On the Pseudorandomness of KASUMI Type Permutations *

Tetsu Iwata† Tohru Yagi‡ Kaoru Kurosawa†

† Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
E-mail: {iwata, kurosawa}@cis.ibaraki.ac.jp

‡Department of Communications and Integrated Systems,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro, Tokyo 152-8552, Japan

July 3, 2003.

Abstract. KASUMI is a block cipher which has been adopted as a standard of 3GPP. In this paper, we study the pseudorandomness of idealized KASUMI type permutations for adaptive adversaries. We show that

- the four round version is pseudorandom and
- the six round version is super-pseudorandom.

Key words: Cryptography, block cipher, KASUMI, pseudorandomness, provable security.

*A preliminary version of this paper appears in *The Eighth Australasian Conference on Information Security and Privacy, ACISP 2003* [5].

Contents

1 Introduction **1**
- 1.1 Pseudorandomness 1
- 1.2 KASUMI 1
- 1.3 Previous work (Non-adaptive) 1
- 1.4 Our contribution (Adaptive) 2
- 1.5 Flaw of the previous work 3

2 Preliminaries **3**
- 2.1 Notation 3
- 2.2 KASUMI type permutation [2] 3
- 2.3 Pseudorandom and super-pseudorandom permutations [8] 4

3 A four round KASUMI type permutation is pseudorandom **5**

4 Proofs of Lemma 3.1and Lemma 3.2 **7**
- 4.1 Proof of Lemma 3.1 7
- 4.2 Proof of Lemma 3.2 14

5 A six round KASUMI type permutation is super-pseudorandom **14**

6 Proof of Lemma 5.1 **15**

7 Conclusion **19**

References **20**

A Flaws in the proof of [6] **21**
- A.1 Flaws on Theorem 1 21
- A.2 Flaws on Theorem 3 22

1 Introduction

1.1 Pseudorandomness

Let R be a randomly chosen permutation and Ψ be a block cipher such that a key is randomly chosen. We then say that

- Ψ is pseudorandom if Ψ and R are indistinguishable and
- Ψ is super-pseudorandom if (Ψ, Ψ^{-1}) and (R, R^{-1}) are indistinguishable.

Luby and Rackoff studied the pseudorandomness of idealized Feistel permutations, where each round function is an independent (pseudo)random function. They proved that

- the three round version is pseudorandom and
- the four round version is super-pseudorandom

for adaptive adversaries [8].

1.2 KASUMI

KASUMI is a block cipher which has been adopted as a standard of 3GPP [2], where 3GPP is the body standardizing the next generation of mobile telephony. The structure of KASUMI is illustrated in Fig. 1. (See [1] for details.)

- The overall structure of KASUMI is a Feistel permutation.
- Each round function consists of two functions, FL function and FO function.
- Each FO function consists of a three round MISTY type permutation, where each round function is called an FI function.
- Each FI function consists of a four round MISTY type permutation.

The initial security evaluation of KASUMI can be found in [3]. Blunden and Escott showed related key attacks on five round and six round KASUMI [4].

1.3 Previous work (Non-adaptive)

We idealize KASUMI as follows.

- Each FL function is ignored. (In [7], the authors stated that the security of KASUMI is mainly based on FO functions.)
- Each FI function is idealized by an independent (pseudo)random permutation.

We call such an idealized KASUMI a "KASUMI type permutation."

However, we do not assume that each FO function is a random permutation. This implies that we can not apply the result of Luby and Rackoff to KASUMI type permutations. (Indeed, Sakurai and Zheng showed that a three round MISTY type permutation is not pseudorandom [11].)

