# Lai-Massey Scheme and Quasi-Feistel Networks (Extended Abstract)

Aaram Yun[1], Je Hong Park[2], and Jooyoung Lee[2]

[1] University of Minnesota - Twin Cities
aaramyun@gmail.com
[2] ETRI Network & Communication Security Division, Korea
{jhpark,jlee05}@etri.re.kr

**Abstract.** We introduce the notion of quasi-Feistel network, which is generalization of the Feistel network, and contains the Lai-Massey scheme as an instance. We show that some of the works on the Feistel network, including the works of Luby-Rackoff, Patarin, Naor-Reingold and Piret, can be naturally extended to our setting. This gives a new proof for theorems of Vaudenay on the security of the Lai-Massey scheme, and also introduces for Lai-Massey a new construction of pseudorandom permutation, analoguous to the construction of Naor-Reingold using pairwise independent permutations.
Also, we prove the birthday security of $(2b-1)$- and $(3b-2)$-round unbalanced quasi-Feistel networks with $b$ branches against CPA and CPCA attacks, respectively. This answers an unsolved problem pointed out by Patarin et al.

**Keywords** Lai-Massey scheme, Feistel network, Luby-Rackoff, block cipher design, pseudorandom function, indistinguishability

## 1 Introduction

### 1.1 Feistel and Lai-Massey

Block cipher is one of the most important primitives of the symmetric-key cryptography. There are many proposed designs, and many important cryptanalytic results, including differential cryptanalysis and linear cryptanalysis. Also some heuristic, but powerful methodologies for giving strength against these attacks are proposed and studied.

Practically, DES, which was a United States federal standard block cipher, was widely used for a long time, until Rijndael replaced it as the new standard block cipher AES. Despite the wide usage, and some heuristic arguments of security against a few concrete attacks, still there was no rigorous proof of security for these practical and popular block ciphers.

The pioneering work of Luby and Rackoff [4] can be considered as a partial remedy for such a situation. They studied the security of Feistel cipher, when the round functions are independent random functions. When the size of the block is $n$, and when the adversary is restricted to ask $q$ queries, they showed that, when $q \ll 2^{n/2}$, 3-round Feistel cipher is secure against adaptive chosen plaintext attacks (CPA), and 4-round Feistel cipher is secure against adaptive chosen plaintext and ciphertext attacks (CPCA), even if the adversary is unconditionally powerful in its computational power.

In theoretical cryptography, the result of Luby and Rackoff implies that pseudorandom permutations exist, if one-way functions exist. In more practical vein, it gives a partial validation for the design of Feistel ciphers, for example, DES. Of course, the security of Feistel

cipher in Luby-Rackoff model does not imply the security for any specific, concrete Feistel ciphers. But the work of Luby and Rackoff shows at least the generic, structural strength of the basic Feistel design.

The seminal work of Luby and Rackoff was extended in many ways by various cryptographers. Roughly, these could be classified into the following three categories:

1. Improving the bound: most results on the Luby-Rackoff model considers adversaries within the birthday bound. However, in a series of papers [6–8, 10, 12–14], Patarin extended the work of Luby and Rackoff beyond the birthday bound.
2. Simplifying the construction: instead of $r$ independent random functions for $r$-round Feistel cipher, some authors studied constructions where only one or two random functions are used, for example in [9]. Also, Naor and Reingold showed how to simplify the construction by using pairwise-independent permutations [5].
3. Exploring other structures: instead of the Feistel network, other structures like MISTY and Lai-Massey were also studied in the Luby-Rackoff model.

Our goal in this paper is to revisit works belonging to the second and the third of the above categories.

Our starting point is the Lai-Massey scheme. The design of the Lai-Massey scheme has two interesting aspects.

- Not so much group theoretic: while the Feistel network, or the MISTY structure is based on a finite abelian group, the Lai-Massey scheme is different. Of course, the structure is defined in terms of a finite abelian group. But in order to obtain security in the Luby-Rackoff model, a mapping called orthomorphism is needed. An orthomorphism is defined for a finite abelian group, but the dependence is only very loose. For example, one may say that a *homomorphism* is strongly tied to the underlying group, but an orthomorphism is not.
  Hence, we have at least one structure which is not group-based, but where a security proof in the Luby-Rackoff model is possible.
- As secure as Feistel: it looks like a coincidence, but the known security of the Lai-Massey scheme is exactly the same as that of the Feistel network, despite the difference in the structure. Vaudenay proved that, within the birthday bound, 3-round Lai-Massey scheme is CPA-secure, and 4-round Lai-Massey scheme is CPCA-secure [20]. This security level is precisely that of the Feistel network studied by Luby and Rackoff.
  This is in contrast to the MISTY structure, where 3-round MISTY structure is not CPA-secure, and 4-round MISTY structure is not CPCA-secure. In case of MISTY, 4-round structure is CPA-secure, and 5-round is CPCA-secure.

### 1.2 Our contribution

In this paper, we show that the above two aspects of the Lai-Massey scheme are not coincident. We introduce the notion of *quasi-Feistel network*, which is a natural generalization of the Feistel network, based on finite quasigroups. We show that this notion contains the original Feistel network and also the Lai-Massey scheme, and we show that many of the works done on the Feistel network can be extended naturally to the quasi-Feistel network. Specifically,

1. We show that the original work of Luby and Rackoff [4] can be extended to quasi-Feistel network; in fact, we generalize this result further to unbalanced cases, and we prove that $(2b-1)$-round $b$-branched unbalanced (contracting) quasi-Feistel network is CPA-secure within the birthday bound, and $(3b-2)$-round is CPCA-secure within the birthday bound.
2. We show that various results on the 3- or 4-round Feistel network using two independent random functions, stated in Patarin's Eurocrypt '92 paper [9], can in fact be lifted to quasi-Feistel network.
3. We generalize Piret's results [17], where random permutations, instead of random functions are used as round functions, to quasi-Feistel network.
4. We also show that the Naor-Reingold construction [5] using pairwise independent permutations can be lifted to our quasi-Feistel setting.

Our first result implies the security of unbalanced Feistel network within the birthday bound. This was an unsolved problem, which was pointed out by Patarin et al. [15]. Also, when restricted to the Lai-Massey scheme, this gives an alternative proof of the Vaudenay's result in [20].

Together, our results show that most of the works on the security of Feistel cipher in the Luby-Rackoff model can in fact be lifted to the quasi-Feistel setting. Hence, in the Luby-Rackoff model, we claim that it is very natural to regard the Lai-Massey scheme and the Feistel network as belonging to the same family.

Despite Vaudenay's work and some others, Lai-Massey scheme seems to be less studied, especially compared with the works on Feistel network in the Luby-Rackoff model. Our results, especially 2–4 above, show that most of such works on Feistel network in fact can be applied to the Lai-Massey scheme as well, and quite increase the number of known results on the Luby-Rackoff security of the Lai-Massey scheme. We believe that the notion of quasi-Feistel network provides a unifying framework by which to study Lai-Massey scheme, and even the Feistel network.

It is also our belief that other results on the Feistel network can also be generalized to the quasi-Feistel setting. For example, it is an interesting open question whether Patarin's work on the Feistel network when $q \ll 2^n$ can be extended to the quasi-Feistel network, therefore also to the Lai-Massey scheme.

### 1.3 Related work

In our work, we generalize results of Luby-Rackoff [4], Patarin [9], Piret [17], and Naor-Reingold [5] to quasi-Feistel network. Also, for proof technique, we rely on the 'Coefficient $H$ Technique' of Patarin, among others.

Early on, Schneier and Kelsey noted that the notion of Feistel network can be generalized by requiring only that 'one part of the block being encrypted controls the encryption of another part of the block' [18]. Thus they introduced the notion of generalized Feistel network, which does not rely on any group structure. Their notion is very similar to the quasi-Feistel network in spirit, but their goal was not to prove the security of the generalized construction, and instead of the round functions $f_i$, the round keys $k_i$ are given as input. Our formulation is crucial for building Luby-Rackoff-like theory. One may see our work as a rigorous treatment of their 'generalized Feistel network'.

Vaudenay proved in [20] that 3 and 4-round Lai-Massey scheme is secure against CPA and CPCA attacks, respectively. Our results on the security of 3 and 4-round quasi-Feistel

network can be directly applied to the Lai-Massey scheme, and in this sense we give a new proof of Vaudenay's theorems using different technique. But his work is formulated in terms of Decorrelation theory [19], and for Lai-Massey scheme, our result is weaker than Vaudenay's. For example, the result of Vaudenay allows 'almost orthomorphisms'.

## 2 Quasi-Feistel network

Let $\mathcal{X}$ be a finite set. Then $\mathcal{X}^k$ denotes the set of all $k$-tuples of elements of $\mathcal{X}$, for any $k$. We denote by $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ the set of all functions $f : \mathcal{X} \to \mathcal{Y}$, and by $\mathsf{Perm}(\mathcal{X})$ the set of all permutations $f : \mathcal{X} \to \mathcal{X}$. We also define $\mathsf{Func}(\mathcal{X}) \stackrel{\text{def}}{=} \mathsf{Func}(\mathcal{X}, \mathcal{X})$.

**Definition 1.** *We call a function $\Gamma : \mathcal{X} \times \mathcal{X} \times \mathcal{Y} \to \mathcal{X}$ a* combiner *over $(\mathcal{X}, \mathcal{Y})$, if*

- *The mapping $x \mapsto \Gamma(x, y, z)$ is a permutation for any $y \in \mathcal{X}$, $z \in \mathcal{Y}$, and*
- *The mapping $y \mapsto \Gamma(x, y, z)$ is a permutation for any $x \in \mathcal{X}$, $z \in \mathcal{Y}$.*

Let $\Gamma$ be a combiner over $(\mathcal{X}, \mathcal{Y})$. If we define, for any $z \in \mathcal{Y}$, $\Gamma_z : \mathcal{X}^2 \to \mathcal{X}$ by $\Gamma_z(x, y) \stackrel{\text{def}}{=} \Gamma(x, y, z)$, then $\Gamma_z$ is a quasigroup for any $z \in \mathcal{X}$. This structure is also known as a Latin square. Therefore, a combiner $\Gamma$ can be considered as a parametrized family $\{\Gamma_z\}_{z \in \mathcal{Y}}$ of quasigroups.

We'll use the following notation to denote a combiner $\Gamma$:

$$\Gamma\,[\![x \star y \,|\, z]\!] \stackrel{\text{def}}{=} \Gamma(x, y, z)$$

From the properties of the combiner $\Gamma$, for any $x$, $y \in \mathcal{X}$, and $z \in \mathcal{Y}$, there exists a unique element $a \in \mathcal{X}$ satisfying $\Gamma\,[\![a \star y \,|\, z]\!] = x$. We'll denote this $a$ by $\Gamma\,[\![x/y \,|\, z]\!]$. Also, we'll denote the unique element $b \in \mathcal{X}$ satisfying $\Gamma\,[\![x \star b \,|\, z]\!] = y$ as $\Gamma\,[\![x\backslash y \,|\, z]\!]$. Then it is clear that the following lemma holds:

**Lemma 1.** *For any $x$, $y \in \mathcal{X}$, and $z \in \mathcal{Y}$, the following equations are satisfied:*

$$\begin{aligned} x &= \Gamma\,[\![\Gamma\,[\![x/y \,|\, z]\!] \star y \,|\, z]\!] \\ x &= \Gamma\,[\![\Gamma\,[\![x \star y \,|\, z]\!] /y \,|\, z]\!] \\ y &= \Gamma\,[\![x \star \Gamma\,[\![x\backslash y \,|\, z]\!] \,|\, z]\!] \\ y &= \Gamma\,[\![x\backslash \Gamma\,[\![x \star y \,|\, z]\!] \,|\, z]\!] \end{aligned}$$

*Remark 1.* In this paper, we'll only use combiners over $(\mathcal{X}, \mathcal{X}^{b-1})$, for some fixed integer $b > 1$. We call them *$b$-combiners* over $\mathcal{X}$.

