-bit* 2*-round Feistel, as described in Ex. 1. Let* a_q *denote an event where* q *inputs to* $\mathbf{R}^{(1)}$ *are distinct. Then* $\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q,\infty) \le \mu(\mathbf{E},\overline{a_q}) + \frac{q^2}{2^{n+1}}$*.*

Lemma 5. *(A corollary from Lemma* 4 (ii) *of [17]) Let* $\mathbf{F}$ *and* $\mathbf{G}$ *be two compatible RFs. If* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$ *for MESs* $\mathcal{A}$ *and* $\mathcal{B}$*, then* $(\mathbf{E}_1\circ\mathbf{F}\circ\mathbf{E}_2)^{\mathcal{A}} \equiv (\mathbf{E}_1\circ\mathbf{G}\circ\mathbf{E}_2)^{\mathcal{B}}$ *holds true, as long as* $(\mathbf{E}_1,\mathbf{E}_2)$ *is independent of* $\mathbf{F}$ *and* $\mathbf{G}$*. Here,* $\mathbf{E}_1$ *and* $\mathbf{E}_2$ *are not necessarily independent of each other.*

Lemma 6. *(Lemma* 1 (iv) *of [17]) Let MESs* $\mathcal{A}$ *and* $\mathcal{B}$ *be defined for* $\mathbf{F}$ *and* $\mathbf{G}$*. Moreover, let* X_i *and* Y_i *denote the i-th input and output of* $\mathbf{F}$ *(or* $\mathbf{G}$*), respectively. Assume* $\mathbf{F}|\mathcal{A} \equiv \mathbf{G}|\mathcal{B}$*. If* $P^{\mathbf{F}}_{a_i|X^iY^{i-1}a_{i-1}} \le P^{\mathbf{G}}_{b_i|X^iY^{i-1}b_{i-1}}$ *for* $i \ge 1$*, which means* $P^{\mathbf{F}}_{a_i|X^iY^{i-1}a_{i-1}}(x^i,y^{i-1}) \le P^{\mathbf{G}}_{b_i|X^iY^{i-1}b_{i-1}}(x^i,y^{i-1})$ *holds for all* (x^i,y^{i-1}) *such that* $P^{\mathbf{F}}_{a_{i-1}|X^{i-1}Y^{i-1}}(x^{i-1},y^{i-1})$ *and* $P^{\mathbf{G}}_{b_{i-1}|X^{i-1}Y^{i-1}}(x^{i-1},y^{i-1})$ *are positive, then there exists an MES* $\mathcal{C}$ *defined for* $\mathbf{G}$ *such that* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}\wedge\mathcal{C}}$*.*

Lemma 7. *(Lemma* 6 (ii) *of [17]) If* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$*, then* $\nu(\mathbf{F},\overline{a_q}) = \nu(\mathbf{G},\overline{b_q})$*.*

Lemma 8. *(Lemma* 6 (iii) *of [17])* $\nu(\mathbf{F},\overline{a_q}\vee\overline{b_q}) \le \nu(\mathbf{F},\overline{a_q}) + \nu(\mathbf{F},\overline{b_q})$ *if* $\mathcal{A}$ *and* $\mathcal{B}$ *are defined for* $\mathbf{F}$*.*

Lemma 9. *(Lemma* 10 (iii) *of [17]) For any two compatible RPs,* $\mathbf{F}$ *and* $\mathbf{G}$*,* $\mathbf{F}^{\mathcal{A}} \equiv \mathbf{G}^{\mathcal{B}}$ *implies* $\langle\mathbf{F}\rangle^{\mathcal{A}} \equiv \langle\mathbf{G}\rangle^{\mathcal{B}}$*.*