Kang et al. then showed that

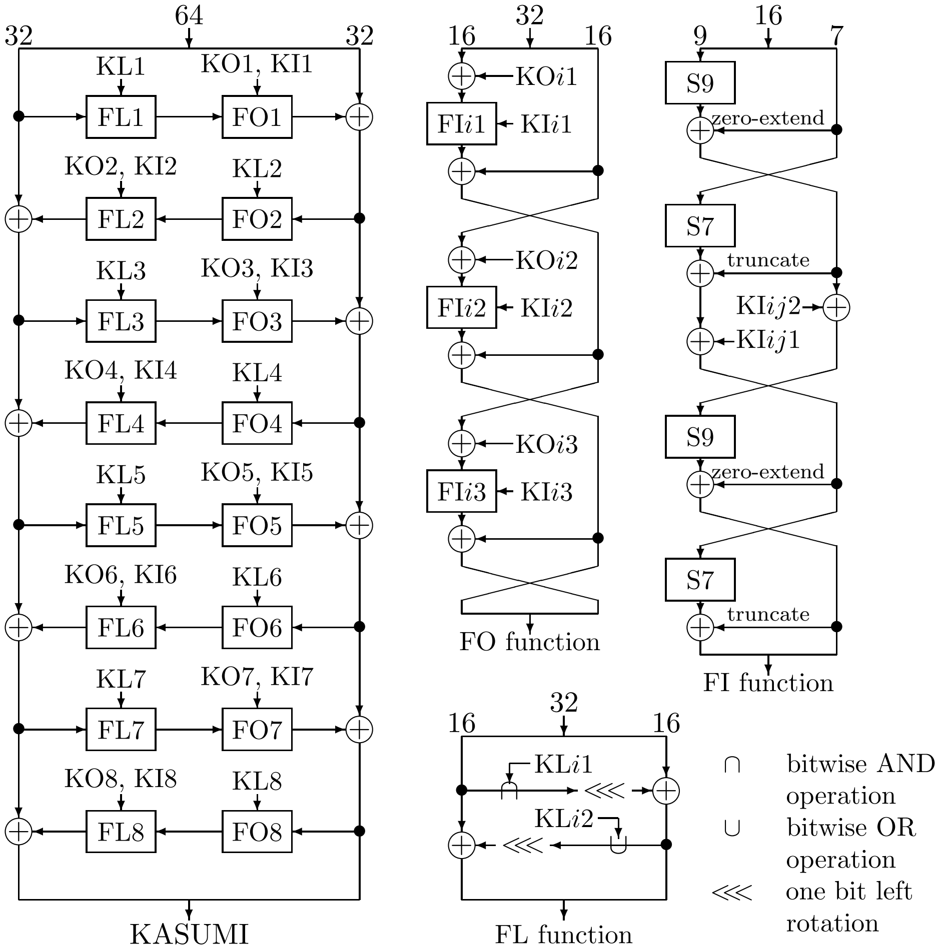

Fig. 1. KASUMI

- the three round version is not pseudorandom and
- the four round version is pseudorandom

for non-adaptive adversaries [7].

1.4 Our contribution (Adaptive)

In this paper, we study the pseudorandomness of KASUMI type permutations for adaptive adversaries. We prove that

- the four round version is pseudorandom and
- the six round version is super-pseudorandom.

See the following table, where $\times$ comes from [7], $\bigcirc^1$ comes from [7] and $\bigcirc^2$ is proved in this paper.

Table 1. Summary of the previous results and our contributions.

Number of rounds	Three	Four	Five	Six
Pseudorandomness (non-adaptive)	$\times$	$\bigcirc^1$	$\bigcirc^1$	$\bigcirc^1$
Pseudorandomness	$\times$	$\bigcirc^2$	$\bigcirc^2$	$\bigcirc^2$
Super-pseudorandomness	$\times$	?	?	$\bigcirc^2$

(We cannot idealize MISTY1 [9, 10] like KASUMI type permutations because each FI function of MISTY1 is a three round MISTY type permutation and three round MISTY type permutation is not pseudorandom [11].)

1.5 Flaw of the previous work

Kang et al. claimed that the four round KASUMI type permutation is pseudorandom for adaptive adversaries [6]. However, we show that their proof is wrong in Appendix A.

2 Preliminaries

2.1 Notation

For a bit string $x \in \{0,1\}^{2n}$, we denote the first (left) n bits of x by x_L and the last (right) n bits of x by x_R. Similarly, for a bit string $x \in \{0,1\}^{4n}$, we denote the first (left) n bits of x by x_{LL}, the next n bits of x by x_{LR}, the third n bits of x by x_{RL}, and the last (right) n bits of x by x_{RR}. That is, $x = (x_{LL}, x_{LR}, x_{RL}, x_{RR})$. For a set of l-bit strings $\{x^{(i)} \mid x^{(i)} \in \{0,1\}^l\}_{1 \le i \le q}$, we say $\{x^{(i)}\}_{1 \le i \le q}$ *are distinct* to mean $x^{(i)} \neq x^{(j)}$ for $1 \le \forall i < \forall j \le q$.

If S is a set, then $s \overset{R}{\leftarrow} S$ denotes the process of picking an element from S uniformly at random.

Denote by P_n the set of all permutations over $\{0,1\}^n$, which consists of $(2^n)!$ permutations in total. For functions f and g, $g \circ f$ denotes the function $x \mapsto g(f(x))$.

2.2 KASUMI type permutation [2]

We define KASUMI type permutations as follows.

Definition 2.1 (The basic KASUMI type permutation) *Let $x \in \{0,1\}^{4n}$. For any permutations $p_1, p_2, p_3 \in P_n$, define the basic KASUMI type permutation $\psi_{p_1,p_2,p_3} \in P_{4n}$ as*

$$\psi_{p_1,p_2,p_3}(x) \overset{\text{def}}{=} y \ ,$$

where

$$\begin{cases} y_{LL} \overset{\text{def}}{=} x_{RL}, \\ y_{LR} \overset{\text{def}}{=} x_{RR}, \\ y_{RL} \overset{\text{def}}{=} x_{RL} \oplus p_1(x_{RR}) \oplus p_2(x_{RL}) \oplus p_3(x_{RL} \oplus p_1(x_{RR})) \oplus x_{LL}, \ \textit{and} \\ y_{RR} \overset{\text{def}}{=} x_{RL} \oplus p_1(x_{RR}) \oplus p_2(x_{RL}) \oplus x_{LR}. \end{cases}$$

