The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants

Mridul Nandi

C.R. Rao AIMSCS Institute, Hyderabad*
mridul.nandi@gmail.com

Abstract. Luby and Rackoff provided a construction (LR) of $2n$-bit (strong) pseudorandom permutation or (S)PRP from n-bit pseudorandom function (PRF), which was motivated by the structure of DES. Their construction consists of four rounds of Feistel permutations (or three rounds, for PRP), each round involves an application of an independent PRF (i.e. with an independent round key). The definition of the LR construction can be extended by reusing round keys in a manner determined by a *key-assigning* function. So far several key-assigning functions had been analyzed (e.g. LR with 4-round keys K_1, K_2, K_2, K_2 was proved secure whereas K_1, K_2, K_2, K_1 is not secure). Even though we already know some key-assigning functions which give secure and insecure LR constructions, the exact characterization of all secure LR constructions for arbitrary number of rounds is still unknown. Some characterizations were being conjectured which were later shown to be wrong. In this paper we solve this long-standing open problem and (informally) prove the following:

> *LR is secure iff its key-assigning is* **not palindrome** (i.e. the order of key indices is not same with its reverse order).

We also study the class of LR-variants where some of its round functions can be tweaked (our previous characterization would not work for the variants). We propose a single-key LR-variant SPRP, denoted by LRv, making only four invocations of the PRF. It is exactly same as single-key, 4-round LR with an additional operation (e.g. rotation) applied to the first round PRF output. So far the most efficient single-key LR construction is due to Patarin, which requires five invocations. Moreover, we show a PRP-distinguishing attack on a wide class of single-key, LR-variants with three PRF-invocations. So,

> *4 invocations of PRF is minimum for a class of a single-key LR-variants SPRP and* LRv *is* **optimum** *in the class.*

Keywords: Luby-Rackoff, Feistel, PRP, SPRP, PRF, distinguisher, palindrome.

* A large part of the work has been done while working in The George Washington University.

G. Gong and K.C. Gupta (Eds.): INDOCRYPT 2010, LNCS 6498, pp. 82–97, 2010.

1 Introduction

Strong Pseudorandom permutations or SPRPs, which were introduced by Luby and Rackoff [4], formalize the well established cryptographic notion of block ciphers. They provided a construction of SPRP, well known as LR construction, which was motivated by the structure of DES [6]. The basic building block is the so called $2n$-bit *Feistel permutation* (or *LR round permutation*) LR_{F_K} based on an n-bit pseudorandom function (PRF) F_K:

$$\mathsf{LR}_{F_K}(x_1, x_2) = (F_K(x_1) \oplus x_2, x_1), \quad x_1, x_2 \in \{0,1\}^n.$$

Their construction consists (see Fig 1) of four rounds of Feistel permutations (or three rounds, for PRP), each round involves an application of an independent PRF (i.e. with independent random keys K_1, K_2, K_3, and K_4). More precisely, $\mathsf{LR}_{K_1,K_2,K_3}$ and $\mathsf{LR}_{K_1,K_2,K_3,K_4}$ are PRP and SPRP respectively where

$$\mathsf{LR}_{K_1,\ldots,K_r} := \mathsf{LR}_{F_{K_1},\ldots,F_{K_r}} := \mathsf{LR}_{F_{K_r}}(\ldots(\mathsf{LR}_{F_{K_1}}(\cdot))\ldots).$$

After this work, many results are known improving performance (reducing the number of invocations of F_K) [5] and reducing the key-sizes (i.e. reusing the round keys [7,8,10,12,11] or generate more keys from single key by using a PRF [2]). However there are some limitations. For example, we cannot use as few as single-key LR (unless we tweak the round permutation) or as few as two-round since they are not secure. Distinguishing attacks for some other LR constructions are also known [8]. We list some of the know related results (see Table 1). Here all keys $K_1, K_2, \ldots$ are independently chosen.

- $\mathsf{LR}_{K_1,K_2,K_3}$ is PRP but not SPRP. [4] and $\mathsf{LR}_{K_1,K_2,K_3,K_4}$ is SPRP. [4]
- $\mathsf{LR}_{K_1,K_2,K_2}$ is PRP. [14]
- $\mathsf{LR}_{K_1,K_2,K_1,K_2}, \mathsf{LR}_{K_1,K_2,K_2,K_2}, \mathsf{LR}_{K_1,K_2,K_1,K_1}$ and $\mathsf{LR}_{K_1,K_1,K_2,K_2}$ are SPRP. [8]

Our Contribution. In [11] author conjectured a necessary and sufficient condition for all secure LR constructions, which was later shown to be wrong [8]. So far we do not know any proven characterization. In this paper we solve it and prove the following theorem.

Theorem 1. Let F_K be a PRF, $K_1, \ldots, K_t$ be t independent keys and $\sigma = (\sigma_1, \ldots, \sigma_r)$ be an r-tuple with elements from $[1..t] := \{1, 2, \ldots t\}$, called a *key-assigning* function. The construction $\mathsf{LR}_{K_{\sigma_1},\ldots,K_{\sigma_r}}$ is (S)PRP if and only if σ is not palindrome[1] and $r \geq 3$ (or 4 respectively). As a corollary, any 4-round LR is SPRP if and only if it is PRP.

Due to the above result we now know that no single-key with any arbitrary round LR can be secure. However if one modifies the round permutation then secure single-key construction is possible. There are some known secure variants [8,11] among which the designs due to Patarin are most efficient. There are

[1] An r-tuple $\sigma = (\sigma_1, \ldots, \sigma_r)$ is called *palindrome* if $\sigma_i = \sigma_{r+1-i}$, $\forall i$.

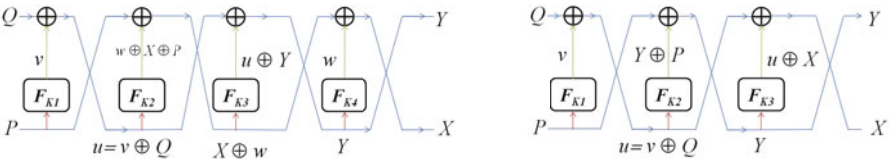

Fig. 1. The 4-round and 3-round LR constructions with independent round keys, i.e. K_1, K_2, K_3 and K_4 are chosen independently

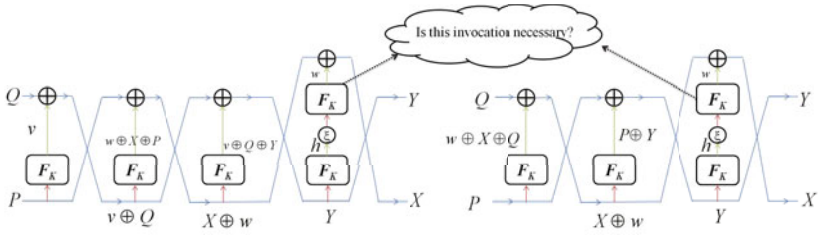

Fig. 2. 4-round (3-round for PRP) single-key LR-variant due to Patarin requires 5 (or 4) invocations of F_K. Here ξ is a simple function with low spreading number [8] e.g. one-bit rotation.