Lemma 10. *(Corollary* 1 (v) *of [17]) If* a_i *(*b_i*) is defined on the inputs (outputs) of* $\mathbf{F}$ *and* $\mathbf{F}^{\mathcal{B}}|\mathcal{A} \equiv \mathbf{U}^{\mathcal{B}}$ *for a source* $\mathbf{U}$ *compatible to* $\mathbf{F}$*, then* $\nu(\mathbf{E}\circ\mathbf{F},\overline{a_q}\vee\overline{b_q}) \le \mu(\mathbf{E},\overline{a_q}) + \mu(\mathbf{U},\overline{b_q})$ *for any* $\mathbf{E}$*. Here, a source is a random system that generates outputs that are independent of corresponding inputs.*

B Proof of Theorem 2

The proof of Theorem 2 is basically the same as the tight security proof of the 3-round Feistel demonstrated by Maurer (Theorem 7 of [17]). The only difference is in the definitions of MESs. Let $\widetilde{\mathbf{R}}_{n,n}$ be the RF:$\mathcal{X} \to \mathcal{X}$ defined as $\widetilde{\mathbf{R}}_{n,n}(x) = \mathbf{R}_{n-1,n}(\tilde{x})$, where $\tilde{x}$ denotes the first $n-1$ bits of x. First, we prove

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{E}\circ\mathbf{M}[\mathbf{R}_{n,n},\widetilde{\mathbf{R}}_{n,n}]}(q,\infty) \le \mu(\mathbf{E},\overline{a_q}) + \frac{q^2}{2^n}, \qquad (12)$$

where a_q denotes an event where q inputs to $\mathbf{R}_{n,n}$ (i.e., the left halves of $\mathbf{E}$'s outputs) are distinct. As well as Theorem 3, $\mu(\mathbf{E}, \overline{a_q})$ corresponds to the maximal probability of a collision occurring in the left halves of $\mathbf{E}$'s outputs, for all non-adaptive attackers.

For any RF:$\mathcal{X}^2 \to \mathcal{X}^2$, let (S_i, T_i) be the i-th input and let (U_i, V_i) be the i-th output, where $S_i, T_i, U_i, V_i \in \mathcal{X}$. Let a_i and b_i denote $\mathrm{dist}(S^i)$ and $\mathrm{dist}(\widetilde{V}^i)$, where $\widetilde{V}^i$ denotes $(\widetilde{V}_1, \ldots, \widetilde{V}_i)$ and $\widetilde{V}_i$ is the first $n-1$ bits of V_i. The first step is to show that

$$\mathbf{M}[\mathbf{R}_{n,n}, \widetilde{\mathbf{R}}_{n,n}]^{\mathcal{A}\wedge\mathcal{B}} \equiv \widehat{\mathbf{R}}^{\mathcal{A}\wedge\mathcal{B}}_{2n,2n} \equiv \mathbf{R}^{\mathcal{A}\wedge\mathcal{B}}_{2n,2n} \equiv \mathbf{P}^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}}_{2n} \tag{13}$$

holds for some MES $\mathcal{C}$ defined for $\mathbf{P}_{2n}$. Here, $\widehat{\mathbf{R}}_{2n,2n}$ behaves just like $\mathbf{R}_{2n,2n}$ taking some distinct inputs, independent of actual inputs (i.e., it always outputs uniformly random and independent values). Recall that $\widetilde{\mathbf{R}}_{n,n}$ behaves just like $\mathbf{R}_{n,n}$, as long as the first $n-1$ bits of the inputs do not include collisions. From this, we observe that

$$P^{\mathbf{M}[\mathbf{R}_{n,n},\widetilde{\mathbf{R}}_{n,n}]}_{U_iV_i|S^iT^iU^{i-1}V^{i-1}a_ib_i} \tag{14}$$

is a uniform distribution on $\mathcal{X} \times \tilde{\mathcal{X}}$, where $\tilde{\mathcal{X}}$ is a set of $v_i \in \mathcal{X}$ satisfying $\mathrm{dist}(\tilde{v}^i)$ (i.e., the first $n-1$ bits of v^i are unique). We thus have