**Definition 2.** *Let $b > 1$ and $r \geq 1$ be fixed integers, and fix a $b$-combiner $\Gamma$ over $\mathcal{X}$. Suppose that $P$, $Q : \mathcal{X}^b \to \mathcal{X}^b$ are permutations. Given $r$ functions $f_1, \ldots, f_r : \mathcal{X}^{b-1} \to \mathcal{X}$, we define a function $\Psi = \Psi^{b,r}_{P,Q}(f_1, \ldots, f_r) : \mathcal{X}^b \to \mathcal{X}^b$ as follows; for $x = (x_1, x_2, \ldots, x_b) \in \mathcal{X}^b$, we compute $y = \Psi(x)$ by*

1. $(z_0, z_1, \ldots, z_{b-1}) \leftarrow P(x)$.
2. $z_{i+b-1} \leftarrow \Gamma\,[\![z_{i-1} \star f_i(z_i \cdots z_{i+b-2}) \,|\, z_i \cdots z_{i+b-2}]\!]$ *for* $i = 1, \ldots, r$.
3. $y \leftarrow Q^{-1}(z_r, z_{r+1}, \ldots, z_{r+b-1})$.

*Clearly, $\Psi$ is a permutation, and its inverse is given by*

1. $(z_r, z_{r+1}, \ldots, z_{r+b-1}) \leftarrow Q(y)$.
2. $z_{i-1} \leftarrow \Gamma\,[\![z_{i+b-1} / f_i(z_i \cdots z_{i+b-2}) \,|\, z_i \cdots z_{i+b-2}]\!]$ *for* $i = r, \ldots, 1$.
3. $x \leftarrow P^{-1}(z_0, z_1, \ldots, z_{b-1})$.

*We call* $\Psi$ *a* $b$*-branched,* $r$*-round* quasi-Feistel permutation *for* $f_1, \ldots, f_r$ *with respect to* $(P, Q, \Gamma)$

We use the notation $\Psi^{b,r}_{P,Q}(f_1, \ldots, f_r)$ for $\Psi$, but when $P$ and $Q$ are unimportant, or clear from the context, then we may simply write $\Psi^{b,r}(f_1, \ldots, f_r)$. Also, $\Psi^{b,r}(f_1, \ldots, f_r)$ can be considered as a mapping

$$\Psi^{b,r} : \mathsf{Func}(\mathcal{X}^{b-1}, \mathcal{X})^r \to \mathsf{Perm}(\mathcal{X}^b).$$

We call this mapping a $b$-branched, $r$-round *quasi-Feistel network* with respect to $(P, Q, \Gamma)$.

We call $\mathcal{X}$ the underlying set, $P$ the pre-processing permutation, and $Q$ the post-processing permutation.

*Remark 2.* We call the quasi-Feistel network *balanced* when $b = 2$, and *unbalanced* when $b > 2$. Also, often by unquantified 'quasi-Feistel network' we refer to the balanced case. When $b = 2$, we omit $b$ in the notation $\Psi^{b,r}$ and simply write this as $\Psi^r$.

The above notion of quasi-Feistel network seems to be very natural extension of the Feistel network. In fact, we feel that, once the general structure is defined by the equation $z_{i+b-1} \leftarrow \Gamma\,[\![z_{i-1} \star f_i(z_i \cdots z_{i+b-2}) \,|\, z_i \cdots z_{i+b-2}]\!]$, the requirements for the combiner $\Gamma$ is almost forced upon us, in order to obtain a method for constructing secure cryptographic permutations; if we would like to make the whole construction invertible, then the best way is to make sure that $x \mapsto \Gamma\,[\![x \star y \,|\, z]\!]$ is invertible. Also, in order to make the whole construction cryptographically secure, we would like that, once $z_{i-1}$ and $z_i \cdots z_{i+b-2}$ are fixed, the distribution of $f_i(z_i \cdots z_{i+b-2})$ should have as much influence in determining the value of $z_{i+b-1}$ as possible, and the best way to achieve this would be to make $y \mapsto \Gamma\,[\![x \star y \,|\, z]\!]$ invertible. For example, at the other extreme, if $y \mapsto \Gamma\,[\![x \star y \,|\, z]\!]$ is constant, then the round functions $f_i$ don't have any influence to the output values, and the resulting permutation is not random at all.

In the next section, we show that the above construction is a generalization which contains both Feistel and Lai-Massey constructions as special cases.

## 3 Examples of quasi-Feistel networks

### 3.1 Feistel

The $r$-round Feistel permutation $\mathcal{F}(x) = \mathcal{F}(x_L, x_R)$ from round functions $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$ is defined as follows:

1. $L_1 \leftarrow x_L$, $R_1 \leftarrow x_R$.
2. $L_{i+1} \leftarrow R_i$, $R_{i+1} \leftarrow L_i \oplus f_i(R_i)$, for $i = 1, \ldots, r$.
3. $y_L \leftarrow L_{r+1}$, $y_R \leftarrow R_{r+1}$.
4. Return $y = (y_L, y_R)$.

Since $L_{i+1} = R_i$ for $i = 1, \ldots, r$, we may define $R_0 \stackrel{\text{def}}{=} L_1$ for consistency. Then we can eliminate $L_i$ completely from the above and it becomes

1. $R_0 \leftarrow x_L$, $R_1 \leftarrow x_R$.
2. $R_{i+1} \leftarrow R_{i-1} \oplus f_i(R_i)$, for $i = 1, \ldots, r$.
3. $y_L \leftarrow R_r$, $y_R \leftarrow R_{r+1}$.
4. Return $y = (y_L, y_R)$.

So, in this case, the underlying set $\mathcal{X}$ is simply $\{0,1\}^n$, and the permutations $P$ and $Q$ are the identity permutation, and the combiner $\Gamma$ is given by

$$\Gamma\,[\![x \star y \,|\, z]\!] = x \oplus y.$$

Therefore, we see that a Feistel network is a special case of the quasi-Feistel network.

### 3.2 Unbalanced Feistel network with contracting functions

Similarly, it is also clear that our quasi-Feistel network generalizes the unbalanced Feistel network with contracting functions, formalized in the paper of Patarin, Nachef, and Berbain [15]. This case is defined by special $b$-combiners over $\{0,1\}^n$, where

$$\Gamma\,[\![x \star y \,|\, z]\!] = x \oplus y.$$

### 3.3 Lai-Massey

The Lai-Massey scheme is slightly more involved than Feistel, and we need to do a little work to fit Lai-Massey into our framework. The Lai-Massey scheme was originally used in the IDEA cipher [2, 3]. But in this paper, by Lai-Massey scheme, we refer to the version given by Vaudenay in [20]. This version contains a simple function called orthomorphism, without which the Lai-Massey scheme suffers a simple distinguishing attack.

Let $G$ be a finite abelian group. An *orthomorphism* $\sigma : G \to G$ is a permutation such that $x \mapsto \sigma(x) - x$ is also a permutation. Given such a $\sigma$, we denote $\sigma(x) - x$ by $\tau(x)$. We assume that all of $\sigma$, $\sigma^{-1}$, $\tau$, $\tau^{-1}$ are very efficient to compute on $G$.

The following definition for the mapping $y = \mathcal{L}(x)$ is description of $r$-round Lai-Massey permutation with orthomorphism $\sigma$, corresponding to round functions $f_1, \ldots, f_r : G \to G$.

1. $\alpha_1 \leftarrow x_L$, $\beta_1 \leftarrow x_R$.
2. $\alpha_{i+1} \leftarrow \sigma(\alpha_i + f_i(\alpha_i - \beta_i))$, $\beta_{i+1} \leftarrow \beta_i + f_i(\alpha_i - \beta_i)$, for $i = 1, \ldots, r$.
3. $y_L \leftarrow \alpha_{r+1}$, $y_R \leftarrow \beta_{r+1}$.
4. Return $y = (y_L, y_R)$.

We define $H : G^2 \to G^2$ by

$$H(x, y) = (\sigma^{-1}x - y, x - y).$$

Then,

**Theorem 1.** *The Lai-Massey scheme is an instance of the quasi-Feistel network; the underlying set $\mathcal{X}$ is the group $G$, the pre- and post-processing permutations $P$ and $Q$ are both $H$, and the combiner $\Gamma$ is given by*

$$\Gamma\,[\![x \star y \,|\, z]\!] = z + \tau\left(z - x + y + \tau^{-1}(z - x)\right).$$

We prove the Theorem 1 in the Appendix A.

## 4 Security of unbalanced quasi-Feistel network

We show that $(2b-1)$-round, $b$-branched quasi-Feistel network is CPA-secure within the birthday bound, and $(3b-2)$-round, $b$-branched quasi-Feistel network is CPCA-secure within the birthday bound. Note that when $b=2$, the balanced case, these imply the results of Luby and Rackoff for 3- and 4-round Feistel ciphers [4]. Also, this shows for the first time that unbalanced Feistel cipher with contracting functions is secure within the birthday bound.

### 4.1 $(2b-1)$-round construction

Consider an information-theoretic adversary $A$ which has oracle access to a function $f : \mathcal{X}^b \to \mathcal{X}^b$. $A$ may query $f$ $q$ times, and we assume that $A$ never makes pointless queries, that is, it never makes the same query more than once. After $q$ queries, $A$ outputs 0 or 1. We define

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CPA}}_{\Psi^{b,r}}(A) = \Big|&\Pr[1 \leftarrow A(\Psi) \,|\, \Psi \leftarrow \Psi^{b,r}(f_1,\ldots,f_r),\ \text{where } f_i \xleftarrow{\$} \mathsf{Func}(\mathcal{X})] \\ &- \Pr[1 \leftarrow A(\rho) \,|\, \rho \xleftarrow{\$} \mathsf{Func}(\mathcal{X}^b)]\Big|\end{aligned}$$

Then,

**Theorem 2.** *For any fixed integer $b > 1$, we get the following:*

$$\mathsf{Adv}^{\mathrm{CPA}}_{\Psi^{b,2b-1}}(A) < \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}.$$

The proof technique of Theorem 2 is similar to that of Theorem 3 below. Therefore, in this extended abstract, we will only prove Theorem 3.