other efficient LR variants where k-wise independent universal hash function is required [5]. The SPRP design $\mathsf{LR}_{F_K \circ \xi \circ F_K}(\mathsf{LR}_{K,K,K}(\cdot))$ due to Patarin requires five invocations of the underlying PRF F_K (see Fig 2). This is almost same as 4-round single-key LR except the last round in which the composition function $F_K \circ \xi \circ F_K := F_K(\xi(F_K(\cdot)))$ is applied instead of F_K where ξ is a simple function, e.g. one-bit rotation. The similar construction is PRP for 3 rounds. The same result is true if we apply the tweak in the first round or use any ξ with small spreading number[2] [8]. In this paper we also prove the following results:

1. We first show that the PRF invocation in the tweak of 3-round Patarin construction (see right part of Fig 2) is essential. If we drop it then we have a PRP distinguishing attack. Moreover, this distinguishing attack works for many other choices of ξ (instead of rotation).
2. One may ask the same for the 4-round construction. Surprisingly, we show that the extra invocation of F_K in the tweak is redundant. In particular, $\mathsf{LR}_{K,K,K}(\mathsf{LR}_{\xi \circ F_K}(\cdot))$ is SPRP (see Fig 3).
3. Next we show that we cannot go below 4 invocations in a wide class of LR variants (with linear shuffle, defined the class and shuffle in Sec 5). In particular we show that any single-key, 3-round, Feistel encryption with linear shuffle is not PRP. So in that class, our construction is optimum. However,

[2] It is a parameter defined in [8]. Spreading of ξ is the $\max_{c \in \{0,1\}^n} \#\{x : x \oplus \xi(x) = c\}$.

we do not know the optimality when we have non-linear shuffle. This is an interesting open problem.

In summary, we prove the following result.

Theorem 2. $\mathsf{LR}_{K,K,K}(\mathsf{LR}_{\xi\circ F_K}(\cdot))$ is SPRP (see Fig 3) whenever F_K is PRF where ξ is one-bit rotation (or other simple function with low spreading number). Moreover, a single-key, 3-round LR-variant with any linear shuffle is not PRP.

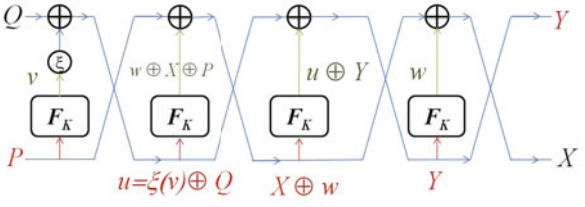

Fig. 3. Our 4-round single-key LR variant requires only 4 invocations of F_K. It is almost same as 4-round single-key LR except the rotation (or ξ) which is applied to the output of the first internal function.

Organization of the paper. We first describe notation and the proof tool, called Patarin's coefficient H-technique in Section 2. In section 3, we demonstrate our distinguishing attacks on LR and some of its variants. Then we characterize the secure LR construction in Section 4. In Section 5, we generalize LR variants and show that 3-round single-key general LR constructions are not secure. In section 6, we propose an optimum 4-round LR variant and prove its SPRP security and finally we conclude.

2 Notation and Preliminaries

A distinguishing adversary A is a probabilistic algorithm which has access to some oracles and which outputs either 0 or 1. Oracles are written as superscripts. The notation $A^{\mathcal{O}_1,\mathcal{O}_2} \Rightarrow 1$ (or $A^{\mathcal{O}} \Rightarrow 1$) denotes the event that the adversary A, interacts with the oracles $\mathcal{O}_1, \mathcal{O}_2$ (or $\mathcal{O}$), and finally outputs the bit 1. In what follows, by the notation $X \xleftarrow{\$} \mathcal{S}$, we will denote the event of choosing X uniformly at random from the finite set $\mathcal{S}$. Let RF_n be an n-bit to n-bit random function. An n-bit pseudorandom function (PRF) is a function $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, where $\mathcal{K} \neq \emptyset$ is the key space of the PRF such that the prf-advantage

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = \left|\Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{F_K} \Rightarrow 1\right] - \Pr\left[A^{\mathsf{RF}_n} \Rightarrow 1\right]\right|$$

is negligible for any efficient adversary A. We denote $\mathbf{Adv}_F^{\mathrm{prf}}(q)$ (or $\mathbf{Adv}_F^{\mathrm{prf}}(q,t)$) by $\max_A \mathbf{Adv}_E^{\mathrm{prf}}(A)$ where maximum is taken over all adversaries which makes at most q queries (and runs in time t respectively). We write $F_K(\,)$ instead of

$F(K,.)$. Let $\mathrm{Perm}(n)$ denote the set of all permutations on $\{0,1\}^n$. We require a blockcipher $E(K,)$, $K \in \mathcal{K}$, to be a strong pseudorandom permutation. The advantage of an adversary A in breaking the strong pseudorandomness of $E(,)$ is defined in the following manner.

$$\mathbf{Adv}_E^{\pm\mathrm{prp}}(A) = |\Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E_K(),E_K^{-1}()} \Rightarrow 1\right] -$$

$$\Pr\left[\pi \xleftarrow{\$} \mathrm{Perm}(n) : A^{\pi(),\pi^{-1}()} \Rightarrow 1\right]|.$$

If adversary has only access to encryption oracle $E(K,\cdot)$ then we call it prp-advantage $\mathbf{Adv}_E^{\mathrm{prp}}(A)$. Similar to prf-advantage we define $\mathbf{Adv}_E^{\pm\mathrm{prp}}(q)$ and $\mathbf{Adv}_E^{\pm\mathrm{prp}}(q,t)$ by $\max_A \mathbf{Adv}_{\mathbf{E}}^{\pm\mathrm{prp}}(A)$. Similar definition can be given for $\mathbf{Adv}_E^{\mathrm{prp}}(q)$ and $\mathbf{Adv}_E^{\mathrm{prp}}(q,t)$. In this paper we reserve q to mean the number of queries.

Pointless queries: Let M and C represent plaintext and ciphertext respectively. We assume that an adversary never repeats a query, i.e., it does not ask the encryption oracle with a particular value of M more than once and neither does it ask the decryption oracle with a particular value of C more than once. Furthermore, an adversary never queries its deciphering oracle with C if it got C in response to an encipher query M for some M and vice versa. These queries are called *pointless* as the adversary knows what it would get as responses for such queries. In this paper we assume adversaries make no pointless queries.

2.1 Patarin's Coefficient H-Technique

The following describes Patarin's coefficient H technique [9] (also known as Decorrelation theorem due to Vaudenay [13]) which would be used in our security analysis.

The view of an adversary $A^{\mathcal{O}_{+1},\mathcal{O}_{-1}}$ is the tuple $\psi := ((M_1,C_1,\delta_1), \ldots, (M_q,C_q,\delta_q))$ where A makes i^{th} query M_i or C_i and obtains responses C_i or M_i if $\delta_i = +1$ or -1 respectively. In case of $\mathcal{O}_{+1} = \mathcal{O}$ and $\mathcal{O}_{-1} = \mathcal{O}^{-1}$ we have that $\mathcal{O}(M_i) = C_i, \forall i$. Since A does not make any pointless query, all M_i (and C_i) are distinct.