$$\mathbf{M}[\mathbf{R}_{n,n}, \widetilde{\mathbf{R}}_{n,n}]|\mathcal{A}\wedge\mathcal{B} \equiv \widehat{\mathbf{R}}_{2n,2n}|\mathcal{A}\wedge\mathcal{B} \equiv \mathbf{R}_{2n,2n}|\mathcal{A}\wedge\mathcal{B}, \tag{15}$$

which immediately means

$$\mathbf{M}[\mathbf{R}_{n,n}, \widetilde{\mathbf{R}}_{n,n}]^{\mathcal{B}}|\mathcal{A} \equiv \widehat{\mathbf{R}}^{\mathcal{B}}_{2n,2n}|\mathcal{A} \equiv \mathbf{R}^{\mathcal{B}}_{2n,2n}|\mathcal{A}. \tag{16}$$

Using Eq. (16) and the fact that a_i is defined on the inputs, we obtain Eq. (13) except for the last equivalence. For the last equivalence, we observe that

$$P^{\mathbf{R}_{2n,2n}}_{a_ib_i|X^iY^{i-1}a_{i-1}b_{i-1}} \leq P^{\mathbf{P}_{2n}}_{a_ib_i|X^iY^{i-1}a_{i-1}b_{i-1}} \tag{17}$$

holds. The inequality above can easily be derived from the definitions of URF and URP. Applying Lemma 6 to Eq. (17), we obtain the last equivalence of Eq. (13).

Next, we apply Lemma 5 to Eq. (13). We then have

$$(\mathbf{E} \circ \mathbf{M}[\mathbf{R}_{n,n}, \widetilde{\mathbf{R}}_{n,n}])^{\mathcal{A}\wedge\mathcal{B}} \equiv (\mathbf{E} \circ \widehat{\mathbf{R}}_{2n,2n})^{\mathcal{A}\wedge\mathcal{B}} \equiv (\mathbf{E} \circ \mathbf{P}_{2n})^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \tag{18}$$

for some MES $\mathcal{C}$. Let $\mathbf{G}$ denote $\mathbf{E} \circ \mathbf{M}[\mathbf{R}_{n,n}, \widetilde{\mathbf{R}}_{n,n}]$. We now have

$$\mathrm{Adv}^{\mathrm{prp}}_{\mathbf{G}}(q, \infty) = \mathrm{Adv}^{\mathrm{cpa}}_{\mathbf{G},\mathbf{E}\circ\mathbf{P}_{2n}}(q, \infty) \leq \nu(\mathbf{G}, \overline{a_q} \vee \overline{b_q}) = \nu(\mathbf{E} \circ \widehat{\mathbf{R}}_{2n,2n}, \overline{a_q} \vee \overline{b_q}), \tag{19}$$

where the inequality follows from Eq. (18) and Theorem 6, and the last equality follows from Eq. (18) and Lemma 7. From Corollary 10, $\nu(\mathbf{E} \circ \widehat{\mathbf{R}}_{2n,2n}, \overline{a_q} \vee \overline{b_q}) \leq \mu(\mathbf{E}, \overline{a_q}) + \mu(\widehat{\mathbf{R}}_{2n,2n}, \overline{b_q})$ is obtained. Note that $\mu(\widehat{\mathbf{R}}_{2n,2n}, \overline{b_q})$ corresponds to the probability of a collision among q uniform random variables of length $n-1$ bits. Thus, $\mu(\mathbf{B}_{2n,2n}, \overline{b_q}) \leq \binom{q}{2}\frac{1}{2^{n-1}} < \frac{q^2}{2^n}$ holds, proving Eq. (12). Theorem 2 is proved using Eq. (12) and triangle inequality,