### 4.2 $(3b-2)$-round construction

Consider an information-theoretic adversary $A$ which has oracle access to a permutation $\pi : \mathcal{X}^b \to \mathcal{X}^b$. $A$ may query $\pi$ or $\pi^{-1}$ $q$ times, and again we assume that $A$ never makes pointless queries, that is, it never makes the same query more than once, and if it queried $\pi(x)$ and got $y$ as the answer, then it never queries $\pi^{-1}(y)$, and vice versa. After $q$ queries, $A$ outputs 0 or 1. We define

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^{b,r}}(A) = \Big|&\Pr[1 \leftarrow A(\Psi,\Psi^{-1}) \,|\, \Psi \leftarrow \Psi^{b,r}(f_1,\ldots,f_r),\ \text{where } f_i \xleftarrow{\$} \mathsf{Func}(\mathcal{X})] \\ &- \Pr[1 \leftarrow A(\rho,\rho^{-1}) \,|\, \rho \xleftarrow{\$} \mathsf{Perm}(\mathcal{X}^b)]\Big|\end{aligned}$$

Then,

**Theorem 3.** *For any fixed integer $b > 1$, we get the following:*

$$\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^{b,3b-2}}(A) < \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}} + \frac{q(q-1)}{2|\mathcal{X}|^{b}}.$$

We prove the Theorem 3 in the Appendix B.

*Remark 3.* Note that

$$\frac{bq(q-1)}{2|\mathcal{X}|^{b-1}} + \frac{q(q-1)}{2|\mathcal{X}|^{b}} < \frac{bq^2}{|\mathcal{X}|^{b-1}}.$$

Therefore, Theorems 2 and 3 means that, as long as

$$q \ll \sqrt{\frac{|\mathcal{X}|^{b-1}}{b}},$$

the $(2b-1)$-round quasi-Feistel permutation $\Psi$ is indistinguishable to a random permutation by any CPA-adversary, and the $(3b-2)$-round quasi-Feistel permutation $\Psi$ is indistinguishable to a random permutation by any CPCA-adversary.

*Remark 4.* Naor and Reingold [5] proved results similar to our Theorems 2 and 3. They showed that, for $b$-branched unbalanced Feistel network with contracting functions, $(b+1)$-round construction is CPA-secure with essentially the same bound as in Theorem 2, provided that the first round is replaced by a pairwise independent permutation, and similarly, $(b+2)$-round construction is CPCA-secure, provided that the first and the last rounds are replaced by pairwise independent permutations. Our results replaces one round of pairwise independent permutation with $b-1$ rounds of normal quasi-Feistel network.

*Remark 5.* According to Patarin et al. in [15], there is a chosen plaintext attack for $(2b-1)$-round, $b$-branched unbalanced Feistel network with contracting functions with the number of plaintext/ciphertext pair greater than or equal to $2^{n(b-\frac{3}{2})}$. This is the best known attack for this case, and this greatly exceeds the birthday bound. Therefore the tightness of our security proof is yet unknown.

## 5 Quasi-Feistel network with two random functions

As a consequence of Theorems 2 and 3 from the previous section, we know that 3- or 4-round (balanced) quasi-Feistel network is CPA-secure or CPCA-secure, respectively, within the birthday bound, when the round functions are chosen independently and uniformly.

For Feistel network, there were some results where the requirement of round function independence was relaxed. For example, in [9], Patarin studied the cases where the round functions are chosen from two independent random functions, or even a single random function.

We obtained generalization of Patarin's results for two independent random functions. In this extended abstract, we'll give only informal statements below.

### 5.1 3-round constructions

Suppose that $f$, $g : \mathcal{X} \to \mathcal{X}$ are independent random functions. Then there are four possible cases of constucting 3-round quasi-Feistel network with round functions chosen from $f$ or $g$: $\Psi^3(f,f,f)$, $\Psi^3(f,f,g)$, $\Psi^3(f,g,f)$, and $\Psi^3(f,g,g)$. Among these, it is easy to show that $\Psi^3(f,f,f)$ and $\Psi^3(f,g,f)$ are not secure. This is because that they are self-inverses of themselves when the left and right halves are swapped.

Thus the remaining cases are $\Psi^3(f,f,g)$ and $\Psi^3(f,g,g)$. We can show that both are CPA-secure within the birthday bound. Due to the possible internal collision, the upper bound

of advantage of adversaries are slightly increased than in the case of independent random functions; the common advantage bound for the two cases is

$$\frac{q(3q-1)}{2|\mathcal{X}|},$$

which is greater than the advantage bound $q(q-1)/|\mathcal{X}|$ for the independent case, which is from Theorem 2 with $b = 2$.

### 5.2 4-round constructions

Similarly, there are eight possible cases of constucting 4-round quasi-Feistel network with round functions chosen from two independent random functions $f$ and $g$. As in 3-round cases, we can easily see that $\Psi^4(f, f, f, f)$ and $\Psi^4(f, g, g, f)$ are not secure.

This leaves six cases: $\Psi^4(f, f, f, g)$, $\Psi^4(f, f, g, f)$, $\Psi^4(f, f, g, g)$, $\Psi^4(f, g, f, f)$, $\Psi^4(f, g, f, g)$, and $\Psi^4(f, g, g, g)$. We showed that they are all CPCA-secure within the birthday bound.

## 6 Quasi-Feistel network with random permutations

In this section, we show that for 3- and 4-round quasi-Feistel network, one can use random permutations as round functions to obtain security within birthday bound. This generalizes Piret's results [17] for Feistel network with random permutations as round functions.

### 6.1 3-round quasi-Feistel with random permutations

As in previous sections, consider an information-theoretic adversary $A$ with up to $q$ oracle queries to its oracle $f$. As usual, assume that $A$ doesn't make pointless queries. This time we define,

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CPA}}_{\Psi^3}(A) = \Big|&\Pr[1 \leftarrow A(\Psi) \,|\, \Psi \leftarrow \Psi^3(f_1, f_2, f_3), \text{ where } f_i \xleftarrow{\$} \mathsf{Perm}(\mathcal{X})] \\ &- \Pr[1 \leftarrow A(f) \,|\, f \xleftarrow{\$} \mathsf{Func}(\mathcal{X}^2)]\Big|\end{aligned}$$

**Theorem 4.**

$$\mathsf{Adv}^{\mathrm{CPA}}_{\Psi^3}(A) \leq \frac{q(q-1)}{|\mathcal{X}|-1} + \frac{q(q-1)}{|\mathcal{X}|}.$$

We give proof of Theorem 4 in Appendix C.

### 6.2 4-round quasi-Feistel with random permutations

Similarly, let $A$ be an adversary with oracle access to a permutation $\pi : \mathcal{X}^2 \to \mathcal{X}^2$ and its inverse. $A$ make at most $q$ queries, and $A$ makes no pointless queries. This time we define,

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^4}(A) = \Big|&\Pr[1 \leftarrow A(\Psi, \Psi^{-1}) \,|\, \Psi \leftarrow \Psi^4(f_1, f_2, f_3, f_4), \text{ where } f_i \xleftarrow{\$} \mathsf{Perm}(\mathcal{X})] \\ &- \Pr[1 \leftarrow A(\pi, \pi^{-1}) \,|\, \pi \xleftarrow{\$} \mathsf{Perm}(\mathcal{X}^2)]\Big|\end{aligned}$$

**Theorem 5.**

$$\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^4}(A) \leq \frac{2q(q-1)}{|\mathcal{X}|-1}.$$

The proof technique of Theorem 5 is similar to that of Theorem 4. Therefore, in this extended abstract we will omit the proof.

## 7 Naor-Reingold construction for quasi-Feistel network

In this section we lift the Naor-Reingold construction [5] of 4-round Feistel construction where pairwise independent permutations are used as first and last rounds, to the quasi-Feistel case.

**Definition 3.** *Let $\mathcal{X}$ be a finite set, $k$ an integer ($2 \leq k \leq |\mathcal{X}|$), and $\mathcal{P}$ a distribution of permutations on $\mathcal{X}$. If for any $k$-tuple $(x_1, \ldots, x_k)$ of distinct elements of $\mathcal{X}$, the distribution $(f(x_1), \ldots, f(x_k))$ for $f \xleftarrow{\$} \mathcal{P}$ is identical to the uniform distribution of distinct $k$-tuples on $\mathcal{X}$, then we say that $\mathcal{P}$ is* $k$-wise independent.

**Theorem 6.** *Let $\mathcal{P}$, $\mathcal{Q}$ be pairwise independent distribution of permutations on $\mathcal{X}^2$. Let $\Psi$ be the 2-round quasi-Feistel network of independent random functions $f_1$, $f_2$, with respect to $(\mathcal{P}, \mathcal{Q}, \Gamma)$. This means that we choose $P \xleftarrow{\$} \mathcal{P}$, $Q \xleftarrow{\$} \mathcal{Q}$, and define $\Psi$ as 2-round quasi-Feistel network of $f_1$, $f_2$ with respect to $(P, Q, \Gamma)$, that is, $\Psi \leftarrow \Psi^2_{P,Q}(f_1, f_2)$. Let $\rho \xleftarrow{\$} \mathsf{Perm}(\mathcal{X}^2)$ be a random permutation of $\mathcal{X}^2$.*

*For any CPCA-adversary $A$ that makes at most $q$ queries, we have*

$$\left|\Pr[1 \leftarrow A(\Psi, \Psi^{-1})] - \Pr[1 \leftarrow A(\rho, \rho^{-1})]\right| < \frac{q^2}{|\mathcal{X}|}$$

Note that one can also prove similar results for CPA-security, where the preprocessing permutation is chosen randomly from pairwise-independent distribution of permutations.

*Remark 6.* When we apply Theorem 6 to the Lai-Massey scheme, we see that 2-round Lai-Massey scheme is CPCA-secure, when pre- and post-processed by pairwise independent permutations. It is a simple consequence of the following obvious fact:

**Lemma 2.** *Let $h$ be a fixed permutation. If $\mathcal{P}$ is a pairwise independent distribution of permutations, then $h^{-1} \circ \mathcal{P} \circ h$ is also a pairwise independent distribution of permutations.* □

Actually, Naor and Reingold proved that only one random function suffices to make the 4-round Naor-Reingold construction CPCA-secure, when pairwise independent permutations are used as before. We also have the corresponding theorem:

**Theorem 7.** *Let $\mathcal{P}$, $\mathcal{Q}$ be pairwise independent distribution of permutations on $\mathcal{X}^2$, and let $f \xleftarrow{\$} \mathsf{Func}(\mathcal{X})$, $P \xleftarrow{\$} \mathcal{P}$, $Q \xleftarrow{\$} \mathcal{Q}$. Then let $\Psi \leftarrow \Psi^2_{P,Q}(f, f)$. Finally, let $\rho \xleftarrow{\$} \mathsf{Perm}(\mathcal{X}^2)$.*

*For any CPCA-adversary $A$ that makes at most $q$ queries, we have*

$$\left|\Pr[1 \leftarrow A(\Psi, \Psi^{-1})] - \Pr[1 \leftarrow A(\rho, \rho^{-1})]\right| < \frac{3q^2}{2|\mathcal{X}|}.$$

We give a brief sketch of proofs for Theorems 6 and 7 in Appendix D.

*Remark 7.* In fact, as mentioned before, Naor and Reingold also proved corresponding results for unbalanced Feistel network. Clearly, this can also be generalized to the quasi-Feistel setting in the similar way, and we'll omit the details.