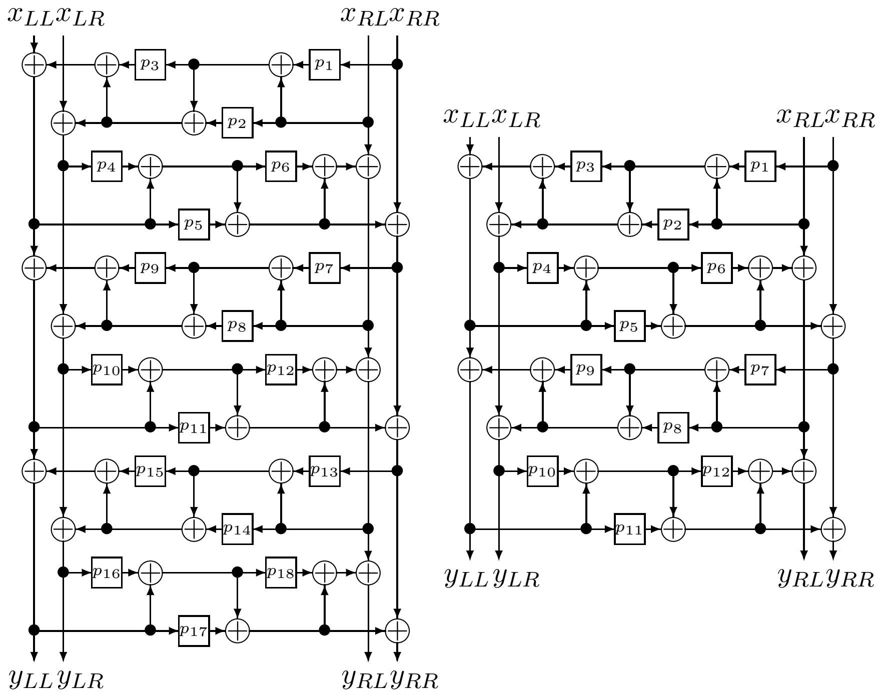

Fig. 2. A six round KASUMI type permutation $\psi(p_1,\dots,p_{18})$ (left) and a four round KASUMI type permutation $\psi(p_1,\dots,p_{15})$ (right).

Note that it is a permutation since $\psi^{-1}_{p_1,p_2,p_3}(y) = x$, where

$$\begin{cases} x_{LL} = y_{LL} \oplus p_1(y_{LR}) \oplus p_2(y_{LL}) \oplus p_3(y_{LL} \oplus p_1(y_{LR})) \oplus y_{RL}, \\ x_{LR} = y_{LL} \oplus p_1(y_{LR}) \oplus p_2(y_{LL}) \oplus y_{RR}, \\ x_{RL} = y_{LL}, \text{ and} \\ x_{RR} = y_{LR}. \end{cases}$$

Definition 2.2 (The r round KASUMI type permutation) *Let $r \geq 1$ be an integer, and $p_1, p_2, \dots, p_{3r} \in P_n$ be permutations.*

Define the r round KASUMI type permutation $\psi(p_1, p_2, \dots, p_{3r}) \in P_{4n}$ as

$$\psi(p_1, p_2, \dots, p_{3r}) \stackrel{\text{def}}{=} \psi_{p_{3r-2},p_{3r-1},p_{3r}} \circ \psi_{p_{3r-5},p_{3r-4},p_{3r-3}} \circ \cdots \circ \psi_{p_1,p_2,p_3} \ .$$

See Fig. 2 for illustrations. For simplicity, swaps are omitted.

2.3 Pseudorandom and super-pseudorandom permutations [8]

Our adaptive adversary $\mathcal{A}$ is modeled as a Turing machine that has black-box access to an oracle (or oracles). The computational power of $\mathcal{A}$ is unlimited, but the total number of oracle calls is limited to a parameter q. After making at most q queries to the oracle(s) adaptively, $\mathcal{A}$ outputs a bit.

The pseudorandomness of a block cipher Ψ over $\{0,1\}^{4n}$ captures its computational indistinguishability from P_{4n}, where the adversary is given access to the forward direction of the permutation. In other words, it measures security of a block cipher against adaptive chosen plaintext attack.

Definition 2.3 (Advantage, prp) *Let a block cipher Ψ be a family of permutations over $\{0,1\}^{4n}$. Let $\mathcal{A}$ be an adversary. Then $\mathcal{A}$'s advantage is defined by*

$$\mathtt{Adv}_{\Psi}^{\mathsf{prp}}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \left| \Pr(\psi \stackrel{R}{\leftarrow} \Psi : \mathcal{A}^{\psi} = 1) - \Pr(R \stackrel{R}{\leftarrow} P_{4n} : \mathcal{A}^{R} = 1) \right| \enspace .$$

The notation $\mathcal{A}^{\psi}$ indicates $\mathcal{A}$ with an oracle which, in response to a query x, returns $y \leftarrow \psi(x)$. The notation $\mathcal{A}^{R}$ indicates $\mathcal{A}$ with an oracle which, in response to a query x, returns $y \leftarrow R(x)$.

The super-pseudorandomness of a block cipher Ψ over $\{0,1\}^{4n}$ captures its computational indistinguishability from P_{4n}, where the adversary is given access to both directions of the permutation. In other words, it measures security of a block cipher against adaptive chosen plaintext and chosen ciphertext attacks.