Patarin's coefficient H technique says that prp-advantage of any distinguisher $A^{\mathcal{O}_{+1},\mathcal{O}_{-1}}$ making total q non-trivial queries to E is small if the followings hold for a subset $S \subseteq (\mathcal{M} \times \mathcal{M} \times \{+1,-1\})^q$ (the set S is known as set of **bad** views):

1. $\Pr[\mathsf{view}(A^{\mathsf{RP}_{\mathcal{M}},\mathsf{RP}_{\mathcal{M}}^{-1}}) \in S] \le \epsilon_1$ i.e. the probability of bad view is small.
2. For any $\psi := ((M_1,C_1,\delta_1),\ldots,(M_q,C_q,\delta_q)) \notin S$ (ψ is called a **good** or non-bad view),

$$\Pr_K[E(K,M_i) = C_i,\ \forall i] \ge \frac{(1-\epsilon_2)}{|\mathcal{M}|^q} = (1-\epsilon_2) \times \Pr[\mathsf{RF}(M_i) = C_i,\ \forall i].$$

So, each good view can occur with probability more than $(1-\epsilon_2)$ times the probability of the view for the random function RF. In other words, on

the average probability of good view are almost same for both $E(K,)$ and random function.

More precisely, if above holds then $\mathbf{Adv}^{\pm\mathrm{prp}}_{E}(A) \leq \epsilon_1 + \epsilon_2 + q(q-1)/2|\mathcal{M}|$. The third term arises from the well known fact [1] that $\mathbf{Adv}^{\pm\mathrm{prp}}_{\mathsf{RF}}(A') \leq \frac{q(q-1)}{2|\mathcal{M}|}$ for any A' making q non-trivial queries. Thus given any encryption algorithm $E(\cdot)$ it suffices to identify a set of bad views S and the values of ϵ_1 and ϵ_2 corresponding to the bad-views set.

3 Distinguishing Attack on Luby-Rackoff and Its Variants

Given $f : \{0,1\}^n \to \{0,1\}^n$, called *internal function*, the Luby-Rackoff (LR) round function (or the Feistel permutaion) $\mathsf{LR}_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is defined by $\mathsf{LR}_f(x_1, x_2) = (f(x_1) \oplus x_2, x_1)$ where $x_1, x_2 \in \{0,1\}^n$. Clearly, $\mathsf{LR}_f^{-1}(y_1, y_2) = (y_2, f(y_2) \oplus y_1)$ and hence we also call it LR round permutation. The r-round LR permutation is defined by the sequential composition of the r round permutations $\mathsf{LR}_{\mathbf{f}} := \mathsf{LR}_{f_r} \circ \ldots \circ \mathsf{LR}_{f_1}$ where $\mathbf{f} = (f_1, \ldots, f_r)$. If the internal functions are keyed functions, i.e. $f_i = F_{K_i}$, then we simply denote the r-round LR encryption by $\mathsf{LR}_{K_1,\ldots,K_r}$. Given a family of function-tuples $\mathcal{F}$, the induced family of LR permutations (or encryption with key $\mathbf{f} \xleftarrow{\$} \mathcal{F}$) is $\mathsf{LR}_{\mathcal{F}} = \{\mathsf{LR}_{\mathbf{f}} : \mathbf{f} \in \mathcal{F}\}$.

A *Key-assigning* is an r-tuple $\sigma = (i_1, \ldots, i_r)$ with elements from $[1..k]$. Now given a sequence of k function families $\mathcal{F} = \langle \mathcal{F}_1, \ldots \mathcal{F}_k \rangle$ we define the function-tuple family $\mathcal{F}^{\otimes\sigma} := \{(f_{i_1}, \ldots f_{i_r}) : f_j \in \mathcal{F}_j\}$. In practice, each function family is indexed by an independent key. The single-key (i.e. $k = 1$) r-round LR for a function family $\mathcal{F}$ is nothing but $\mathcal{F}^{\otimes 1^r}$. In case of k independent random functions $\Gamma = \langle \Gamma_1, \ldots, \Gamma_k \rangle$ mapping n-bits to n-bits, we have a random function tuple $\Gamma^{\otimes\sigma}$. It is easy to see that if σ is palindrome then $\mathcal{F}^{\otimes\sigma}$ is a family of palindrome function tuples. By using hybrid argument one can show that for any PRF F,

$$\mathbf{Adv}^{\pm\mathrm{prp}}_{\mathsf{LR}_{K_{\sigma_1},\ldots,K_{\sigma_r}}}(q) \leq \mathbf{Adv}^{\pm\mathrm{prp}}_{\mathsf{LR}_{\Gamma^{\otimes\sigma}}}(q) + \mathbf{Adv}^{\mathrm{prf}}_{F}(rq).$$

Because of it, we always assume random function instead of PRF. The Table 1 provides some known designs which are proved (or mentioned) secure.

Table 1. Some known secure, efficient LR designs and its variants. Let $\Gamma = (\Gamma_1, \Gamma_2)$ where Γ_1 and Γ_2 are independent random functions. $\sigma' = (1,2,2)$, $\sigma \in \{(1,2,2,2), (1,2,1,1), (1,2,1,2), (1,1,2,2)\}$. The author of [8] did not provide any proof, only mentioned that H technique can be applied to prove these SPRP. However in this paper we provide a general proof which covers the proof of these constructions.

Construction	$(\Gamma_1 \circ \xi \circ \Gamma_1, \Gamma_1, \Gamma_1)$	$(\Gamma_1 \circ \xi \circ \Gamma_1, \Gamma_1, \Gamma_1, \Gamma_1)$	$\Gamma^{\otimes\sigma}$	$\Gamma^{\otimes\sigma'}$
Security	PRP [8]	SPRP [8]	SPRP [8]	PRP [14]

3.1 Distinguishing Attack on Luby-Rackoff Encryptions with Palindrome Key-Assigning

Let $\mathsf{sw} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ be the swap-function i.e. $\mathsf{sw}(x_1, x_2) = (x_2, x_1)$. Note that for any function f and palindrome function-tuple $\mathbf{f} = (f_1, \ldots, f_r)$ we have $(\mathsf{LR}_f \circ \mathsf{sw} \circ \mathsf{LR}_f)(x_1, x_2) = \mathsf{LR}_f(x_1, f(x_1) \oplus x_2) = (x_2, x_1)$ and hence we have the following (see Fig 4)

$$\begin{aligned}\mathsf{LR}_{\mathbf{f}} \circ \mathsf{sw} \circ \mathsf{LR}_{\mathbf{f}} &= \mathsf{LR}_{f_1} \circ \ldots \circ (\mathsf{LR}_{f_r} \circ \mathsf{sw} \circ \mathsf{LR}_{f_r}) \circ \ldots \circ \mathsf{LR}_{f_1} \quad \text{(since } \mathbf{f} \text{ is palindrome)} \\ &= \mathsf{LR}_{f_1} \circ \ldots \circ (\mathsf{LR}_{f_{r-1}} \circ \mathsf{sw} \circ \mathsf{LR}_{f_{r-1}}) \circ \ldots \circ \mathsf{LR}_{f_1} \\ &= \ldots = \mathsf{LR}_{f_1} \circ \mathsf{sw} \circ \mathsf{LR}_{f_1} = \mathsf{sw}\end{aligned}$$

So, if $\mathcal{F}$ is any palindrome family then $\Pr_{\mathbf{f} \xleftarrow{\$} \mathcal{F}}[\mathsf{LR}_{\mathbf{f}} \circ \mathsf{sw} \circ \mathsf{LR}_{\mathbf{f}}(\mathbf{0}, \mathbf{0}) = (\mathbf{0}, \mathbf{0})] = 1$. So, $\mathsf{LR}_{\mathcal{F}}$ can be distinguished from the random permutation RP by making two adaptive queries $(Y_1, Y_2) := \mathcal{O}(\mathbf{0}, \mathbf{0})$ and $(Z_1, Z_2) := \mathcal{O}(Y_2, Y_1)$. The probability that $Z_1 = Z_2 = \mathbf{0}$ is one when $\mathcal{O} = \mathsf{LR}_{\mathcal{F}}$ (this also gives ciphertext-forging attack). When the distinguisher is interacting with RP, the probability is almost $1/2^{2n}$. Hence $\mathbf{Adv}^{\mathrm{prp}}_{\mathsf{LR}_{\Gamma \otimes \sigma}}(2, t) \geq 1 - 1/2^{2n}$. As a corollary single-key LR with any number of rounds is not PRP.