## 8 Quasi-Feistel network and block cipher design

From our results above, we see that most of the works for Feistel network in the Luby-Rackoff model can be naturally extended to the quasi-Feistel case. Also, quasi-Feistel network includes the Lai-Massey scheme as an instance. Therefore, we may conclude that, the Lai-Massey scheme (or for that matter, any other quasi-Feistel network) does not have any advantage over the Feistel in terms of the Luby-Rackoff model, because both are instances belonging to the same class, namely the quasi-Feistel network.

Of course, that is not true when we apply a quasi-Feistel network to block cipher design. In our results, we considered quasi-Feistel ciphers which use random functions as round functions, or some variations thereof. Therefore, our results cannot be applied to more concrete versions of quasi-Feistel ciphers. The designer of a block cipher usually gives heuristic estimation for security against various known attacks, and most of these attacks rely on specific structures of the block cipher; in terms of our quasi-Feistel network, we cannot talk much about the security of a quasi-Feistel block cipher, unless the concrete description of the combiner $\Gamma$ is specified. Therefore it is not true that all quasi-Feistel networks are equal in these cases.

As an example, consider the specification of the FOX block cipher [1] which is now known as IDEA NXT. In the security analysis part, the designers considered Luby-Rackoff-like security, linear/differential cryptanalysis, integral attacks, statistical attacks, slide and related-key attacks, and so on. Among these, all we can say at the generic quasi-Feistel network level is the following:

1. The structure of a quasi-Feistel block cipher has security in the Luby-Rackoff model.
2. When the round functions have sufficiently small differential probabilities, and when the number of rounds, $r$, is large enough, a quasi-Feistel block cipher is resistant to the differential attack; this is simply because, in a quasi-Feistel network, any differential characteristic on two rounds must involve at least one round function.

Note that the observation on differential characteristic is identical to that of the designers of FOX block cipher. Also, in general, we cannot say anything about linear cryptanalysis, unless a concrete specification is given.

Apart from the above two, almost all other attacks rely on specific structures of the block cipher, therefore even within the family of quasi-Feistel networks, it is quite possible that some are better than others, in terms of security against various attacks.

## 9 Conclusion

In this paper, we introduced the notion of quasi-Feistel network, and showed that some of the works on the Feistel network can be naturally extended to our setting. Also we proved the birthday security of $(2b-1)$- and $(3b-2)$-round quasi-Feistel networks against CPA and CPCA attacks, respectively.

In the quasi-Feistel network, due to the requirement that the round functions should be indeed functions, many constraints occur. For example, from the equality $X_i = \Gamma[\![L_i \star f_1(R_i) \mid R_i]\!]$, we get

$$R_i = R_j \quad \longrightarrow \quad \Gamma[\![L_i \backslash X_i \mid R_i]\!] = \Gamma[\![L_j \backslash X_j \mid R_j]\!]$$

These systems of equations are dependent on the specific choice of the actual combiner $\Gamma$ used. So, different quasi-Feistel networks produce different systems of equations. Usually these equations are intertwined in complicated ways.

However, we notice that, only security up to the birthday bound is studied in many works on the Feistel network. In that case, collision of intermediate values cannot occur with high probability, therefore most of the equations in the system describing the construction simply disappear. In this type of works, specific choice of the Feistel combiner $\Gamma[\![x \star y \mid z]\!] = x \oplus y$ doesn't really matter that much, and often one may reproduce the proof using an arbitrary combiner.

In a sense, we might say that, what was done in many works on Feistel was to keep away from the inner complication of the Feistel network, by avoiding internal collisions as much as possible when the number of queries is less than the birthday bound. We believe that these works are in fact not dealing with Feistel network, but actually quasi-Feistel networks, since only general properties of the quasi-Feistel network as a family, not some specific property of the Feistel network, are used in the proof.

A notable exception to the above summary is the work of Patarin. Patarin studied the security of the Luby-Rackoff cipher when $q$ is less than $2^n$, and possibly greater than the birthday bound. In this situation, one cannot afford to simply discard problematic cases of internal collision, and one has to seriously analyze the complicated system of equations. It is quite possible that in Patarin's work, some properties exclusive to the Feistel network have actually been used.

Despite this, it is an interesting open problem whether it is possible to prove Patarin's theorem for the quasi-Feistel network, therefore automatically also for the Lai-Massey scheme. Direct translation of Patarin's proof to the quasi-Feistel setting seems to be difficult, but one may hope that some different proof technique could be devised for this generalized situation.

In [15], Patarin et al. gave generic attacks for unbalanced Feistel networks with contracting functions. The attack modes were KPA and CPA, and they gave attacks for different $r$, the number of rounds. In comparison, we showed CPA-security-until-birthday-bound of the case $r = 2b - 1$. The attack of Patarin et al. for this case requires the number of queries $q$ much greater than the birthday bound. It would be an interesting further study to close this gap between security proofs and the attacks. Also, one may study different types of unbalanced quasi-Feistel networks.

## References


1. P. Junod and S. Vaudenay. FOX: a new family of block ciphers. *Selected Areas in Cryptography - SAC 2004*, LNCS 2595, pp. 131–146, Springer-Verlag, 2004.
2. X. Lai. On the design and security of block ciphers. *ETH Series in Information Processing*, vol. 1, Hartung-Gorre Verlag, Konstanz, 1992.
3. X. Lai and J. L. Massey. A proposal for a new block encryption standard. *Advances in Cryptology - EUROCRYPT'90*, LNCS 473, pp. 389–404, Springer-Verlag, 1991.
4. M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373–386, April 1988.
5. M. Naor and O. Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology*, vol. 12, no. 1, pp. 29–66, 1999.
6. J. Patarin. Pseudorandom permutations based on the DES scheme. *Coding Theory and Applications - EUROCODE'90*, LNCS 514, pp. 193–204, Springer-Verlag, 1991.
7. J. Patarin. New results on pseudorandom permutation generators based on the DES scheme. *Advances in Cryptology - CRYPTO'91*, LNCS pp. 301–312, Springer-Verlag, 1992.
8. J. Patarin. *Etude des générateurs de permutations pseudo-aléatoires basés sur le schéma du D.E.S.*. Ph. D. Thesis, INRIA, Domaine de Voluceau, Le Chesnay, France, 1991.
9. J. Patarin. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. *Advances in Cryptology - EUROCRYPT'92*, LNCS 658, pp. 256–266, Springer-Verlag, 1993.

10. J. Patarin. About Feistel schemes with 6 (or More) rounds. *Fast Software Encryption - FSE'98*, LNCS 1372, pp. 103–121, Springer-Verlag, 1998.
11. J. Patarin. Generic attacks on Feistel schemes. *Advances in Cryptology - ASIACRYPT 2001*, LNCS 2248, pp. 222–238, Springer-Verlag, 2001.
12. J. Patarin. Luby-Rackoff: 7 rounds are enough for $2^{n(1-\epsilon)}$ security. *Advances in Cryptology - CRYPTO 2003*, LNCS 2729, pp. 513–529, Springer-Verlag, 2003.
13. J. Patarin. Security of random Feistel schemes with 5 or more rounds. *Advances in Cryptology - CRYPTO 2004*, LNCS 3152, pp. 106–122, Springer-Verlag, 2004.
14. J. Patarin. Security of random Feistel schemes with 5 or more rounds. Extended version of [13], preprint.
15. J. Patarin, V. Nachef and C. Berbain. Generic attacks on unbalanced Feistel schems with contracting functions. *Advances in Cryptology - ASIACRYPT 2006*, LNCS 4284, pp. 396–411, Springer-Verlag, 2006.
16. S. Patel, Z. Ramzan and G. S. Sundaram. Luby-Rackoff Ciphers over Finite Algebraic Structures or Why XOR is not so Exclusive. *Selected Areas in Cryptography - SAC 2002*, LNCS 2595, pp. 271–290. Springer-Verlag, 2003.
17. G. Piret. Luby-Rackoff Revisited: On the Use of Permutations as Inner Functions of a Feistel Scheme. *Designs, Codes and Cryptography*, vol. 39, no. 2, pp. 233–245, 2006.
18. B. Schneier and J. Kelsey. Unbalanced Feistel Networks and Block-Cipher Design. *Fast Software Encryption - FSE'96*, LNCS 1039, Springer-Verlag, pp. 121–144, 1996.
19. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. *Theoretical Aspects of Computer Science - STACS'98*, LNCS 1373, pp. 249–275, Springer-Verlag, 1998.
20. S. Vaudenay. On the Lai-Massey Scheme. *Advances in Cryptology - ASIACRYPT'99*, LNCS 1716, pp. 8–19, Springer-Verlag, 1999.

## A Proof of Theorem 1

Recall that $H : G^2 \to G^2$ is given by

$$H(x, y) = (\sigma^{-1}x - y, x - y).$$

Then a simple calculation shows that

$$H^{-1}(s, t) = \left(t - s + \tau^{-1}(t - s), -s + \tau^{-1}(t - s)\right).$$

We denote $\alpha_i - \beta_i$ by $z_i$. One immediately sees from the definition of Lai-Massey that $\sigma^{-1}\alpha_{i+1} - \beta_{i+1} = \alpha_i - \beta_i = z_i$. Then we have

$$(z_{i-1}, z_i) = (\sigma^{-1}\alpha_i - \beta_i, \alpha_i - \beta_i) = H(\alpha_i, \beta_i).$$

Using $H$ and the Lai-Massey formula

$$(\alpha_{i+1}, \beta_{i+1}) = (\sigma(\alpha_i + f_i(\alpha_i - \beta_i)), \beta_i + f_i(\alpha_i - \beta_i)),$$

we may compute $z_{i+1}$ from $z_{i-1}$, $z_i$, and $f_i(z_i)$; starting with $(z_{i-1}, z_i)$, applying $H^{-1}$, we get $(\alpha_i, \beta_i)$, from which we compute $(\alpha_{i+1}, \beta_{i+1})$, from which we get $(z_i, z_{i+1})$ by applying $H$. By expanding the formulas for $H$ and $H^{-1}$ explicitly, we get

$$z_{i+1} = z_i + \tau\left(z_i - z_{i-1} + f_i(z_i) + \tau^{-1}(z_i - z_{i-1})\right).$$

Also, from the above description, it is clear that given $z_{i+1}$, $z_i$, and $f_i(z_i)$, we can compute $z_{i-1}$.