Definition 2.4 (Advantage, sprp) *Let a block cipher Ψ be a family of permutations over $\{0,1\}^{4n}$. Let $\mathcal{A}$ be an adversary. Then $\mathcal{A}$'s advantage is defined by*

$$\mathtt{Adv}_{\Psi}^{\mathsf{sprp}}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \left| \Pr(\psi \stackrel{R}{\leftarrow} \Psi : \mathcal{A}^{\psi,\psi^{-1}} = 1) - \Pr(R \stackrel{R}{\leftarrow} P_{4n} : \mathcal{A}^{R,R^{-1}} = 1) \right| \enspace .$$

The notation $\mathcal{A}^{\psi,\psi^{-1}}$ indicates $\mathcal{A}$ with an oracle which, in response to a query $(+,x)$, returns $y \leftarrow \psi(x)$, and in response to a query $(-,y)$, returns $x \leftarrow \psi^{-1}(y)$. The notation $\mathcal{A}^{R,R^{-1}}$ indicates $\mathcal{A}$ with an oracle which, in response to a query $(+,x)$, returns $y \leftarrow R(x)$, and in response to a query $(-,y)$, returns $x \leftarrow R^{-1}(y)$.

3 A four round KASUMI type permutation is pseudorandom

Theorem 3.1 *For $1 \le i \le 12$, let $p_i \in P_n$ be a random permutation. Let $\psi = \psi(p_1,\ldots,p_{12})$ be a four round KASUMI type permutation, $R \in P_{4n}$ be a random permutation, and $\Psi \stackrel{\mathrm{def}}{=} \{\psi \mid \psi = \psi(p_1,\ldots,p_{12}), p_i \in P_n \text{ for } 1 \le i \le 12\}$.*

Then for any adversary $\mathcal{A}$ that makes at most q queries in total,

$$\mathtt{Adv}_{\Psi}^{\mathsf{prp}}(\mathcal{A}) \le \frac{15}{2} \cdot \frac{q(q-1)}{2^n - 1} \enspace .$$

Proof. Let $\mathcal{O}$ be either R or ψ. The adversary $\mathcal{A}$ has oracle access to $\mathcal{O}$. $\mathcal{A}$ can make a query x and the oracle returns $y = \mathcal{O}(x)$. For the i-th query $\mathcal{A}$ makes to $\mathcal{O}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{4n} \times \{0,1\}^{4n}$, where $\mathcal{A}$'s query was $x^{(i)}$ and the answer it got was $y^{(i)}$. Define view v of $\mathcal{A}$ as $v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$. We say that $v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$ is a *possible view* if there exists some permutation $p \in P_{4n}$ such that $p(x^{(i)}) = y^{(i)}$ for $1 \le \forall i \le q$ (or, equivalently, $v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$ is a possible view if $\{x^{(i)}\}_{1 \le i \le q}$ are distinct and $\{y^{(i)}\}_{1 \le i \le q}$ are distinct).

Since $\mathcal{A}$ is computationally unbounded, we may without loss of generality assume that $\mathcal{A}$ is deterministic. This implies that for every $1 \le i \le q$ the i-th query $x^{(i)}$ is fully determined by the first $i-1$ query-answer pairs, and the final output of $\mathcal{A}$ (0 or 1) depends only on v. Therefore, there exists a function $\mathcal{C}_{\mathcal{A}}(\cdot)$ such that

$$\begin{cases} \mathcal{C}_{\mathcal{A}}(x^{(1)}, y^{(1)}, \ldots, x^{(i-1)}, y^{(i-1)}) = x^{(i)} \text{ for } 1 \le i \le q \text{ and} \\ \mathcal{C}_{\mathcal{A}}(v) = \mathcal{A}\text{'s final output.} \end{cases}$$

Let $\boldsymbol{v}_{one} \stackrel{\text{def}}{=} \{v \mid \mathcal{C}_{\mathcal{A}}(v) = 1\}$ and $N_{one} \stackrel{\text{def}}{=} \#\boldsymbol{v}_{one}$. Further, we let $\boldsymbol{v}_{good}$ be a set of all possible view $v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$ which satisfies the following four conditions:

- $\mathcal{C}_{\mathcal{A}}(v) = 1$,
- $\{y_{LL}^{(i)}\}_{1 \le i \le q}$ are distinct,
- $\{y_{LR}^{(i)}\}_{1 \le i \le q}$ are distinct, and
- $\{x_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LL}^{(i)} \oplus y_{LR}^{(i)}\}_{1 \le i \le q}$ are distinct.

We also let $N_{good} \stackrel{\text{def}}{=} \#\boldsymbol{v}_{good}$.

Evaluation of p_R. We first evaluate $p_R \stackrel{\text{def}}{=} \Pr(R \stackrel{R}{\leftarrow} P_{4n} : \mathcal{A}^R = 1)$. We have $p_R = \frac{\#\{R \mid \mathcal{A}^R = 1\}}{(2^{4n})!}$. For each $v \in \boldsymbol{v}_{one}$, the number of R such that

$$R(x^{(i)}) = y^{(i)} \text{ for } 1 \le \forall i \le q \tag{1}$$

is exactly $(2^{4n} - q)!$. Therefore, we have $p_R = \sum_{v \in \boldsymbol{v}_{one}} \frac{\#\{R \mid R \text{ satisfying (1)}\}}{(2^{4n})!} = N_{one} \cdot \frac{(2^{4n}-q)!}{(2^{4n})!}$.