C Proof of Lemma 4

Let us abbreviate $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$ to $\mathbf{N}_2^*$. Recall that for any RF:$\mathcal{X}^2 \to \mathcal{X}^2$, (S_i, T_i) denotes the i-th input, where $S_i, T_i \in \mathcal{X}$. Similarly, (U_i, V_i) denotes the i-th output, where $U_i, V_i \in \mathcal{X}$. For example, if $\mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}]$ is considered, then $U_i = \mathbf{P}_n(S_i)$ and $V_i = \mathbf{R}_{n,n}(\mathbf{P}_n(S_i)) \oplus T_i$. We observe that a_i (i.e., $\text{dist}(S^i)$) and b_i (i.e., $\text{dist}(U^i)$) are equivalent events if $\mathbf{N}_2^*$ is considered, since $U_i = \mathbf{P}_n(S_i)$. Therefore, we have to prove that $\mathbf{N}_2^{*\mathcal{A}\wedge\mathcal{C}} \equiv \mathbf{P}_{2n}^{\mathcal{A}\wedge\mathcal{B}}$ holds for some MES $\mathcal{C}$. We first prove $\mathbf{N}_2^*|\mathcal{A} \equiv \mathbf{P}_{2n}|\mathcal{A} \wedge \mathcal{B}$. To prove this, we have to verify that

$$P^{\mathbf{N}_2^*}_{U_iV_i|U^{i-1}V^{i-1}S^iT^ia_i} = P^{\mathbf{P}_{2n}}_{U_iV_i|U^{i-1}V^{i-1}S^iT^ia_ib_i} \tag{20}$$

holds, where Eq. (20) means the both sides are equal as functions of (s^i, t^i, u^i, v^i) (see Def. 6 for example). Note that both sides of Eq. (20) are defined for all $S^i = s^i$ and $U^{i-1} = u^{i-1}$ such that $\text{dist}(s^i)$ and $\text{dist}(u^{i-1})$ hold. If u_i collides with u_j for some $1 \le j \le i-1$, then b_i does not hold. Therefore, both sides are 0 for such u_i (note that a_i is equivalent to b_i for $\mathbf{N}_2^*$). Otherwise b_i holds and so, the lhs of Eq. (20) is $1/((2^n - i + 1) \cdot 2^n)$ since U_i is uniformly distributed on $\mathcal{X} \setminus \{u_1, \dots, u_{i-1}\}$ and V_i is uniformly random on $\mathcal{X}$. Therefore, we have to verify if the rhs of Eq. (20) is $1/((2^n - i + 1) \cdot 2^n)$ in this case. Using simple decomposition, we have

$$P^{\mathbf{P}_{2n}}_{U_iV_i|U^{i-1}V^{i-1}S^iT^ia_ib_i} = \frac{P^{\mathbf{P}_{2n}}_{U^iV^i|S^iT^ia_ib_i}}{P^{\mathbf{P}_{2n}}_{U^{i-1}V^{i-1}|S^{i-1}T^{i-1}a_{i-1}b_{i-1}}}. \tag{21}$$

The numerator of the rhs of Eq. (21) is a uniform distribution on a set of all (u^i, v^i) that satisfies $\text{dist}(u^i)$. The number of such (u^i, v^i) is $(2^n \cdot (2^n - 1) \cdot \dots \cdot (2^n - i + 1)) \cdot (2^n)^i$. Similarly, the denominator is a uniform distribution on the set of size $(2^n \cdot (2^n - 1) \cdot \dots \cdot (2^n - i + 2)) \cdot (2^n)^{i-1}$. Thus the rhs of Eq. (21) equals

$$\left(\frac{(2^n \cdot (2^n - 1) \cdot \dots \cdot (2^n - i + 1)) \cdot (2^n)^i}{(2^n \cdot (2^n - 1) \cdot \dots \cdot (2^n - i + 2) \cdot (2^n)^{i-1}} \right)^{-1} = \frac{1}{(2^n - (i-1)) \cdot 2^n}. \tag{22}$$