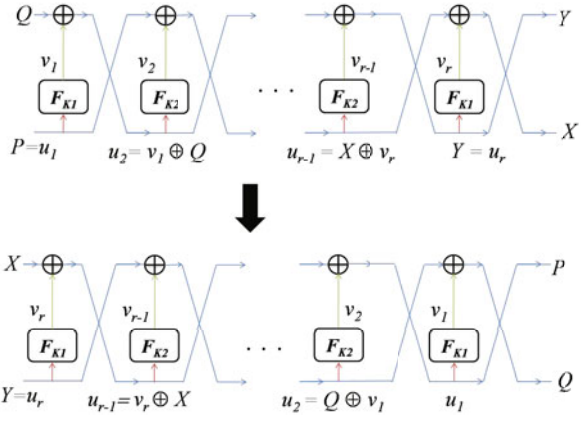

Fig. 4. It illustrates how the distinguishing attacks works for palindrome key-assigning

3.2 Distinguishing Attack on Some Variant of Single-Key 3-Round Luby-Rackoff Encryptions

From the previous section we now know that the any r-round single-key (or 3-round, double-key with key assigning $\sigma = \langle 1, 2, 1 \rangle$) LR is not PRP. The best known PRP, single-key LR variant is due to Patarin [8]. In this variant (see Fig 2) the last round (or the first round) internal function is defined as $f \circ \xi \circ f$ where ξ is the one-bit left rotation. As mentioned in Fig 2, we want to study whether we can simply use rotation tweak without using the extra invocation of f (to

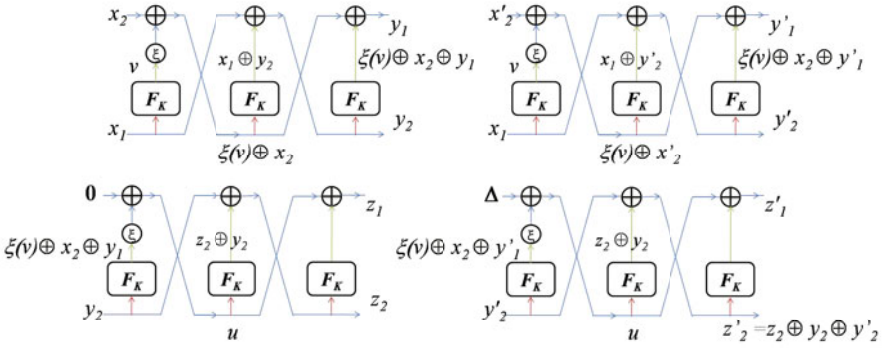

Fig. 5. It gives an idea how our 3-round LR variant (simpler version of Patarin's 3-round by dropping one invocation) distinguishing attack works. Here $u = v^{<<2} \oplus (x_2 \oplus y_1)^{<<1}$ and $\Delta = (x_2 \oplus x'_2 \oplus y_1 \oplus y'_1)^{<<1}$.

save one extra invocation of f). Here we show that we cannot do that for three round constructions. We provide a distinguishing attack where the rotation is applied to the first round instead of the last round. Same analysis would work for the last round, too. The function family of this modification can be described as $\mathcal{F}^{(2)} := \{(\xi \circ f, f, f) : f \in \mathcal{F}\}$. Our attack on $\mathsf{LR}_\xi := \mathsf{LR}_{\mathcal{F}^{(2)}}$ requires four encryption queries.

1. 1^{st} *and* 2^{nd} *Query*: (1) $\mathsf{LR}_\xi(x_1, x_2) = (y_1, y_2)$ and (2) $\mathsf{LR}_\xi(x_1, x'_2) = (y'_1, y'_2)$. Call this event by E_1 and let $\Delta = (x_2 \oplus x'_2 \oplus y_1 \oplus y'_1)^{<<1}$.

   Lemma 1. $\Pr_{f \xleftarrow{\$} \mathcal{F}}[f(x_1)^{<<1} \oplus f(y_2) = x_2 \oplus y_1 \mid E_1] = 1$

2. 3^{rd} *and* 4^{th} *Query*: (3) $\mathsf{LR}_\xi(y_2, \mathbf{0}) = (z_1, z_2)$ and (4) $\mathsf{LR}_\xi(y'_2, \Delta) = (z'_1, z'_2)$. Call this event by E_2.

   Lemma 2. $\Pr_{f \xleftarrow{\$} \mathcal{F}}[z_2 \oplus z'_2 = y_2 \oplus y'_2 \mid E_1, E_2] = 1$.

The above two lemmas are easy to verify from the Fig 5 and hence we skip the proofs. When distinguisher is interacting with $2n$-bit random permutations the probability $\Pr[z_2 \oplus z'_2 = y_2 \oplus y'_2 \mid E_1, E_2] \approx 1/2^{2n}$. So, we can use this event to make a distinguishing attack. Hence $\mathbf{Adv}^{\text{prp}}_{\mathsf{LR}_\xi}(4) \geq 1 - 1/2^{2n}$.

Remark 1. Similar attack can be carried out for the other simple variants, e.g. when $\xi(x) = \alpha \cdot x$ (the Galois field multiplication by the primitive element α) or any other linear function ξ (note that both rotation, or multiplication by a primitive element are linear over $GF(2)$ and $GF(2^n)$, respectively). In fact, with a closer look on the attack one can see that attack works for any function ξ such that $\Pr_{v \xleftarrow{\$} \{0,1\}^n}[\xi(\xi(v \oplus c_1)) \oplus \xi(\xi(v \oplus c_1)) = \Delta]$ is significantly high for some fixed constant Δ (depending on c_1 and c_2). Here the probability is computed over random choice of v. Note that this measurement is completely different from the spreading number considered in [8].

4 Security Analysis of LR with Non-palindrome Key-Assigning Function

Here we characterize all secure LR encryptions. Informally we prove that LR is secure if and only if the key-assigning is not palindrome. We have already seen the "only if" part which is more intuitive. However it is not obvious why non-palindrome key-assigning give a secure LR encryption. To understand the intuition let us first assume that $\sigma_1 \neq \sigma_r$, i.e. the first and last round keys are independent. Then the input to the first round function can be collided due to choices of plaintext (the first n-bit same as that of a previous plaintext). But we cannot control anymore collisions after that. It does not matter if we choose first n bits of plaintext same as the last n bits of the ciphertext as they are fed to independent random functions. The similar argument works when an attacker chooses a ciphertext. In general, for a non-palindrome σ, there must exist $r' < r/2 - 1$ such that $\sigma_i = \sigma_{r+1-i}$ for $i = 1, .., r'$ but $\sigma_i \neq \sigma_{r+1-i}$ for $i = r' + 1$. The similar argument would be applied to the random functions at rounds $r' + 1$ and $r - r'$. The random functions $\Gamma_{\sigma_{r'+1}}$ and $\Gamma_{\sigma_{r-r'}}$ at round $r' + 1$ and $r - r'$ are protecting a plaintext and ciphertext query respectively.