Evaluation of p_ψ. We evaluate $p_\psi \stackrel{\text{def}}{=} \Pr(\psi \stackrel{R}{\leftarrow} \Psi : \mathcal{A}^{\psi, \psi^{-1}} = 1)$. Note that "$\psi \stackrel{R}{\leftarrow} \Psi$" is equivalent to "$p_i \stackrel{R}{\leftarrow} P_n$ for $1 \le i \le 12$ and then let $\psi \leftarrow \psi(p_1, \ldots, p_{12})$." We have $p_\psi = \frac{\#\{(p_1, \ldots, p_{12}) \mid \mathcal{A}^{\psi, \psi^{-1}} = 1\}}{\{(2^n)!\}^{12}}$.

We have the following lemma. A proof of this lemma is given in Section 4.1.

Lemma 3.1 (Main Lemma for $\psi(p_1, \ldots, p_{12})$) *For any fixed possible view*

$$v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$$

such that $\{y_{LL}^{(i)}\}_{1 \le i \le q}$ are distinct, $\{y_{LR}^{(i)}\}_{1 \le i \le q}$ are distinct, and $\{x_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LL}^{(i)} \oplus y_{LR}^{(i)}\}_{1 \le i \le q}$ are distinct, the number of $(p_1, \ldots, p_{12})$ which satisfies

$$\psi(x^{(i)}) = y^{(i)} \textit{ for } 1 \le \forall i \le q \tag{2}$$

is at least $\left(1 - \frac{6q(q-1)}{2^n - 1}\right) \cdot \{(2^n)!\}^8 \cdot \{(2^n - q)!\}^4$.

Then from Lemma 3.1, we have

$$\begin{aligned} p_\psi &\ge \sum_{v \in \boldsymbol{v}_{good}} \frac{\#\{(p_1, \ldots, p_{12}) \mid (p_1, \ldots, p_{12}) \text{ satisfying (2)}\}}{\{(2^n)!\}^{12}} \\ &\ge \sum_{v \in \boldsymbol{v}_{good}} \left(1 - \frac{6q(q-1)}{2^n - 1}\right) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \ . \end{aligned}$$

Now we have the following lemma. See Section 4.2 for a proof.

Lemma 3.2 $N_{good} \geq N_{one} - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}$.

From Lemma 3.2, we have

$$\begin{aligned} p_\psi &\geq \left(N_{one} - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}\right) \cdot \left(1 - \frac{6q(q-1)}{2^n-1}\right) \cdot \frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \\ &= \left(p_R - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1}\right) \cdot \left(1 - \frac{6q(q-1)}{2^n-1}\right) \cdot \frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n}-q)!\}} \ . \end{aligned}$$

Now it is easy to see that $\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n}-q)!\}} \geq 1$ (this can be shown easily by an induction on q). Then $p_\psi \geq \left(p_R - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1}\right) \cdot \left(1 - \frac{6q(q-1)}{2^n-1}\right) \geq p_R - \frac{15}{2} \cdot \frac{q(q-1)}{2^n-1}$. Applying the same argument to $1-p_\psi$ and $1-p_R$ yields that $1-p_\psi \geq 1-p_R - \frac{15}{2} \cdot \frac{q(q-1)}{2^n-1}$, and we have $|p_\psi - p_R| \leq \frac{15}{2} \cdot \frac{q(q-1)}{2^n-1}$.
Q.E.D.

From Theorem 3.1, it is straightforward to show that $\psi = \psi(p_1, \ldots, p_{12})$ is pseudorandom even if each p_i is a pseudorandom permutation by using a standard hybrid argument. For example, see [8].

4 Proofs of Lemma 3.1 and Lemma 3.2

4.1 Proof of Lemma 3.1

First, we need the following lemma.

Lemma 4.1 *For $1 \leq i \leq q$, let $X^{(i)} = (X_L^{(i)}, X_R^{(i)}) \in \{0,1\}^{2n}$ be fixed bit strings such that $\{X_L^{(i)}\}_{1 \leq i \leq q}$ are distinct and $\{X_R^{(i)}\}_{1 \leq i \leq q}$ are distinct. Similarly, for $1 \leq i \leq q$, let $Y^{(i)} = (Y_L^{(i)}, Y_R^{(i)}) \in \{0,1\}^{2n}$ be fixed bit strings such that $\{Y_L^{(i)} \oplus Y_R^{(i)}\}_{1 \leq i \leq q}$ are distinct. Let $P_1, P_2, P_3 \in P_n$ be permutations. Then the number of (P_1, P_2, P_3) such that*

- $P_1(X_L^{(i)}) \oplus X_R^{(i)} \oplus P_2(X_R^{(i)}) = Y_R^{(i)}$ *for* $1 \leq \forall i \leq q$, *and*
- $P_3(P_1(X_L^{(i)}) \oplus X_R^{(i)}) \oplus P_1(X_L^{(i)}) \oplus X_R^{(i)} \oplus P_2(X_R^{(i)}) = Y_L^{(i)}$ *for* $1 \leq \forall i \leq q$

is at least $\left(1 - \frac{q(q-1)}{2^n-1}\right) \cdot (2^n)! \cdot \{(2^n-q)!\}^2$.