Hence, we may define the combiner $\Gamma$ by

$$\Gamma[\![x \star y \,|\, z]\!] = z + \tau\left(z - x + y + \tau^{-1}(z - x)\right).$$

**Lemma 3.** *$\Gamma$ is indeed a combiner over $G$; $x \mapsto \Gamma[\![x \star y \,|\, z]\!]$ and $y \mapsto \Gamma[\![x \star y \,|\, z]\!]$ are permutations for any $x$, $y$, $z \in G$.*

*Proof.* Since we can invert the above procedure to get $(z_{i-1}, z_i)$ from $(z_i, z_{i+1})$, the mapping $x \mapsto \Gamma[\![x \star y \,|\, z]\!]$ should be invertible. Indeed, by manipulating the above formula, we get

$$\Gamma[\![x/y \,|\, z]\!] = y + z - \tau^{-1}(x - z) + \sigma^{-1}\left(\tau^{-1}(x - z) - y\right).$$

Also, we see that $y \mapsto \Gamma[\![x \star y \,|\, z]\!]$ is invertible for any $x$, $z \in G$, which is because that $y$ occurs only once in $\Gamma[\![x \star y \,|\, z]\!]$, and the formula is built by either adding a group element or taking a permutation. Explicitly, we have

$$\Gamma[\![x \backslash y \,|\, z]\!] = x - z - \tau^{-1}(z - x) + \tau^{-1}(y - z).$$

□

Now we can prove Theorem 1:

*Proof (Of Theorem 1).* We give the following equivalent description of the Lai-Massey scheme; given the input $x = (x_L, x_R) = (\alpha_1, \beta_1)$, we apply $H$ to compute $(z_0, z_1) = \mathcal{H}(\alpha_1, \beta_1)$. Then by the equation

$$z_{i+1} = z_i + \tau\left(z_i - z_{i-1} + f_i(z_i) + \tau^{-1}(z_i - z_{i-1})\right) = \Gamma[\![z_{i-1} \star f_i(z_i) \,|\, z_i]\!],$$

we compute $z_2$, $z_3$, …, $z_t$, $z_{r+1}$. Finally, we compute the output $(\alpha_{r+1}, \beta_{r+1})$ by $(\alpha_{r+1}, \beta_{r+1}) = H^{-1}(z_r, z_{r+1})$. □

## B Proof of Theorem 3

First, we'll show that, often, without loss of generality, we may assume that the pre- and post-processing permutations $P$ and $Q$ are both identity permutations in the Luby-Rackoff model. The following Lemma is stated for the case of CPCA-adversary for unbalanced quasi-Feistel network, but it is clear that one can easily prove corresponding results for other cases.

**Lemma 4.** *Consider a $b$-branched, $r$-round unbalanced quasi-Feistel network $\Psi$ with respect to $(P, Q, \Gamma)$. Let's define $\Psi'$ to be the unbalanced quasi-Feistel network with respect to $(I, I, \Gamma)$, where $I : \mathcal{X}^b \to \mathcal{X}^b$ is the identity permutation $I(x) = x$. Then, for any CPCA-adversary $A$,*

$$\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^{b,r}}(A) = \mathsf{Adv}^{\mathrm{CPCA}}_{\Psi'^{b,r}}(A).$$

*Proof.* We have

$$\Psi = Q^{-1} \circ \Psi' \circ P.$$

If $\pi$ is a random permutation, then $\pi' = Q \circ \pi \circ P^{-1}$ is also a random permutation. We see that the advantage of distinguishing $\Psi$ from $\pi$ is identical to that of distinguishing $\Psi'$ from $\pi'$. □

Hence, we assume that $P = Q = I$ in this section and also in other parts of this paper.

We prove security of $(3b-2)$-round unbalanced quasi-Feistel networks. For convenience, we would like to introduce some notational conventions for this section. First, we label the $3b-2$ random functions by

$$f_1, f_2, \ldots, f_{b-1}, g_1, g_2, \ldots, g_b, h_1, h_2, \ldots, h_{b-1}.$$

For inputs $x_i = (x_i^1, x_i^2, \ldots, x_i^b)$ and outputs $y_i = (y_i^1, y_i^2, \ldots, y_i^b)$, we would like to estimate the probability that $\Psi(x_i) = y_i$ for $\forall i = 1, \ldots, q$. Instead of the usual intermediate variables $z_j^{(i)}$ for $i^{\text{th}}$ input, we'll re-label the old variables by introducing variables $X_i^j$ and $Y_i^j$. The correspondence is represented by the following table.

| | | | |
|---|---|---|---|
| $z_0^{(i)}\ z_1^{(i)}\ \ldots\ z_{b-1}^{(i)}$ | $z_b^{(i)}\ z_{b+1}^{(i)}\ \ldots\ z_{2b-2}^{(i)}$ | $z_{2b-1}^{(i)}\ z_{2b}^{(i)}\ \ldots\ z_{3b-3}^{(i)}$ | $z_{3b-2}^{(i)}\ z_{3b-1}^{(i)}\ \ldots\ z_{4b-3}^{(i)}$ |
| $x_i^1\ x_i^2\ \ldots\ x_i^b$ | $X_i^1\ X_i^2\ \ldots\ X_i^{b-1}$ | $Y_i^1\ Y_i^2\ \ldots\ Y_i^{b-1}$ | $y_i^1\ y_i^2\ \ldots\ y_i^b$ |

The relation between the above new functions and variables are summarized in Table 1.

From our notational conventions, we see that, in order that

$$\Psi^{b,3b-2}(f_1, f_2, \ldots, f_{b-1}, g_1, g_2, \ldots, g_b, h_1, h_2, \ldots, h_{b-1})(x_i) = y_i$$

**Table 1.** Internal variables for $3b-2$ rounds

| Round | Function | Internal variables | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | $f_1$ | $x^1$ | $x^2$ | | $\cdots$ | | | $x^b$ |
| 2 | $f_2$ | $x^2$ | $x^3$ | | $\cdots$ | | $x^b$ | $X^1$ |
| 3 | $f_3$ | $x^3$ | $x^4$ | | $\cdots$ | $x^b$ | $X^1$ | $X^2$ |
| | | | | | $\vdots$ | | | |
| $b-2$ | $f_{b-2}$ | $x^{b-2}$ | $x^{b-1}$ | $x^b$ | $\cdots$ | | $X^{b-4}$ | $X^{b-3}$ |
| $b-1$ | $f_{b-1}$ | $x^{b-1}$ | $x^b$ | $X^1$ | $\cdots$ | | $X^{b-3}$ | $X^{b-2}$ |
| $b$ | $g_1$ | $x^b$ | $X^1$ | | $\cdots$ | | $X^{b-2}$ | $X^{b-1}$ |
| $b+1$ | $g_2$ | $X^1$ | $X^2$ | | $\cdots$ | | $X^{b-1}$ | $Y^1$ |
| $b+2$ | $g_3$ | $X^2$ | $X^3$ | | $\cdots$ | $X^{b-1}$ | $Y^1$ | $Y^2$ |
| | | | | | $\vdots$ | | | |
| $2b-2$ | $g_{b-1}$ | $X^{b-2}$ | $X^{b-1}$ | $Y^1$ | $\cdots$ | | $Y^{b-3}$ | $Y^{b-2}$ |
| $2b-1$ | $g_b$ | $X^{b-1}$ | $Y^1$ | $Y^2$ | $\cdots$ | | $Y^{b-2}$ | $Y^{b-1}$ |
| $2b$ | $h_1$ | $Y^1$ | $Y^2$ | | $\cdots$ | | $Y^{b-1}$ | $y^1$ |
| $2b+1$ | $h_2$ | $Y^2$ | $Y^3$ | | $\cdots$ | $Y^{b-1}$ | $y^1$ | $y^2$ |
| | | | | | $\vdots$ | | | |
| $3b-3$ | $h_{b-2}$ | $Y^{b-2}$ | $Y^{b-1}$ | $y^1$ | $\cdots$ | | $y^{b-3}$ | $y^{b-2}$ |
| $3b-2$ | $h_{b-1}$ | $Y^{b-1}$ | $y^1$ | | $\cdots$ | | $y^{b-2}$ | $y^{b-1}$ |
| | | $y^1$ | $y^2$ | | $\cdots$ | $y^{b-2}$ | $y^{b-1}$ | $y^b$ |

holds for $\forall i = 1, \ldots, q$, the following equations should be satisfied:

$$
\begin{aligned}
X_i^1 &= \Gamma\left[\left[x_i^1 \star f_1(x_i^2 \cdots x_i^b) \,|\, x_i^2 \cdots x_i^b\right]\right] \\
X_i^2 &= \Gamma\left[\left[x_i^2 \star f_2(x_i^3 \cdots x_i^b X_i^1) \,|\, x_i^3 \cdots x_i^b X_i^1\right]\right] \\
&\vdots \\
X_i^{b-1} &= \Gamma\left[\left[x_i^{b-1} \star f_{b-1}(x_i^b X_i^1 \cdots X_i^{b-2}) \,|\, x_i^b X_i^1 \cdots X_i^{b-2}\right]\right] \\
Y_i^1 &= \Gamma\left[\left[x_i^b \star g_1(X_i^1 \cdots X_i^{b-1}) \,|\, X_i^1 \cdots X_i^{b-1}\right]\right] \\
Y_i^2 &= \Gamma\left[\left[X_i^1 \star g_2(X_i^2 \cdots X_i^{b-1} Y_i^1) \,|\, X_i^2 \cdots X_i^{b-1} Y_i^1\right]\right] \\
&\vdots \\
Y_i^{b-1} &= \Gamma\left[\left[X_i^{b-2} \star g_{b-1}(X_i^{b-1} Y_i^1 \cdots Y_i^{b-2}) \,|\, X_i^{b-1} Y_i^1 \cdots Y_i^{b-2}\right]\right] \\
y_i^1 &= \Gamma\left[\left[X_i^{b-1} \star g_b(Y_i^1 \cdots Y_i^{b-1}) \,|\, Y_i^1 \cdots Y_i^{b-1}\right]\right] \\
y_i^2 &= \Gamma\left[\left[Y_i^1 \star h_1(Y_i^2 \cdots Y_i^{b-1} y_i^1) \,|\, Y_i^2 \cdots Y_i^{b-1} y_i^1\right]\right] \\
&\vdots \\
y_i^b &= \Gamma\left[\left[Y_i^{b-1} \star h_{b-1}(y_i^1 \cdots y_i^{b-1}) \,|\, y_i^1 \cdots y_i^{b-1}\right]\right]
\end{aligned}
$$

From the above, we see that, given $(x_i^1, \ldots, x_i^b)$ and $(y_i^1, \ldots, y_i^b)$, the collection of random functions $(f_1, \ldots, f_{b-1})$ determines the values $(X_i^1, \ldots, X_i^{b-1})$, and similarly $(h_1, \ldots, h_{b-1})$ determines the values $(Y_i^1, \ldots, Y_i^{b-1})$.

**Lemma 5.** *Fix some $i$, $j$ such that $1 \le i < j \le q$. Also, fix some $k$ such that $1 \le k \le b$. Then, the probability that by randomly choosing $f_1, \ldots, f_{b-1}$,*

$$X_i^k \cdots X_i^{b-1} = X_j^k \cdots X_j^{b-1}$$

*holds is at most*

$$\frac{1}{|\mathcal{X}|^{b-k}}.$$

*Proof.* The condition

$$X_i^k \cdots X_i^{b-1} = X_j^k \cdots X_j^{b-1}$$

is equivalent to the following $b-k$ conditions:

$$X_i^k = X_j^k, \quad X_i^{k+1} = X_j^{k+1}, \quad \ldots, \quad X_i^{b-1} = X_j^{b-1}.$$

Intuitively, each condition contributes at most $1/|\mathcal{X}|$ to the probability, therefore the overall probability is at most $1/|\mathcal{X}|^{b-k}$.