Theorem 1. *Let σ be an r-sequence. Then $\mathsf{LR}_{\Gamma^{\otimes\sigma}}$ is (S)PRP if and only if σ is not palindrome and $r \geq 3$ (or $r \geq 4$ respectively). In this case, $\mathbf{Adv}^{\mathrm{prp}}_{\mathsf{LR}_{\Gamma^{\otimes\sigma}}}(q,t)$ (or $\mathbf{Adv}^{\pm\mathrm{prp}}_{\mathsf{LR}_{\Gamma^{\otimes\sigma}}}(q,t)$ for SPRP) is at most $\frac{(1+r^2)q^2}{2^n-1} + \frac{q^2}{2^{2n}}$.*

Corollary 1. *Let $r \geq 4$. Then $\mathsf{LR}_{\Gamma^{\otimes\sigma}}$ is SPRP if it is PRP.*

The corollary is interesting as it says that any PRP LR for more than 4 round has to be SPRP. Note that it is not true for three rounds as we already know three round independent-keyed is PRP but not SPRP. This is a straightforward application of the theorem. We prove the theorem by using Patarin H-coefficient-technique as describe in Sec 2.1

Construction of the set of bad views S and computation of ϵ_1
For $1 \leq i \leq q$, we denote $M_i = (P_i, Q_i), C_i = (X_i, Y_i) \in \{0,1\}^n \times \{0,1\}^n$. We first define a set of bad views S (as we discuss in Patarin H coefficient technique). Given a view $\psi = ((M_1, C_1, \delta_1), \ldots, (M_q, C_q, \delta_q))$ we call P_j fresh if $P_j \neq P_i, Y_i, Y_j$ for all $i < j$. Similarly Y_j is fresh if $Y_j \neq P_i, Y_i, P_j$ for all $i < j$.

Definition 1. *A view $\psi = ((M_1, C_1, \delta_1), \ldots, (M_q, C_q, \delta_q)) \in (\{0,1\}^{2n} \times \{0,1\}^{2n} \times \{+1, -1\})^q$ is called* **bad** *if there is a j such that either P_j is not fresh and $\delta_j = -1$ or Y_j is not fresh and $\delta_j = 1$.*

Let S be the set of all bad views. Now we provide an upper bound of the probability that a view is bad when an adversary is interacting with a random permutation RP and its inverse RP^{-1}. We show that

$$\Pr[\mathrm{view}(A^{\mathsf{RP},\mathsf{RP}^{-1}}) \in S] \leq \epsilon_1 := \frac{q^2}{2^n - 1} \tag{1}$$

If the i^{th} query is encryption (i.e. $\delta_i = 1$) then $C_i = (X_i, Y_i)$ is uniformly distributed over a set of size at least $2^{2n} - i + 1$. Thus $\Pr[Y_i = c] \leq 1/(2^n - 1)$ for any constant $c \in \{0,1\}^n$ provided $q \leq 2^n$ (o.w. the equation is obviously true). Thus Y_i is one of P_j or Y_j or P_i has probability at most $2i - 1$. Similar result is true when $\delta_i = -1$. Thus a view is bad view, has probability at most $q^2/(2^n - 1)$. So we have proved the Eq. 1.

Some Notations and Properties of Good Views. We say that $M_i = (P_i, Q_i)$ is fresh if $M_i \neq \mathsf{sw}(C_j)$, $j < i$. Similarly we define a fresh C_i. Let $r \geq 4$ and σ be a non-palindrome sequence such that r' is the size of the common prefix of σ and σ^{rev}. Note that $r' \leq r/2 - 1$. Given a good (non-bad) view $\psi = ((M_1, C_1, \delta_1), \ldots, (M_q, C_q, \delta_q))$ we define the following sets of query-indices

$$N_{\psi,P} = \{i : P_i \text{ is fresh}\},\ N_{\psi,Y} = \{i : Y_i \text{ is fresh}\},$$

$$N_{\psi,M} = \{i : M_i \text{ is fresh}\},\ N_{\psi,C} = \{i : C_i \text{ is fresh}\}.$$

In the following, we state some lemmas whose proofs are straightforward and easy to verify.

Lemma 3. *For all i, $P_i \neq Y_i$. We also have $i \in N_{\psi,P}$ or $i \in N_{\psi,Y}$ if $\delta_i = -1$ or $+1$ respectively. Let $M_i = \mathsf{sw}(C_j)$, then $j \in N_{\psi,C}$ (i.e. C_j is fresh) or $j \in N_{\psi,M}$ (i.e. M_j is fresh) if $j < i$ or $i < j$ respectively.*

For each query number i, we define two sets of round numbers $I'_i \subseteq I_i \subseteq [1..r]$ as follows:

1. $\delta_i = 1$: We define $I_i := [1..r]$ or $[2..r]$ or $[r'+1..r]$ if P_i is fresh or M_i is fresh or M_i is not fresh, respectively. $I'_i = I_i \setminus \{r-1, r\}$ (note that $r \geq 3$).
2. $\delta_i = -1$: We define $I_i := [1..r]$ or $[1..r-1]$ or $[1..r-r']$ if Y_i is fresh or C_i is fresh or C_i is not fresh, respectively. We define $I'_i = I_i \setminus \{1, 2\}$.

Some Observations on LR. Now we state some useful and easy to verify properties of the r-round LR computations $\mathsf{LR}(P, Q) = (X, Y)$. Let $u[\ell], v[\ell]$ denote the input and output of the internal function at the ℓ^{th} round.

Lemma 4. *The ℓ^{th} intermediate input $u[\ell] = (v[\ell-1] \oplus v[\ell-3] \oplus \ldots v[\ell\%2 + 1]) \oplus R$ where $R = P$ or Q if ℓ is odd or even respectively.*

If $\ell \notin I_i \setminus \{1, r\}$ then either $\ell \leq r'$ or $r - \ell \leq r'$. Moreover there is a $j < i$ such $r - \ell \in I_j$. In that case $u_i[\ell] = u_j[r - \ell]$ and $v_i[\ell] = v_j[r - \ell]$ (similar proof can be made as we did for distinguishing attack on palindrome key-assigning).[3] Thus $u_i[\ell]$ (or $v_i[\ell]$) for $\ell \in I_i, i \in [1..q]$ (we denote it by u_I) together determine all intermediate inputs (or outputs respectively). This can be further extended to the following result.

[3] If r' or $r - r' \notin I_i$ (i.e either M_i or C_i is not fresh) then $u_i[\ell] = u_j[r - \ell]$ where $\ell = r' + 1$ or $r - r'$. However $\sigma_\ell \neq \sigma_{r-\ell}$ (by definition of r'). Hence independent random functions are applied to these same intermediate input.