See Fig. 3 for an illustration.

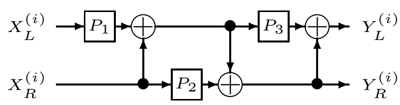

Fig. 3. Illustration of the conditions in Lemma 4.1.

Proof. First observe that the number of P_1 such that

$$P_1(X_L^{(i)}) \oplus X_R^{(i)} \oplus Y_R^{(i)} = P_1(X_L^{(j)}) \oplus X_R^{(j)} \oplus Y_R^{(j)} \text{ for } 1 \leq \exists i < \exists j \leq q \tag{3}$$

is at most $\binom{q}{2} \cdot \frac{\{(2^n)!\}}{2^n-1}$, since $X_L^{(i)} \neq X_L^{(j)}$ for $1 \leq \forall i < \forall j \leq q$.

Next we see that the number of P_1 such that

$$P_1(X_L^{(i)}) \oplus X_R^{(i)} = P_1(X_L^{(j)}) \oplus X_R^{(j)} \text{ for } 1 \leq \exists i < \exists j \leq q \tag{4}$$

is at most $\binom{q}{2} \cdot \frac{\{(2^n)!\}}{2^n-1}$, since $X_L^{(i)} \neq X_L^{(j)}$ for $1 \leq \forall i < \forall j \leq q$.

We now fix any P_1 which does *not* satisfy either (3) or (4). We have at least $(2^n)! \cdot \left(1 - \frac{q(q-1)}{2^n-1}\right)$ choice of such P_1. This implies that P_1 is fixed in such a way that $\{P_1(X_L^{(i)}) \oplus X_R^{(i)} \oplus Y_R^{(i)}\}_{1 \leq i \leq q}$ (which are the outputs of P_2) are distinct, and $\{P_1(X_L^{(i)}) \oplus X_R^{(i)}\}_{1 \leq i \leq q}$ (which are the inputs to P_3) are distinct.

We know from our condition that $\{X_R^{(i)}\}_{1 \leq i \leq q}$ (which are the inputs of P_2) are distinct, and $\{Y_L^{(i)} \oplus Y_R^{(i)}\}_{1 \leq i \leq q}$ (which are the outputs of P_3) are distinct. Therefore, we have exactly $(2^n - q)!$ choice of P_2 and $(2^n - q)!$ choice of P_3 for any such fixed P_1.

Q.E.D.

Now for $1 \leq i \leq q$ and $1 \leq j \leq 12$, let $I_j^{(i)}$ denote the input to p_i when the input to ϕ is $x^{(i)}$ and the output is $y^{(i)}$. Similarly, let $O_j^{(i)}$ denote the output of p_i when the input to ϕ is $x^{(i)}$ and the output is $y^{(i)}$.

We next have the following lemma.

Lemma 4.2 *For any fixed possible view $v = \langle (x^{(1)}, y^{(1)}), \ldots, (x^{(q)}, y^{(q)}) \rangle$, the number of (p_1, p_2, p_3, p_4) such that*

$$I_6^{(i)} = I_6^{(j)} \text{ or } I_6^{(i)} \oplus x_{RR}^{(i)} = I_6^{(j)} \oplus x_{RR}^{(j)}, \text{ for } 1 \leq \exists i < \exists j \leq q \tag{5}$$

is at most $\frac{2q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4$.

Proof. First, we fix i and j such that $1 \leq i < j \leq q$, and consider the condition

$$I_6^{(i)} = I_6^{(j)} \text{ or } I_6^{(i)} \oplus x_{RR}^{(i)} = I_6^{(j)} \oplus x_{RR}^{(j)} \tag{6}$$

in the following four cases:

Case $x_{RR}^{(i)} \neq x_{RR}^{(j)}$. First, consider the condition

$$p_1(x_{RR}^{(i)}) \oplus x_{RL}^{(i)} \oplus x_{LR}^{(i)} = p_1(x_{RR}^{(j)}) \oplus x_{RL}^{(j)} \oplus x_{LR}^{(j)} \ . \tag{7}$$

The number of p_1 which satisfies (7) is at most $\frac{(2^n)!}{2^n-1}$ since $x_{RR}^{(i)} \neq x_{RR}^{(j)}$, and thus we have

$$\#\{(p_1, \ldots, p_4) \mid (p_1, \ldots, p_4) \text{ satisfies both (6) and (7)}\} \leq \frac{\{(2^n)!\}^4}{2^n - 1} \ . \tag{8}$$

Next, consider any p_1 which does not satisfy (7), that is,

$$p_1(x_{RR}^{(i)}) \oplus x_{RL}^{(i)} \oplus x_{LR}^{(i)} \neq p_1(x_{RR}^{(j)}) \oplus x_{RL}^{(j)} \oplus x_{LR}^{(j)} \ . \tag{9}$$