Therefore, Eq. (20) holds true and hence we have $\mathbf{N}_2^*|\mathcal{A} \equiv \mathbf{P}_{2n}|\mathcal{A} \wedge \mathcal{B}$. To apply Lemma 6, we need to check if

$$P^{\mathbf{P}_{2n}}_{a_ib_i|U^{i-1}V^{i-1}S^iT^ia_{i-1}b_{i-1}} \le P^{\mathbf{N}_2^*}_{a_i|U^{i-1}V^{i-1}S^iT^ia_{i-1}} \tag{23}$$

holds true for all possible arguments $(u^{i-1}, v^{i-1}, s^i, t^i)$. When s^i does not satisfy a_i, clearly Eq. (23) holds, since both sides are 0. When s^i satisfies a_i, the rhs of Eq. (23) is 1. Thus, Eq. (23) is proved. Combining Eq. (23) and Lemma 6, we have $\mathbf{N}_2^{*\mathcal{A}\wedge\mathcal{C}} \equiv \mathbf{P}_{2n}^{\mathcal{A}\wedge\mathcal{B}}$ for some MES $\mathcal{C}$ defined for $\mathbf{N}_2^*$. Therefore, $\mathbf{N}_2^{*\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \equiv \mathbf{P}_{2n}^{\mathcal{A}\wedge\mathcal{B}}$ is proved.

D Proof of Theorem 5

Let $\mathbf{Q}^*$ be $\mathbf{E}_1 \circ \mathbf{P}_{2n} \circ \mathbf{E}_2^{-1}$ and let $\mathbf{Q}$ be $\mathbf{E}_1 \circ \mathbf{N}_2[\mathbf{P}_n, \mathbf{R}_{n,n}] \circ \mathbf{E}_2^{-1}$. From Lemmas 4 and 5,

$$\mathbf{Q}^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \equiv \mathbf{Q}^{*\mathcal{A}\wedge\mathcal{B}} \tag{24}$$

holds, where $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are the MESs appearing in Lemma 4. From Eq. (24) and Lemma 9, we obtain $\langle \mathbf{Q} \rangle^{\mathcal{A}\wedge\mathcal{B}\wedge\mathcal{C}} \equiv \langle \mathbf{Q}^* \rangle^{\mathcal{A}\wedge\mathcal{B}}$. This conditional equivalence and Theorem 6 indicate $\mathrm{Adv}^{\mathrm{cca}}_{\mathbf{Q},\mathbf{Q}^*}(q,\infty) \le \nu(\langle \mathbf{Q}^* \rangle, \overline{a_q} \vee \overline{b_q})$, which corresponds to the maximal probability of $\overline{a_q}$ (i.e., a collision in the left halves of inputs to $\mathbf{P}_{2n}$) or $\overline{b_q}$ (i.e., a collision in the left halves of $\mathbf{P}_{2n}$'s outputs) for all (q,∞)-CCAs . Therefore, we have

$$\mathrm{Adv}^{\mathrm{sprp}}_{\mathbf{Q}}(q,\infty) = \mathrm{Adv}^{\mathrm{cca}}_{\mathbf{Q},\mathbf{Q}^*}(q,\infty) \le \nu(\langle \mathbf{Q}^* \rangle, \overline{a_q} \vee \overline{b_q}) \le \nu(\langle \mathbf{Q}^* \rangle, \overline{a_q}) + \nu(\langle \mathbf{Q}^* \rangle, \overline{b_q}). \tag{25}$$

The first equality holds since $\mathbf{Q}^* \equiv \mathbf{P}_{2n}$, and the last inequality follows from Lemma 8.

We next analyze $\nu(\langle \mathbf{Q}^* \rangle, \overline{a_q})$. Let us use the following notations. The i-th input and output of $\mathbf{Q}^*$ are X_i and Y_i, respectively. In addition, let $\hat{X}_i$ denote (S_i, T_i) and $\hat{Y}_i$ denote (U_i, V_i). Note that $\hat{X}_i$ and $\hat{Y}_i$ correspond to the i-th input and output of $\mathbf{P}_{2n}$ in $\mathbf{Q}^*$. Observe that