To be more precise, let's choose the functions $f_1, \ldots, f_{k-1}$ arbitrarily. This determines $X_i^1, \ldots, X_i^{k-1}$. Then,

$$\begin{aligned} X_i^k &= \Gamma\left[\left[x_i^k \star f_k(x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}) \,|\, x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}\right]\right] \\ X_j^k &= \Gamma\left[\left[x_j^k \star f_k(x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}) \,|\, x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}\right]\right] \end{aligned}$$

We claim that the probability for $X_i^k = X_j^k$ to hold is at most $1/|\mathcal{X}|$. To prove this, we divide the cases. First, conside the case when

$$x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1} = x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}. \tag{1}$$

In this case, suppose that $X_i^k = X_j^k$ holds. Then,

$$\begin{aligned} x_i^k &= \Gamma\left[\left[X_i^k / f_k(x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}) \,|\, x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}\right]\right] \\ &= \Gamma\left[\left[X_j^k / f_k(x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}) \,|\, x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}\right]\right] \\ &= x_j^k \end{aligned}$$

Then $x_i^k = x_j^k$, and this implies that

$$x_i^k x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1} = x_j^k x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}.$$

Then we have $X_i^{k-1} = X_j^{k-1}$ and

$$x_i^k x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-2} = x_j^k x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-2}.$$

Repeating this, we conclude that $x_i^1 \cdots x_i^b = x_j^1 \cdots x_j^b$ which contradicts that the inputs are all distinct. Hence, we conclude that when (1) holds, no function $f_k$ can make $X_i^k = X_j^k$,

hence the probability is 0. Next, consider the case when (1) does not hold. In this case, when $f_k(x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1})$ is determined, we have

$$\begin{aligned}
&f_k(x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}) \\
&= \Gamma\left[\left[x_k^k \backslash X_j^k \mid x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}\right]\right] \\
&= \Gamma\left[\left[x_k^k \backslash X_i^k \mid x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}\right]\right] \\
&= \Gamma\left[\left[x_k^k \backslash \Gamma\left[\left[x_i^k \star f_k(x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}) \mid x_i^{k+1} \cdots x_i^b X_i^1 \cdots X_i^{k-1}\right]\right] \mid x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}\right]\right]
\end{aligned}$$

Then, we can choose $f_k$ freely, except that the value for $x_j^{k+1} \cdots x_j^b X_j^1 \cdots X_j^{k-1}$ is constrained by the above formula. Then the probability is $1/|\mathcal{X}|$.

Then, regardless of whether (1) holds or not, the probability that $X_i^k = X_j^k$ holds is less than or equal to $1/|\mathcal{X}|$. Choose any $f_k$ which satisfies the equation.

Now, we see that the exact same argument can be used to show that the probability that $X_i^{k+1} = X_j^{k+1}$ holds is less than or equal to $1/|\mathcal{X}|$. Choose any $f_{k+1}$ which satisfies the equation. Continuing in this way, the probability that all of $b-k$ equations

$$X_i^k = X_j^k, \quad X_i^{k+1} = X_j^{k+1}, \quad \ldots, \quad X_i^{b-1} = X_j^{b-1}$$

are satisfied is less than or equal to $1/|\mathcal{X}|^{b-k}$. □

**Corollary 1.** *Fix some $i$, $j$ such that $1 \leq i < j \leq q$. Also, fix some $k$ such that $1 \leq k \leq b$. Then, the probability that by randomly choosing $h_1, \ldots, h_{b-1}$,*

$$Y_i^1 \cdots Y_i^{k-1} = Y_j^1 \cdots Y_j^{k-1}$$

*holds is at most*

$$\frac{1}{|\mathcal{X}|^{k-1}}.$$

*Proof.* The functions $h_1, \ldots, h_{b-1}$ defines the variables $Y_i^1, \ldots, Y_i^{b-1}$. The proof is essentially the same as the Lemma 5. □

**Corollary 2.** *Fix some $i$, $j$ such that $1 \leq i < j \leq q$. Also, fix some $k$ such that $1 \leq k \leq b$. Then, the probability that by randomly choosing $f_1, \ldots, f_{b-1}$, $h_1, \ldots, h_{b-1}$,*

$$X_i^k \cdots X_i^{b-1} Y_i^1 \cdots Y_i^{k-1} = X_j^k \cdots X_j^{b-1} Y_j^1 \cdots Y_j^{k-1}$$

*is at most*

$$\frac{1}{|\mathcal{X}|^{b-1}}.$$

*Proof.* The condition

$$X_i^k \cdots X_i^{b-1} Y_i^1 \cdots Y_i^{k-1} = X_j^k \cdots X_j^{b-1} Y_j^1 \cdots Y_j^{k-1}$$

is equivalent to two conditions

$$X_i^k \cdots X_i^{b-1} = X_j^k \cdots X_j^{b-1} \text{ and } Y_i^1 \cdots Y_i^{k-1} = Y_j^1 \cdots Y_j^{k-1}.$$

The two conditions are independent, and the probability that each holds are at most

$$\frac{1}{|\mathcal{X}|^{b-k}} \text{ and } \frac{1}{|\mathcal{X}|^{k-1}}, \text{ respectively.}$$

□

**Corollary 3.** *The probability that*

$$X_i^k \cdots X_i^{b-1} Y_i^1 \cdots Y_i^{k-1} = X_j^k \cdots X_j^{b-1} Y_j^1 \cdots Y_j^{k-1}$$

*does not hold for any* $1 \leq i < j \leq q$ *and any* $1 \leq k \leq b$ *is at least*

$$1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}.$$

□

The Corollary 3 gives us a guarantee that no internal collision occurs with at least that probability.

In order to prove Theorem 3, we need the following Theorem 8. Note that this estimation of transition probability from given inputs to given outputs is the core of Patarin's 'coefficient $H$ technique'.

**Theorem 8.** *Let* $x_i \in \mathcal{X}^b$, $1 \leq i \leq q$ *be distinct inputs, and let* $y_i \in \mathcal{X}^b$, $1 \leq i \leq q$ *be distinct outputs.*

*Let's denote by* $h$ *the probability that* $\Psi$*, the* $b$*-branched,* $(3b-2)$*-round unbalanced quasi-Feistel permutation for* $3b-2$ *random functions, satisfies* $\forall i, 1 \leq i \leq q$*,*

$$\Psi(x_i) = y_i.$$

*Then we have*

$$h \geq \frac{1}{|\mathcal{X}|^{bq}} \left(1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}\right).$$

*Proof.* With probability at least

$$1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}},$$

we may choose random functions $f_1, \ldots, f_{b-1}, h_1, \ldots, h_{b-1}$ such that

$$X_i^k \cdots X_i^{b-1} Y_i^1 \cdots Y_i^{k-1} \neq X_j^k \cdots X_j^{b-1} Y_j^1 \cdots Y_j^{k-1}$$

for any $1 \leq i < j \leq q$ and any $1 \leq k \leq b$. Then the probability that we may choose random functions $g_1, \ldots, g_b$ so that

$$\begin{aligned}
Y_i^1 &= \Gamma\left[\left[x_i^b \star g_1(X_i^1 \cdots X_i^{b-1}) \,|\, X_i^1 \cdots X_i^{b-1}\right]\right] \\
Y_i^2 &= \Gamma\left[\left[X_i^1 \star g_2(X_i^2 \cdots X_i^{b-1} Y_i^1) \,|\, X_i^2 \cdots X_i^{b-1} Y_i^1\right]\right] \\
&\vdots \\
Y_i^{b-1} &= \Gamma\left[\left[X_i^{b-2} \star g_{b-1}(X_i^{b-1} Y_i^1 \cdots Y_i^{b-2}) \,|\, X_i^{b-1} Y_i^1 \cdots Y_i^{b-2}\right]\right] \\
y_i^1 &= \Gamma\left[\left[X_i^{b-1} \star g_b(Y_i^1 \cdots Y_i^{b-1}) \,|\, Y_i^1 \cdots Y_i^{b-1}\right]\right]
\end{aligned}$$

holds for $i = 1, \ldots, q$ is equal to $(1/|\mathcal{X}|^b)^q$. Putting all of the above together, we get the result. □

Now we are ready to go back to proof of the Theorem 3:

*Proof (Of Theorem 3).* The queries of $A$ to its oracle $\pi$ have form $\pi(x_i)$ or $\pi^{-1}(y_i)$. We may write the queries as $\pi^{\epsilon_i}(Q_i)$, and denote by $\sigma_i$ the answer of the oracle to the query. Then $(\epsilon_1, Q_1)$ is dependent only to $A$, and $(\epsilon_2, Q_2)$ is dependent to $A$ and $\sigma_1$, and $(\epsilon_3, Q_3)$ is dependent to $A$ and $\sigma_1$, $\sigma_2$, and so on. Finally $A(\pi)$, the answer of $A$ is dependent only to $A$ and $\sigma_1, \ldots, \sigma_q$; if $\pi' : \mathcal{X}^b \to \mathcal{X}^b$ is another permutation such that $\pi'^{\epsilon_i}(Q_i) = \sigma_i$, then $A$'s queries to both $\pi$ and $\pi'$ would be identical, and the answers would be identical, therefore $A(\pi) = A(\pi')$.

Hence, if the queries of $A$ to its oracle $\pi$ are $(\epsilon_i, Q_i)$, and if the answers it gets are $\sigma_i$, then we may write $A(\sigma_1, \ldots, \sigma_q)$, instead of $A(\pi)$. Let's define

$$P_1 \stackrel{\text{def}}{=} \Pr[1 \leftarrow A(\Psi, \Psi^{-1}) \,|\, \Psi \leftarrow \Psi^{b,3b-2}(f_1, \ldots, f_{3b-2}), \text{ where } f_i \stackrel{\$}{\leftarrow} \mathsf{Func}(\mathcal{X})]$$
$$P_1^{**} \stackrel{\text{def}}{=} \Pr[1 \leftarrow A(\pi, \pi^{-1}) \,|\, \pi \stackrel{\$}{\leftarrow} \mathsf{Perm}(\mathcal{X}^b)]$$

Note that by definition, $\mathsf{Adv}^{\text{CPCA}}_{\Psi^{b,3b-2}}(A) = |P_1 - P_1^{**}|$.
If $N$ is the number of $\sigma_1, \ldots, \sigma_q$ such that $1 \leftarrow A(\sigma_1, \ldots, \sigma_q)$, then

$$\begin{aligned}
P_1^{**} &= \frac{\text{Number of } \pi \in \mathsf{Perm}(\mathcal{X}^b) \text{ such that } 1 \leftarrow A(\pi)}{\text{Number of } \pi \in \mathsf{Perm}(\mathcal{X}^b)} \\
&= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{\text{Number of } \pi \in \mathsf{Perm}(\mathcal{X}^b) \text{ compatible with } \sigma_1, \ldots, \sigma_q}{\text{Number of } \pi \in \mathsf{Perm}(\mathcal{X}^b)} \\
&= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{(|\mathcal{X}|^b - q)!}{(|\mathcal{X}|^b)!} \\
&= \frac{N}{|\mathcal{X}|^{bq}\left(1 - \frac{1}{|\mathcal{X}|^b}\right)\left(1 - \frac{2}{|\mathcal{X}|^b}\right)\cdots\left(1 - \frac{q-1}{|\mathcal{X}|^b}\right)}
\end{aligned}$$