For this p_1, we consider the condition

$$p_2(x_{RL}^{(i)}) \oplus p_1(x_{RR}^{(i)}) \oplus x_{RL}^{(i)} \oplus x_{LR}^{(i)} = p_2(x_{RL}^{(j)}) \oplus p_1(x_{RR}^{(j)}) \oplus x_{RL}^{(j)} \oplus x_{LR}^{(j)} \ , \tag{10}$$

which is equivalent to $I_4^{(i)} = I_4^{(j)}$. Since (9) holds, the number of p_2 which satisfies (10) is at most $\frac{(2^n)!}{2^n-1}$, and thus we have

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6), (9) and (10)}\} \le \frac{\{(2^n)!\}^4}{2^n-1} \ . \tag{11}$$

Next, consider any p_1 which satisfies (9), and any p_2 which does not satisfy (10). That is,

$$p_2(x_{RL}^{(i)}) \oplus p_1(x_{RR}^{(i)}) \oplus x_{RL}^{(i)} \oplus x_{LR}^{(i)} \ne p_2(x_{RL}^{(j)}) \oplus p_1(x_{RR}^{(j)}) \oplus x_{RL}^{(j)} \oplus x_{LR}^{(j)} \ , \tag{12}$$

which is equivalent to $I_4^{(i)} \ne I_4^{(j)}$. For these p_1, p_2 and any p_3, the number of p_4 which satisfies

$$p_4(I_4^{(i)}) \oplus I_5^{(i)} = p_4(I_4^{(j)}) \oplus I_5^{(i)} \ , \tag{13}$$

which is equivalent to $I_6^{(i)} = I_6^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, and the number of p_4 which satisfies

$$p_4(I_4^{(i)}) \oplus I_5^{(i)} \oplus x_{RR}^{(i)} = p_4(I_4^{(j)}) \oplus I_5^{(i)} \oplus x_{RR}^{(j)} \ , \tag{14}$$

which is equivalent to $I_6^{(i)} \oplus x_{RR}^{(i)} = I_6^{(j)} \oplus x_{RR}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$. Therefore

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6), (9) and (12)}\} \le \frac{2 \cdot \{(2^n)!\}^4}{2^n-1} \ . \tag{15}$$

Thus, from (8), (11) and (15), we have

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6)}\} \le \frac{4 \cdot \{(2^n)!\}^4}{2^n-1} \ . \tag{16}$$

Case $x_{RL}^{(i)} \ne x_{RL}^{(j)}$ and $x_{RR}^{(i)} = x_{RR}^{(j)}$. For any p_1, the number of p_2 which satisfies (10) is at most $\frac{(2^n)!}{2^n-1}$ since $x_{RL}^{(i)} \ne x_{RL}^{(j)}$, and thus we have

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6) and (10)}\} \le \frac{\{(2^n)!\}^4}{2^n-1} \ . \tag{17}$$

Next, for any p_1, any p_2 which satisfies (12), and any p_3, the number of p_4 which satisfies (13) is at most $\frac{(2^n)!}{2^n-1}$. Note that (13) is equivalent to (14) in this case. Therefore we have

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6) and (12)}\} \le \frac{\{(2^n)^{2^n}\}^4}{2^n} \ . \tag{18}$$

Thus, from (17) and (18), we have

$$\#\{(p_1,\ldots,p_4) \mid (p_1,\ldots,p_4) \text{ satisfies (6)}\} \le \frac{2 \cdot \{(2^n)!\}^4}{2^n-1} \ . \tag{19}$$

Case $x_{LR}^{(i)} \neq x_{LR}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$, and $x_{RR}^{(i)} = x_{RR}^{(j)}$. For any p_1 and any p_2, (12) is satisfied. Therefore, for any p_1, any p_2, and any p_3, the number of p_4 which satisfies (13) (which is equivalent to (14)) is at most $\frac{(2^n)!}{2^n-1}$. Therefore we have

$$\#\{(p_1,p_2,p_3,p_4) \mid (p_1,p_2,p_3,p_4) \text{ satisfies } (6)\} \leq \frac{\{(2^n)!\}^4}{2^n-1} \ . \tag{20}$$

Case $x_{LL}^{(i)} \neq x_{LL}^{(j)}$, $x_{LR}^{(i)} = x_{LR}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$, and $x_{RR}^{(i)} = x_{RR}^{(j)}$. There exists no p_1, p_2, p_3, and p_4 that satisfies (6). Therefore we have

$$\#\{(p_1,p_2,p_3,p_4) \mid (p_1,p_2,p_3,p_4) \text{ satisfies } (6)\} = 0 \ . \tag{21}$$

Completing the proof. By taking the maximum of (16), (19), (20) and (21),

$$\#\{(p_1,\dots,p_4) \mid (p_1,\dots,p_4) \text{ satisfies } (6)\} \leq \frac{4 \cdot \{(2^n)!\}^4}{2^n-1} \ . \tag{22}$$

for any case.

From (22) and since we have $\binom{q}{2}$ choice of i and j the lemma follows.

Q.E.D.

Next we show the following lemma.

Lemma 4.3 *For any fixed possible view $v = \langle (x^{(1)},y^{(1)}),\dots,(x^{(q)},y^{(q)})\rangle$ which satisfies the condition of Lemma 3.1, the number of (p_1,p_2,p_3,p_4) such that*

$$O_9^{(i)} = O_9^{(j)} \text{ for } 1 \leq \exists i < \exists j \leq q \tag{23}$$

is at most $\frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4$.