Lemma 5. *$v_{I'} := \{v_i[\ell] : \ell \in I'_i, i \in [1..q]\}$ and ψ together determine all intermediate inputs and outputs.*

We denote the relation by the function $\mathcal{I}$, i.e. $\mathcal{I}(v_{I'}, \psi)$ is the tuple of all intermediate inputs. Now we see that if we choose $v_{I'}$ at random then the probability that all intermediate inputs in u_I are distinct is at least $(1-\epsilon_2)$ where $\epsilon_2 := r^2q^2/2^n$.

Proposition 1. *For any ℓ, ℓ' with $\sigma_\ell = \sigma_{\ell'}$, $\Pr_{v_{I'} \xleftarrow{\$}}[u_i[\ell] = u_j[\ell']] \le 1/2^n$ where $u_i[\ell]$ and $u_j[\ell']$ are determined from $\mathcal{I}(v_{I'})$ and $v_{I'}$ is chosen at uniform distribution.*

Proof. We prove it in different cases. If $\ell, \ell' \in \{1, r\}$ then the probability is zero because the view ψ is good. In fact, if one of these is either 1 or r then the probability is $1/2^n$ as that one is constant (determined by ψ not by $v_{I'}$) and the other one is non-trivial linear function of $v_{I'}$. For any $\ell \notin \{1, r\}$, $u_i[\ell]$ is indeed non-trivial linear function of $v_{I'}$. Now if we show that the linear functions are different for $u_i[\ell]$ and $u_j[\ell]$ then by randomness of $v_{I'}$ the above probability is $1/2^n$. Let $j < i$ and $\ell = r' + 1$ (if $M_i = \mathsf{sw}(C_{i'-1})$) or $r - r'$ (if $C_i = \mathsf{sw}(M_{i'-1})$). Then $u_i[\ell] = u_{i'}[r - \ell]$ and $r - \ell - 1 \in I'_i$. Hence $v_j[r - \ell - 1]$ contributes to $u_i[\ell]$. If $i' \neq j$ then we are done. Otherwise note that if $\ell' = r - \ell$ then $\sigma_\ell \neq \sigma_{\ell'}$. So $\ell' \neq r - \ell$ and hence by above lemma the two linear functions are indeed different. ∎

Proof of Theorem 1. We apply Patarin's coefficient H-technique. We already have defined the set of bad views S and we know $\epsilon_1 := q^2/(2^n - 1)$. Let E be the event that for all ℓ, ℓ' with $\sigma_\ell = \sigma_{\ell'}$, $u_i[\ell] \neq u_j[\ell']$ where $\ell \in I_i$ and $\ell' \in I_j$. By the Proposition 1, we know that $\Pr[E] \le \epsilon_2 := r^2q^2/2^n$ since there are at most r^2q^2 possible values of i, ℓ, j, ℓ'. So the number of possible $v_{I'}$ values such that $u_{I'}$ are all distinct is at least $2^{n|I'|}(1-\epsilon_2)$. Given any such $v_{I'}$ (which determines the rest of the intermediate outputs) the probability that these are indeed the intermediate outputs is exactly $2^{-n|I|} = 2^{-n(|I'|+2q)}$. This is true since $|I| = |I'| + 2q$ and there are $|I|$'s distinct inputs for the internal random functions which takes some specific given values v_I. Thus, for any fixed good view ψ, $\Pr[\text{view} = \psi] \ge (1-\epsilon_2)/2^{2nq}$ where $\epsilon_2 := r^2q^2/2^n$. Hence we have proved our theorem by applying the Patarin's H-technique as described in Sec 2.1.

5 General Feistel Round Permutation

The LR round permutation can be expressed as $\mathsf{LR}_f(x_1, x_2) = \rho(f(x_1), x_1, x_2)$ where $\rho(v, x_1, x_2) = (v \oplus x_2, x_1)$, $v, x_1, x_2 \in \{0,1\}^n = \mathbb{F}$. So $\rho : \mathbb{F}^3 \to \mathbb{F}^2$ is a linear function which can be characterized by the matrix $M = \binom{L_1}{L_2}$ where $L_1 = (1, 0, 1) \in \mathbb{F}^3$ and $L_2 = (0, 1, 0) \in \mathbb{F}^3$. A *general Feistel* function $\mathsf{F}_{f,\rho} : \{0,1\}^{2n} \to \{0,1\}^{2n}$ with the internal function f and mix function ρ is defined by $\mathsf{F}_{f,\rho}(X) = \rho(f(X[1..n]), X)$ (see Fig 6). In practice, the internal function f is a strong cryptographic object and the mix function is a simple (mostly using xor or rotation or at most modular addition) efficiently computable function. We do

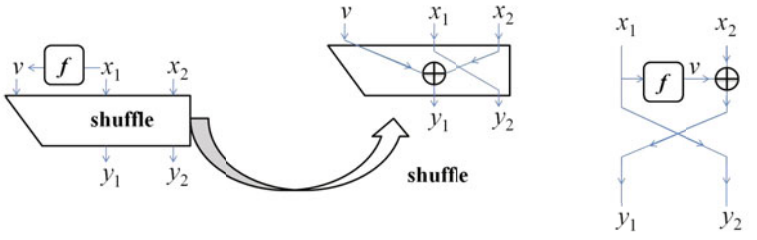

Fig. 6. A general LR or Feistel round permutation

not use or assume any cryptographic property on the mix function. However we require the Feistel function to be invertible (independent of the internal function) and hence we need some types of the mix function, called *shuffle*.

Definition 2 (Shuffle). *A function* $\rho : \{0,1\}^{3n} \to \{0,1\}^{2n}$ *is called* **shuffle** *if for any* $v \in \{0,1\}^n$, $\rho(v,\cdot,\cdot) := \rho_v$ *is a permutation over* $\{0,1\}^{2n}$ *and there exists a function* $\tau : \{0,1\}^{2n} \to \{0,1\}^n$ *such that* $\tau(\rho(v,x_1,x_2)) = x_1$, $\forall v, x_1, x_2 \in \{0,1\}^n$, *i.e. the function* $\rho_{v,1}^{-1}$ *is independent of* v *where* $\rho_v^{-1} = (\rho_{v,1}^{-1}, \rho_{v,2}^{-1})$. *Moreover it is called* **smooth** *if* ρ, ρ_v^{-1} *and* τ *are efficiently computable.*

Now we prove that (smooth) shuffle is the necessary and sufficient to have (efficiently computable) invertibility of the Feistel function.

Lemma 6. *The Feistel function* $\mathsf{F}_{f,\rho}$ *is permutation for all functions* f *if and only if the mix function* ρ *is shuffle. In this case,* $\mathsf{F}_{f,\rho}$ *and* $\mathsf{F}_{f,\rho}^{-1}$ *are efficiently computable if the shuffle* ρ *is smooth and the function* f *is efficiently computable.*

Proof. When ρ is a shuffle the inverse of the Feistel function can be shown to be $\mathsf{F}_{f,\rho}^{-1}(y_1,y_2) = \rho_v^{-1}(y_1,y_2)$ where $v = f(\tau(y_1,y_2))$. Hence $\mathsf{F}_{f,\rho}^{-1}$ is efficiently computable if f, τ, ρ_v^{-1} are efficiently computable. Clearly $\mathsf{F}_{f,\rho}$ is efficient if f and ρ are so. To prove the "only if" part it is easy to see that for all v, ρ_v must be invertible by choosing the constant internal function $f(x_1) = v, \forall x_1$. We show that the first n bit of the inverse does not depend on v. If not then for some v, v', $x_1 \neq x_1'$ and x_2, x_2' we have $\rho(v,x_1,x_2) = \rho(v',x_1',x_2')$. If we define a function f such that $f(x_1) = v$ and $f(x_1') = v'$ then the Feistel mapping is not injective as $\mathsf{F}_{f,\rho}(x_1,x_2) = \mathsf{F}_{f,\rho}(x_1',x_2')$. ■

The r-round Feistel function (or permutation when we have shuffle) $\mathsf{F}_{(f_r,\rho_r)} \circ \ldots \circ \mathsf{F}_{(f_1,\rho_1)}$ is similarly denoted by $\mathsf{F}_{\mathbf{f},\boldsymbol{\rho}}$ where $\mathbf{f} = (f_1,\ldots,f_r)$ and $\boldsymbol{\rho} = (\rho_1,\ldots,\rho_r)$.