Hence, we get

$$\begin{aligned}
\frac{N}{|\mathcal{X}|^{bq}} &= P_1^{**} \prod_{i=1}^{q-1}\left(1 - \frac{i}{|\mathcal{X}|^b}\right) \\
&\geq P_1^{**}\left(1 - \sum_{i=1}^{q-1}\frac{i}{|\mathcal{X}|^b}\right) \\
&= P_1^{**}\left(1 - \frac{q(q-1)}{2|\mathcal{X}|^b}\right)
\end{aligned} \tag{2}$$

Then,

$$\begin{aligned}
P_1 &= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \mathsf{Pr}\left[(f_1, \ldots, f_{3b-2}) \text{ is compatible with } \sigma_1, \ldots, \sigma_q\right] \\
&\geq \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{1}{|\mathcal{X}|^{bq}}\left(1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}\right) = \frac{N}{|\mathcal{X}|^{bq}}\left(1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}\right) \\
&\geq P_1^{**}\left(1 - \frac{q(q-1)}{2|\mathcal{X}|^b}\right)\left(1 - \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}}\right) \\
&> P_1^{**} - \left(\frac{bq(q-1)}{2|\mathcal{X}|^{b-1}} + \frac{q(q-1)}{2|\mathcal{X}|^b}\right).
\end{aligned}$$

If we switch the outputs 1 and 0 of $A$, in the same way we also get,

$$1 - P_1 > 1 - P_1^{**} - \left( \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}} + \frac{q(q-1)}{2|\mathcal{X}|^b} \right)$$

From the above two inequalities, we finally get

$$\mathsf{Adv}^{\mathrm{CPCA}}_{\Psi^{b,3b-2}}(A) = |P_1 - P_1^{**}| < \frac{bq(q-1)}{2|\mathcal{X}|^{b-1}} + \frac{q(q-1)}{2|\mathcal{X}|^b}.$$

□

## C Proof of Theorem 4

In order to prove Theorem 4, we need some preparations.

We know that without loss of generality, we may set $P = Q = I$.

**Lemma 6.** *Suppose that $L_i$, $R_i$, $X_i$, $S_i$, $T_i \in \mathcal{X}$ are given, for $i = 1, \ldots, q$, such that $(L_i, R_i)$ are distinct. Also suppose that the following five conditions are satisfied;*

$$R_i = R_j \longleftrightarrow \Gamma[\![L_i \backslash X_i \,|\, R_i]\!] = \Gamma[\![L_j \backslash X_j \,|\, R_j]\!] \tag{C1}$$

$$X_i \text{ are distinct} \tag{C2}$$

$$S_i \text{ are distinct} \tag{C3}$$

$$\Gamma[\![R_i \backslash S_i \,|\, X_i]\!] \text{ are distinct} \tag{C4}$$

$$\Gamma[\![X_i \backslash T_i \,|\, S_i]\!] \text{ are distinct} \tag{C5}$$

*Then, the number of 3-tuples $(f_1, f_2, f_3) \in \mathsf{Perm}(\mathcal{X})^3$ satisfying*

$$X_i = \Gamma[\![L_i \star f_1(R_i) \,|\, R_i]\!]$$
$$S_i = \Gamma[\![R_i \star f_2(X_i) \,|\, X_i]\!]$$
$$T_i = \Gamma[\![X_i \star f_3(S_i) \,|\, S_i]\!]$$

*is equal to*

$$(|\mathcal{X}| - q + r)! \cdot (|\mathcal{X}| - q)! \cdot (|\mathcal{X}| - q)!$$

*where $r$ is the number of independent equations of form $R_i = R_j$.*

*Proof.* In other words, $q - r = |\{R_i \,|\, i = 1, \ldots, q\}|$.

$f_1$ is free as a permutation except for the prescribed $q - r$ points. Therefore there are precisely $(|\mathcal{X}| - q + r)!$ such functions $f_1$, satisfying $X_i = \Gamma[\![L_i \star f_1(R_i) \,|\, R_i]\!]$. Similarly there are $(|\mathcal{X}| - q)!$ $f_2$'s, and $(|\mathcal{X}| - q)!$ $f_3$'s. □

**Lemma 7.** *Suppose that $L_i$, $R_i \in \mathcal{X}$ are given, for $i = 1, \ldots, q$, such that $(L_i, R_i)$ are distinct. Then the number of $q$-tuples $(X_1, \ldots, X_q)$ satisfying*

$$R_i = R_j \longleftrightarrow \Gamma[\![L_i \backslash X_i \,|\, R_i]\!] = \Gamma[\![L_j \backslash X_j \,|\, R_j]\!] \tag{C1}$$

*is equal to*

$$\frac{|\mathcal{X}|!}{(|\mathcal{X}| - q + r)!}$$

*where $r$ is the number of independent equations of form $R_i = R_j$.*

*Proof.* If we set

$$X_i = \Gamma\left[\!\left[L_i \star f(R_i) \,|\, R_i\right]\!\right],$$

then the condition (C1) is equivalent to

$$R_i = R_j \longleftrightarrow f(R_i) = f(R_j).$$

Let $R_{i_1}$, $R_{i_2}$, ..., $R_{i_{q-r}}$ be any set of $q-r$ representative elements for $\{R_i \,|\, i = 1, \ldots, q\}$. Then, choosing $X_i$ satisfying (C1) is equivalent to choosing distinct $f(R_{i_j})$, $j = 1, \ldots, q-r$. There are exactly

$$|\mathcal{X}| \cdot (|\mathcal{X}| - 1) \cdots (|\mathcal{X}| - (q-r-1)) = \frac{|\mathcal{X}|!}{(|\mathcal{X}| - q + r)!}$$

such choices. □

**Lemma 8.** *Suppose that $L_i$, $R_i \in \mathcal{X}$ are given, for $i = 1, \ldots, q$, such that $(L_i, R_i)$ are distinct. Then the number of three $q$-tuples $(X_1, \ldots, X_q)$, $(S_1, \ldots, S_q)$, $(T_1, \ldots, T_q)$ satisfying*

$$R_i = R_j \longleftrightarrow \Gamma\left[\!\left[L_i \backslash X_i \,|\, R_i\right]\!\right] = \Gamma\left[\!\left[L_j \backslash X_j \,|\, R_j\right]\!\right] \tag{C1}$$

$$X_i \text{ are distinct} \tag{C2}$$

$$S_i \text{ are distinct} \tag{C3}$$

$$\Gamma\left[\!\left[R_i \backslash S_i \,|\, X_i\right]\!\right] \text{ are distinct} \tag{C4}$$

$$\Gamma\left[\!\left[X_i \backslash T_i \,|\, S_i\right]\!\right] \text{ are distinct} \tag{C5}$$

*is at least*

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}| - q + r)!} \cdot \left(1 - \frac{q(q-1)}{(|\mathcal{X}| - 1)} - \frac{q(q-1)}{|\mathcal{X}|}\right)$$

*where $r$ is the number of independent equations of form $R_i = R_j$.*

*Proof.* By Lemma 7, The number of choices for $X_i$, $S_i$, $T_i$ satisfying (C1) is

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}| - q + r)!},$$

because (C1) does not depend on $S_i$, $T_i$, so these can be freely chosen.

Then, in order to find a lower bound for tuples satisfying all of (C1), ..., (C5), we have to find an upper bound for tuples satisfying (C1) but not some of (C2), ..., (C5). First, consider the case where (C1) holds but (C2) is not true.

Fix an arbitrary $i$, $j$ such that $1 \le i < j \le q$. Consider the case when (C1) holds and also $X_i = X_j$ is true. In the proof of Lemma 7, we may set $R_{i_1} = R_i$, and $R_{i_2} = R_j$. We have $|\mathcal{X}|$ choices for $f_1(R_{i_1})$, but once this is chosen, the value for $f_2(R_{i_2})$ is fixed due to the equation $X_i = X_j$. Therefore, there are at most

$$|\mathcal{X}| \cdot (|\mathcal{X}| - 2) \cdots (|\mathcal{X}| - (q-r-1)) = \frac{|\mathcal{X}|!}{(|\mathcal{X}| - q + r)! \cdot (|\mathcal{X}| - 1)}$$

choices in total. Since there are $q(q-1)/2$ choices for $i < j$, and $|\mathcal{X}|^{2q}$ unrestricted choices for $S_i$ and $T_i$, there are at most

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2(|\mathcal{X}| - 1)}$$

choices where (C1) is true but (C2) is false.

Next, consider the case when (C1) is true but (C3) is false. In this case, $X_i$ can be chosen just like Lemma 7, but, unrelated to the choices for $X_i$, the choices for $S_i$ should satisfy $S_i = S_j$ for some $i < j$. Therefore, the number of choices is at most

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2|\mathcal{X}|}.$$

We can argue almost identically for the case when (C1) is true but (C4) is false; the number of choices for this case is again at most

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2|\mathcal{X}|}$$

Finally, the analysis for the case when (C1) is true but (C5) is false can be handled identical to the case when (C1) is true but (C2) is false; the number is again at most

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2(|\mathcal{X}| - 1)}$$

Therefore, there are at least

$$\begin{aligned}
&\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}| - q + r)!} - \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2(|\mathcal{X}| - 1)} \\
&\qquad - \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2|\mathcal{X}|} \\
&\qquad - \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2|\mathcal{X}|} \\
&\qquad - \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q} \cdot q(q-1)}{(|\mathcal{X}| - q + r)! \cdot 2(|\mathcal{X}| - 1)} \\
= \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}| - q + r)!} &\cdot \left(1 - \frac{q(q-1)}{(|\mathcal{X}| - 1)} - \frac{q(q-1)}{|\mathcal{X}|}\right)
\end{aligned}$$

choices where all of (C1), ..., (C5) are true. □

Now we are ready to prove Theorem 4. The proof is similar to that of Theorem 3, but we have to be carefully introduce the extra variable $X_i$ into our probability estimation.

*Proof (Of Theorem 4).* Let's define

$$\begin{aligned}
P_1 &\stackrel{\text{def}}{=} \Pr[1 \leftarrow A(\Psi) \,|\, \Psi \leftarrow \Psi^3(f_1, f_2, f_3), \text{ where } f_i \stackrel{\$}{\leftarrow} \mathsf{Perm}(\mathcal{X})] \\
P_1^* &\stackrel{\text{def}}{=} \Pr[1 \leftarrow A(f) \,|\, f \stackrel{\$}{\leftarrow} \mathsf{Func}(\mathcal{X}^2)]
\end{aligned}$$

Note that by definition, $\mathsf{Adv}^{\text{CPA}}_{\Psi^3}(A) = |P_1 - P_1^*|$.

The queries of $A$ to its oracle $f$ have form $f(\tau_i)$. Let's denote by $\sigma_i$ the answer of the oracle to the query $f(\tau_i)$. Then $\tau_1$ is dependent only to $A$, and $\tau_2$ is dependent to $A$ and $\sigma_1$, and $\tau_3$ is dependent to $A$ and $\sigma_1$, $\sigma_2$, and so on. Finally $A(f)$, the answer of $A$ is dependent only to $A$ and $\sigma_1, \ldots, \sigma_q$; if $f' : \mathcal{X}^2 \to \mathcal{X}^2$ is another function such that $f'(\tau_i) = \sigma_i$, then $A$'s

queries to both $f$ and $f'$ would be identical, and the answers would be identical, therefore $A(f) = A(f')$.