$$\begin{aligned}\nu(\langle \mathbf{Q}^* \rangle, \overline{a_q}) &= \max_{\mathbf{D}:(q,\infty)\text{-CCA}} \sum_{x^q, y^q} P^{\mathbf{Q}^*}_{\overline{a_q}|X^qY^q}(x^q, y^q) \cdot P^{\mathbf{D}\diamond\langle \mathbf{Q}^* \rangle}_{X^qY^q}(x^q, y^q) \\ &\le \max_{x^q, y^q} P^{\mathbf{Q}^*}_{\overline{a_q}|X^qY^q}(x^q, y^q) \end{aligned} \tag{26}$$

holds, where $\mathbf{D} \diamond \langle \mathbf{Q}^* \rangle$ denotes an environment where $\mathbf{D}$ attacks $\mathbf{Q}^*$ by means of CCA, and the second maximum is taken over all x^q and y^q satisfying $\mathrm{dist}(x^q)$ and $\mathrm{dist}(y^q)$. Let $\beta_q \subset (\mathcal{X}^2)^q$ be the set of $\hat{x}^q = (s^q, t^q)$ such that a_q (i.e., $\mathrm{dist}(s^q)$) does not hold but $\mathrm{dist}(\hat{x}^q)$ holds. Now we have

$$P^{\mathbf{Q}^*}_{\overline{a_q}|X^qY^q}(x^q, y^q) = \frac{\sum_{\hat{x}^q \in \beta_q} P^{\mathbf{E}_1}_{\hat{X}^q|X^q}(\hat{x}^q, x^q) \cdot P^{\mathbf{Q}^*}_{Y^q|\hat{X}^qX^q}(y^q, \hat{x}^q, x^q)}{(\prod_{i=0}^{q-1} 2^{2n} - i)^{-1}}. \tag{27}$$

It is not difficult to verify that $P^{\mathbf{Q}^*}_{Y^q|\hat{X}^qX^q}(y^q, \hat{x}^q, x^q)$ equals to

$$\sum_{\hat{y}^q \in (\mathcal{X}^2)^q} P^{\mathbf{P}_{2n}}_{\hat{Y}^q|\hat{X}^qX^q}(\hat{y}^q, \hat{x}^q, x^q) \cdot P^{\mathbf{E}_2^{-1}}_{Y^q|\hat{Y}^q\hat{X}^qX^q}(y^q, \hat{x}^q, x^q) = \frac{1}{\prod_{i=0}^{q-1} 2^{2n} - i}. \tag{28}$$

The last equality results from the fact that $\mathbf{P}_{2n}$ is a URP and $\mathbf{E}_2$ is invertible. From Eqs. (27) and (28), we have $P^{\mathbf{Q}^*}_{\overline{a_q}|X^qY^q}(x^q, y^q) = \sum_{\hat{x}^q \in \beta_q} P^{\mathbf{E}_1}_{\hat{X}^q|X^q}(\hat{x}^q, x^q)$, which is at most $\mu(\mathbf{E}_1, \overline{a_q})$ (see Def. 8). Similarly, $\nu(\langle \mathbf{Q} \rangle, \overline{b_q})$ is no more than $\mu(\mathbf{E}_2, \overline{b_q})$. Thus, the first claim is proved. Note that the above proof is valid even if $\mathbf{E}_1$ and $\mathbf{E}_2$ are dependent. Combining this observation and the fact that one Feistel round, $\mathbf{E}$, is an involution (i.e., $\mathbf{E}^{-1} \equiv \mathbf{E}$), the second claim is proved.

E Figure of Hybrid Large Block PRP and SPRP

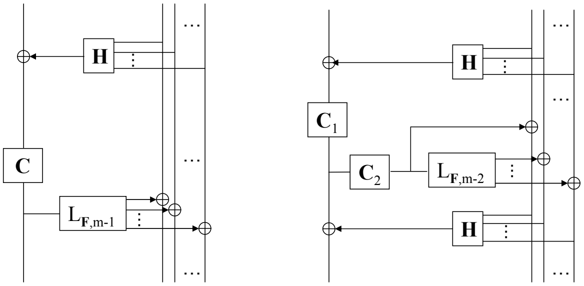

Fig. 2. Hybrid large block PRP (left) and SPRP (right)