In case of linear shuffle functions ρ_i's are characterized by 2×3 matrix over $GF(2^n)$. The Lemma 7 characterizes all linear shuffles. More generally when we have linear shuffle over $GF(2)$ we have $2n \times 3n$ matrix over $GF(2)$. However we can have non-linear shuffle functions too. One such example is $\rho(v,x_1,x_2) = (v \boxplus (v \oplus x_2), x_1)$ where $\boxplus$ is modulo 2^n integer addition. A more complicated shuffle function may look like $\rho(v,x_1,x_2) = (y_1 := \pi_{v,x_1}(x_2), \pi'_{y_1}(x_1))$ where π_{v,x_1} and π'_{y_1} are any permutations. In fact, it is a general form of a shuffle if

we assume that $\rho(v, x_1, \cdot)$ (equivalently $\tau(y_1, \cdot)$) is a permutation over $\{0,1\}^n$. This assumption is reasonable, otherwise we do not have complete diffusion in two rounds. In this paper we are only interested in linear shuffles. Now we state the version of Lemma 6 in case of linear shuffle. The proof is an immediate application of Lemma 6.

Lemma 7. *A linear function $M_{2\times 3}$ is shuffle if and only if*
(1) $c_1 \cdot M_{1*} \oplus c_2 \cdot M_{2*} = (0,1,0)$ for some pair of constants $(c_1, c_2) \in \mathbb{F}^2$ and
(2) $\mathsf{rank}(M_{*2}\ M_{*3}) = 2$, i.e. the 2×2 matrix $(M_{*2}\ M_{*3})$ is invertible.

5.1 PRP Attack on Three Round Linear-Mix Single-Key Feistel Function

Now we provide a PRP distinguishing attack on three-round single key Feistel function with any linear shuffles (may be different for each round). Let $\mathbf{f} = (f, f, f)$ and $\boldsymbol{\rho} = (\rho_1, \rho_2, \rho_3)$ be tuple of three linear shuffles. A very similar distinguishing attack as in Sec. 3 also works for $\mathsf{F} := \mathsf{F}_{\mathbf{f},\boldsymbol{\rho}}$. Our attack requires four encryption queries.

1. 1^{st} *and* 2^{nd} *Query*: (1) $\mathsf{F}(x_1, x_2) = (y_1, y_2)$ and (2) $\mathsf{F}(x_1, x_2') = (y_1', y_2')$. Call this event by E_1. Let $c_1 \cdot Y_1 \oplus c_2 \cdot Y_2 = \rho_3^{-1}(Y_1, Y_2)[1..n]$ since ρ_3 is linear shuffle.

   Lemma 8. *There is a constant Δ, a linear function of $x_1, x_2, x_2', y_1, y_2, y_1'$ and y_2', such that*

   $$\Pr_{f \xleftarrow{\$} \mathcal{F}}[\rho_1(f(\tau), \tau, \mathbf{0})[1..n] = \rho_1(f(\tau'), \tau', \Delta)[1..n] \mid E_1] = 1$$

   where $\tau = c_1 \cdot y_1 \oplus c_2 \cdot y_2$, and $\tau' = c_1 \cdot y_1' \oplus c_2 \cdot y_2'$.

2. 3^{rd} *and* 4^{th} *Query*: (3) $\mathsf{F}(\tau, \mathbf{0}) = (z_1, z_2)$ and (4) $\mathsf{F}(\tau', \Delta) = (z_1', z_2')$. Call this event by E_2.

   Lemma 9. *There is a constant Δ', a linear function of $x_1, x_2, x_2', y_1, y_2, y_1'$ and y_2', such that*

   $$\Pr_{f \xleftarrow{\$} \mathcal{F}}[c_1 \cdot (z_1 \oplus z_1') \oplus c_2 \cdot (z_2 \oplus z_2') = \Delta' \mid E_1, E_2] = 1$$

The above two lemmas are straightforward and tedious (the main thing is to compute Δ and Δ'). The idea of the proof is provided in the Figure 7. When distinguisher is interacting with $2n$-bit random permutations the above probability approximately $1/2^{2n}$. So we can use this event to make a distinguishing attack. So, at least four invocations of the underlying PRF are required to obtain a secure Feistel encryption.

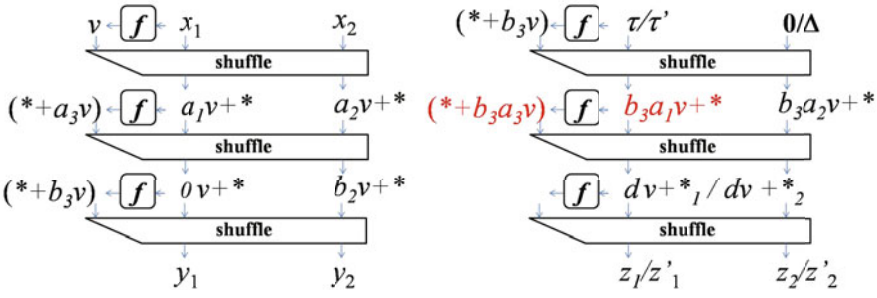

Fig. 7. It gives an idea how our attack works for 3-round Feistel with linear shuffle. The * denotes a linear function without involving v. We can express all internal variable by linear functions of v. The $\Delta' = *_1 - *_2$ and Δ is defined in a way such that the second internal inputs (for the queries $(\tau, \mathbf{0})$ and τ', Δ) in the right half of the figure match. This can be done as the second input has non-zero coefficient in the first output and the coefficient of v (only unknown variable) are same for both queries.

6 SPRP Security Analysis of Single-Key 4-Round Feistel Function

In this section we first study the following simple variant of 4-round single-key LR. Let ρ be the LR shuffle and $\rho'(v, x_1, x_2) = (\xi(v) \oplus x_2, x_1)$ where $\xi(v) := v^{<<1}$ is one-bit left rotation. Let $\mathsf{LRv} = \mathsf{F}_{\mathcal{F}^{\otimes 1^4}, \boldsymbol{\rho}}$ where $\boldsymbol{\rho} = (\rho', \rho, \rho, \rho)$. A similar security analysis would work for any function ξ with low spreading number, i.e. $\Pr_{v \xleftarrow{\$}}[\xi(v) \oplus v = c]$ is small for all c. We illustrated our design in Fig 3. In this section, we prove the SPRP security of this. In other words, we would that the Patarin's single-key SPRP LR-variant is not optimum and one invocation of PRF is completely of redundant. We follow the similar notation as in the proof of Theorem 1. In fact, the main idea of the proof remain same.