Hence, if the queries of $A$ to its oracle $f$ are $\tau_i$, and if the answers it gets are $\sigma_i$, then we may write $A(\sigma_1, \ldots, \sigma_q)$, instead of $A(f)$. Let $N$ be the number of $q$-tuples $(\sigma_1, \ldots, \sigma_q)$ satisfying $1 \leftarrow A(\sigma_1, \ldots, \sigma_q)$. Then, If $N$ is the number of $\sigma_1, \ldots, \sigma_q$ such that $1 \leftarrow A(\sigma_1, \ldots, \sigma_q)$, then

$$\begin{aligned}
P_1^* &= \frac{\text{Number of } f \in \mathsf{Func}(\mathcal{X}^2) \text{ such that } 1 \leftarrow A(f)}{\text{Number of } f \in \mathsf{Func}(\mathcal{X}^2)} \\
&= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{\text{Number of } f \in \mathsf{Func}(\mathcal{X}^2) \text{ compatible with } \sigma_1, \ldots, \sigma_q}{\text{Number of } f \in \mathsf{Func}(\mathcal{X}^2)} \\
&= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{(|\mathcal{X}|^2)^{|\mathcal{X}|^2-q}}{(|\mathcal{X}|^2)^{|\mathcal{X}|^2}} \\
&= \frac{N}{|\mathcal{X}|^{2q}}
\end{aligned}$$

Then,

$$\begin{aligned}
P_1 &= \frac{\text{Number of } (f_1, f_2, f_3) \text{ such that } 1 \leftarrow A(\Psi^3(f_1, f_2, f_3))}{|\,\mathsf{Perm}(\mathcal{X})|^3} \\
&= \sum_{\substack{\sigma_1,\ldots,\sigma_q \\ 1 \leftarrow A(\sigma_1,\ldots,\sigma_q)}} \frac{\text{Number of } (f_1, f_2, f_3) \text{ compatible with } \sigma_1, \ldots, \sigma_q}{|\,\mathsf{Perm}(\mathcal{X})|^3} \\
&= \sum_{\substack{\sigma_i \\ 1 \leftarrow A(\sigma_i)}} \sum_{X_i/(C1)} \frac{\text{Number of } (f_1, f_2, f_3) \text{ compatible with } X_i, \sigma_i}{|\,\mathsf{Perm}(\mathcal{X})|^3} \\
&\geq \sum_{\substack{X_i,\sigma_i/(C1),\ldots,(C5) \\ 1 \leftarrow A(\sigma_i)}} \frac{\text{Number of } (f_1, f_2, f_3) \text{ compatible with } X_i, \sigma_i}{|\,\mathsf{Perm}(\mathcal{X})|^3} \\
&= \sum_{\substack{X_i,\sigma_i/(C1),\ldots,(C5) \\ 1 \leftarrow A(\sigma_i)}} \frac{(|\mathcal{X}| - q + r)! \cdot (|\mathcal{X}| - q)! \cdot (|\mathcal{X}| - q)!}{(|\mathcal{X}|!)^3} \qquad (\because \text{Lemma 6}) \\
&= (\text{No. of } X_i, \sigma_i, \text{ satisfying (C1), } \ldots, \text{ (C5) and } 1 \leftarrow A(\sigma_i)) \\
&\quad \cdot \frac{(|\mathcal{X}| - q + r)! \cdot (|\mathcal{X}| - q)! \cdot (|\mathcal{X}| - q)!}{(|\mathcal{X}|!)^3}
\end{aligned}$$

We have to estimate the number of $X_i$, $\sigma_i$ satisfying (C1), ..., (C5) and also $1 \leftarrow A(\sigma_i)$. By Lemma 7, There are

$$N \cdot \frac{|\mathcal{X}|!}{(|\mathcal{X}| - q + r)!}$$

choices for $X_i$, $\sigma_i$ satisfying (C1) and $1 \leftarrow A(\sigma_i)$. It is because that, for each $N$ choices of $\sigma_i$ with $1 \leftarrow A(\sigma_i)$, one can choose $X_i$ by Lemma 7.

By Lemma 7 and Lemma 8, There are at most

$$\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}| - q + r)!} \cdot \left( \frac{q(q-1)}{|\mathcal{X}| - 1} + \frac{q(q-1)}{|\mathcal{X}|} \right)$$

choices for $X_i$, $\sigma_i$ satisfying (C1) but not satisfying some of (C2), ..., (C5). Therefore, the number of $X_i$, $\sigma_i$ satisfying all of (C1), ..., (C5) and also $1 \leftarrow A(\sigma_i)$ is at least

$$\begin{aligned}
&N \cdot \frac{|\mathcal{X}|!}{(|\mathcal{X}|-q+r)!} - \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}|-q+r)!} \cdot \left( \frac{q(q-1)}{|\mathcal{X}|-1} + \frac{q(q-1)}{|\mathcal{X}|} \right) \\
=&\frac{|\mathcal{X}|!}{(|\mathcal{X}|-q+r)!} \left( N - |\mathcal{X}|^{2q} \left( \frac{q(q-1)}{|\mathcal{X}|-1} + \frac{q(q-1)}{|\mathcal{X}|} \right) \right) \\
=&\frac{|\mathcal{X}|!}{(|\mathcal{X}|-q+r)!} \left( |\mathcal{X}|^{2q} \cdot P_1^* - |\mathcal{X}|^{2q} \left( \frac{q(q-1)}{|\mathcal{X}|-1} + \frac{q(q-1)}{|\mathcal{X}|} \right) \right) \\
=&\frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}|-q+r)!} \left( P_1^* - \frac{q(q-1)}{|\mathcal{X}|-1} - \frac{q(q-1)}{|\mathcal{X}|} \right)
\end{aligned}$$

When we put this into the above, we get

$$\begin{aligned}
P_1 \geq\ & (\text{No. of } X_i, \sigma_i, \text{ satisfying (C1), ..., (C5) and } 1 \leftarrow A(\sigma_i)) \\
& \cdot \frac{(|\mathcal{X}|-q+r)! \cdot (|\mathcal{X}|-q)! \cdot (|\mathcal{X}|-q)!}{(|\mathcal{X}|!)^3} \\
=\ & \frac{|\mathcal{X}|! \cdot |\mathcal{X}|^{2q}}{(|\mathcal{X}|-q+r)!} \left( P_1^* - \frac{q(q-1)}{|\mathcal{X}|-1} - \frac{q(q-1)}{|\mathcal{X}|} \right) \cdot \frac{(|\mathcal{X}|-q+r)! \cdot ((|\mathcal{X}|-q)!)^2}{(|\mathcal{X}|!)^3} \\
=\ & \left( P_1^* - \frac{q(q-1)}{|\mathcal{X}|-1} - \frac{q(q-1)}{|\mathcal{X}|} \right) \left( \frac{|\mathcal{X}|^q \cdot (|\mathcal{X}|-q)!}{|\mathcal{X}|!} \right)^2 \\
\geq\ & P_1^* - \frac{q(q-1)}{|\mathcal{X}|-1} - \frac{q(q-1)}{|\mathcal{X}|}.
\end{aligned}$$

By switching the outputs 1 and 0 of $A$, we obtain

$$1 - P_1 \geq 1 - P_1^* - \frac{q(q-1)}{|\mathcal{X}|-1} - \frac{q(q-1)}{|\mathcal{X}|}.$$

These two inequalities prove the Theorem 4. □

## D Proof sketch of Theorems 6 and 7

In the proof of Theorem 3 in Appendix B, we used Theorem 8 crucially. For the balanced case, that is when $b = 2$, Theorem 8 estimates the transition probability for given input/output pairs for 4-round unbalanced quasi-Feistel permutation. When we choose pre- and post-processing permutations $P$, $Q$ randomly from pairwise independent distributions, we can prove the analogue of Theorem 8 for 2-round balanced quasi-Feistel network.

**Lemma 9.** *Let $x^{(i)} = (x_L^{(i)}, x_R^{(i)}) \in \mathcal{X}^2$, $1 \leq i \leq q$ be distinct inputs, and let $y^{(i)} = (y_L^{(i)}, y_R^{(i)}) \in \mathcal{X}^2$, $1 \leq i \leq q$ be distinct outputs.*

*Let $\mathcal{P}$, $\mathcal{Q}$ be pairwise independent distributions of permutations on $\mathcal{X}^2$. Let $f_1$, $f_2 \xleftarrow{\$} \mathsf{Func}(\mathcal{X})$, and let $P \xleftarrow{\$} \mathcal{P}$, $Q \xleftarrow{\$} \mathcal{Q}$.*

*Let's denote by $h$ the probability that $\forall i, 1 \leq i \leq q$,*

$$\Psi_{P,Q}^2(f_1, f_2)(x^{(i)}) = y^{(i)}.$$

*Then we have*

$$h \geq \frac{1}{|\mathcal{X}|^{2q}} \left( 1 - \frac{q(q-1)}{|\mathcal{X}|} \right).$$

*Remark 8.* Note that when $b = 2$, the inequality in the Theorem 8 is identical to the above inequality.

*Proof.* Let's define random variables $L_i$, $R_i$, $S_i$, $T_i$ on $\mathcal{X}$, $i = 1, \ldots, q$, by $(L_i, R_i) \leftarrow p(x^{(i)})$, $(S_i, T_i) \leftarrow q(y^{(i)})$.

Since $\mathcal{P}$ is pairwise independent distribution of permutations, we know that for any given $i \neq j$, the probability that $R_i = R_j$ is at most $1/|\mathcal{X}|$. So, the probability that $R_i$ are not distinct is at most $q(q-1)/(2|\mathcal{X}|)$. Hence, the probability that $R_i$ are distinct is at least

$$1 - \frac{q(q-1)}{2|\mathcal{X}|}.$$

Similarly, the probability that $S_i$ are distinct is again at least

$$1 - \frac{q(q-1)}{2|\mathcal{X}|}.$$

Now, under the condition that $R_i$ are distinct and $S_i$ are distinct, the probability that

$$S_i = \Gamma\left[\!\left[L_i \star f_1(R_i) \,|\, R_i\right]\!\right]$$
$$T_i = \Gamma\left[\!\left[R_i \star f_2(S_i) \,|\, S_i\right]\!\right]$$

holds for $\forall i = 1, \ldots, q$ is exactly $|\mathcal{X}|^{-q} \cdot |\mathcal{X}|^{-q}$. Combining all of the above, we get

$$h \geq \frac{1}{|\mathcal{X}|^{2q}} \left(1 - \frac{q(q-1)}{2|\mathcal{X}|}\right)^2 \geq \frac{1}{|\mathcal{X}|^{2q}} \left(1 - \frac{q(q-1)}{|\mathcal{X}|}\right).$$

□

Now the proof of Theorem 6 is simple; we argue essentially identical to the proof of Theorem 3, but use Lemma 9, instead of Theorem 8.

Then, the proof of Theorem 7 is also easy; we again estimate the transition probability as in Lemma 9, but this time we have to consider the probability that $R_i = S_j$. The rest of the proof is identical to that of Theorem 6.