Let $f_K(P_i) = V_i$ and $f_K(Y_i) = W_i$. The four intermediate inputs of f_K during the computation $\mathsf{LR}'_{f^4}(P_i, Q_i) = (X_i, Y_i)$ are

$$P_i,\ a_i := V_i^{<<1} \oplus Q_i,\quad b_i := X_i \oplus W_i,\quad \text{and } Y_i.$$

We want to prove that except the forced collisions (due to the choice of plaintexts or ciphertexts) all intermediate inputs are distinct with high probability given that a view is good or non-bad (the same definition of bad views as we have for Theorem 1). We have defined $N_{\psi,P}$ and $N_{\psi,Y}$. Given a good view ψ, let the pair $(\mathbf{v}, \mathbf{w})$ be called ψ-compatible if $v_i = v_j$ (or w_j) whenever $P_i = P_j$ or Y_j and $w_i = w_j$ whenever $Y_i = Y_j$ where $\mathbf{v} = (v_1, \ldots, v_q)$ and $\mathbf{w} = (w_1, \ldots, w_q)$. Let N denote the number of distinct P_i's and Y_i's (which are actually intermediate inputs).

Lemma 10. *Given a good view the number of ψ-compatible pairs is 2^{nN}. Among which there are at least $2^{nN}(1 - 13q^2/2^n)$ compatible elements give distinct $a_i :=$*

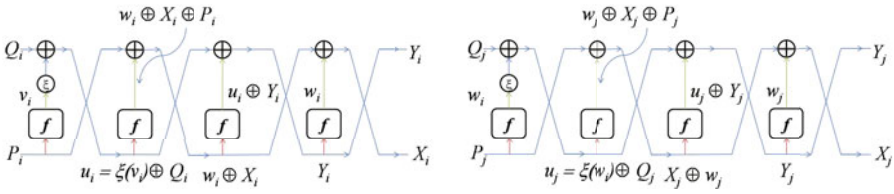

Fig. 8. Case: $\delta_j = +1$, $P_j = Y_i$ and $i < j$

$v_i^{<<1} \oplus Q_i, b_i = X_i \oplus w_i$, *for all* $1 \le i \le q$ *and they are different from* P_j*'s and* Y_j*'s for all* $1 \le j \le q$. *We call these* DI-compatible *(distinct-input compatible).*

Proof. We compute the probability of the complement event when we choose compatible pairs at random. We consider the case when $\delta_j = +1$ (i.e. an encryption query) and $P_j = Y_i$, $i < j$ (illustrated in Figure 8). In this case, the four intermediate inputs for i^{th} query are $P_i, Y_i, a_i = \xi(v_i) \oplus Q_i$ and $b_i = w_i \oplus X_i$. Since $P_j = Y_i$, the four intermediate inputs for j^{th} query are $P_j, Y_j, a_j = \xi(w_i) \oplus Q_j$ and $b_i = w_j \oplus X_j$. Note that v_i, w_i and w_j are chosen at random. Hence $(\mathbf{v}, \mathbf{w})$ is not DI-compatible due to the i^{th} and j^{th} query has probability at most $13/2^n$. In particular, except the case for $b_i = a_j$, the probability is $1/2^n$ and there are 11 such possible collisions. The $\Pr[b_i = a_j] = \Pr[w_i \oplus \xi(w_i) = c] = 1/2^{n-1}$ (it can be easily checked and was shown in [8]) where $c = X_i \oplus Q_j$. The other cases can be proved similarly. Since there are $\binom{q}{2}$ pair of queries and for each pair the probability is bounded by $13/2^n$, we have proved that probability that a random compatible pair is DI-compatible is at least $(1 - 13/2^n)$. ∎

If a DI-compatible pair becomes all intermediate outputs then the all intermediate inputs are determined by these. Moreover these intermediate inputs are distinct. There are $N + 2q$ distinct intermediate inputs (including P_i's and Y_i's). Hence probability that the intermediate outputs are given by a specific DI-compatible pairs is exactly $2^{-n(N+2q)}$. So we have proved that

$$\Pr[\text{view} = \psi] \ge 2^{nN}(1 - 13q^2/2^n) \times 2^{-n(N+2q)} = \frac{1 - 13q^2/2^n}{2^{2nq}}.$$

Hence we have proved the SPRP-security of our proposal LRv.

Theorem 2. $\mathbf{Adv}^{\pm\text{prp}}_{\mathsf{LRv}}(q,t) \le \frac{14q^2}{2^n - 1} + \frac{q^2}{2^{2n}}$.

7 Conclusion

This paper characterizes all secure LR constructions. So we know which LR are secure and which are not. If we make simple tweak in the LR-round then we can have secure single-key construction. Previously proposed tweak due to Patarin costs an extra invocation. In this paper we show that this extra invocation is

redundant in case of SPRP design (4-round) but completely necessary in case of PRP design (3-round). We also provide a distinguishing attack on a wide class of single-key LR variants which invoke the underlying internal function 3 times. So 4-invocations is necessary for single-key LR type designs. Hence our proposed design is optimum. However we do not know yet whether there are any non-linear shuffles such that single-key Feistel with three rounds is SPRP.

Acknowledgement. This work was supported in part by the National Science Foundation, Grant CNS-0937267. Author would like to thank Donghoon Chang for his comments.

References

1. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (2003)
2. Iwata, T., Kurosawa, K.: How to Re-use Round Function in Super-Pseudorandom Permutation. Information Security and Privacy, 224–235 (2004)
3. Koren, T.: On the construction of pseudorandom block ciphers, M.Sc. Thesis (in Hebrew), CS Dept., Technion, Israel (May 1989)
4. Luby, M., Rackoff, C.: How to construct pseudorandom permutations and pseudorandom functions. 2nd SIAM J. Comput. 17, 373–386 (1988)
5. Naor, M., Reingold, O.: On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. J. Cryptology 12(1), 29–66 (1999)
6. National Bureau of Standards, Data encryption standard, Federal Information Processing Standard, PT U.S. Department of Commerce, FIPS PUB 46, Washington, DC (1977)
7. Patarin, J.: Pseudorandom permutations based on the DES scheme. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, Springer, Heidelberg (1991)
8. Patarin, J.: How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom pseudorandom function. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 256–266. Springer, Heidelberg (1993)
9. Patarin, J.: The "Coefficients H" Technique. Selected Areas in Cryptography 2008, 328–345 (2008)
10. Pieprzyk, J.: How to construct pseudorandom permutations from single pseudorandom functions. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 140–150. Springer, Heidelberg (1991)
11. Sadeghiyan, B., Pieprzyk, J.: On necessary and sufficient conditions for the construction of super pseudorandom permutations. In: Matsumoto, T., Imai, H., Rivest, R.L. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 194–209. Springer, Heidelberg (1993)
12. Sadeghiyan, B., Pieprzyk, J.: A construction for super pseudorandom permutations from a single pseudorandom function. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, Springer, Heidelberg (1992)
13. Vaudenay, S.: Decorrelation: A Theory for Block Cipher Security. J. Cryptology 16(4), 249–286 (2003)
14. Zheng, Y., Matsumoto, T., Imai, H.: Impossibility and optimally results on constructing pseudorandom permutations. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 412–422. Springer, Heidelberg (1990)