Proof. First, we fix i and j such that $1 \leq i < j \leq q$, and consider $O_9^{(i)} = O_9^{(j)}$. Now observe that for any p_1 and p_2, $O_9^{(i)} = O_9^{(j)}$ is equivalent to the following condition:

$$p_3(I_3^{(i)}) \oplus x_{LL}^{(i)} \oplus y_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LR}^{(i)} = p_3(I_3^{(j)}) \oplus x_{LL}^{(j)} \oplus y_{LL}^{(j)} \oplus x_{LR}^{(j)} \oplus y_{LR}^{(j)} \ . \tag{24}$$

Then the number of p_3 which satisfies (24) is at most $\frac{(2^n)!}{2^n-1}$, since $x_{LL}^{(i)} \oplus y_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LR}^{(i)} \neq x_{LL}^{(j)} \oplus y_{LL}^{(j)} \oplus x_{LR}^{(j)} \oplus y_{LR}^{(j)}$.

Therefore, we have

$$\#\{(p_1,\dots,p_4) \mid (p_1,\dots,p_4) \text{ satisfies } (6)\} \leq \frac{\{(2^n)!\}^4}{2^n-1}$$

and since we have $\binom{q}{2}$ choice of i and j the lemma follows.

Q.E.D.

We now prove Lemma 3.1.

Proof of Lemma 3.1. Initially, $x^{(1)},\dots,x^{(q)},y^{(1)},\dots,y^{(q)}$ are fixed. See Fig. 4.

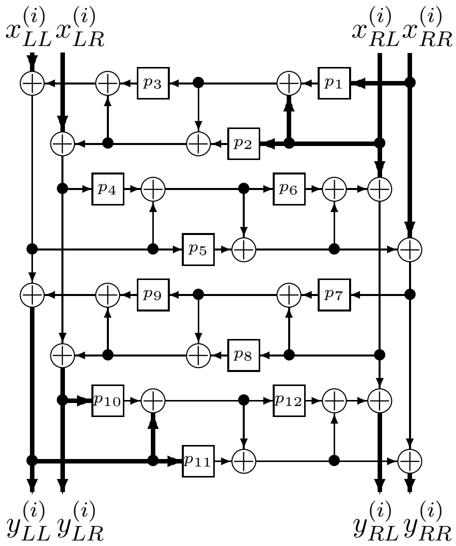

Fig. 4. $x^{(i)}$ and $y^{(i)}$ are fixed.

Number of $(p_1, \ldots, p_4)$**.** From Lemma 4.2 and 4.3, the number of $(p_1, \ldots, p_4)$ such that:

- $I_6^{(i)} \neq I_6^{(j)}$, $I_6^{(i)} \oplus x_{RR}^{(i)} \neq I_6^{(j)} \oplus x_{RR}^{(j)}$, and $O_9^{(i)} \neq O_9^{(j)}$ for $1 \leq \forall i < \forall j \leq q$,

is at least $\{(2^n)!\}^4 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4 - \frac{2q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4$. Fix any $(p_1, \ldots, p_4)$ which satisfy these three conditions. See Fig. 5.

Number of p_5**.** For any fixed i and j such that $1 \leq i < j \leq q$, the number of p_5 such that $p_5(I_5^{(i)}) \oplus I_6^{(i)} \oplus x_{RR}^{(i)} = p_5(I_5^{(j)}) \oplus I_6^{(j)} \oplus x_{RR}^{(j)}$, which is equivalent to $I_7^{(i)} = I_7^{(j)}$, is at most $\frac{\{(2^n)!\}^4}{2^n-1}$ since $I_6^{(i)} \oplus x_{RR}^{(i)} \neq I_6^{(j)} \oplus x_{RR}^{(j)}$. Then the number of p_5 such that

- $I_7^{(i)} \neq I_7^{(j)}$ for $1 \leq \forall i < \forall j \leq q$

is at least $(2^n)! - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any such p_5. See Fig. 6.

Number of p_6**.** For any fixed i and j such that $1 \leq i < j \leq q$, the number of p_6 which satisfies $p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_5^{(i)} \oplus x_{RL}^{(i)} = p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_5^{(j)} \oplus x_{RL}^{(j)}$, which is equivalent to $I_8^{(i)} = I_8^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Similarly, the number of p_6 which satisfies $p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_5^{(i)} \oplus x_{RL}^{(i)} \oplus I_7^{(i)} \oplus y_{RL}^{(i)} \oplus y_{RR}^{(i)} = p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_5^{(j)} \oplus x_{RL}^{(j)} \oplus I_7^{(j)} \oplus y_{RL}^{(j)} \oplus y_{RR}^{(j)}$, which is equivalent to $O_{12}^{(i)} = O_{12}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Then, the number of p_6 which satisfies:

- $I_8^{(i)} \neq I_8^{(j)}$ and $O_{12}^{(i)} \neq O_{12}^{(j)}$ for $1 \leq \forall i < \forall j \leq q$,

is at least $(2^n)! - \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any p_6 which satisfy the above two conditions. See Fig. 7.

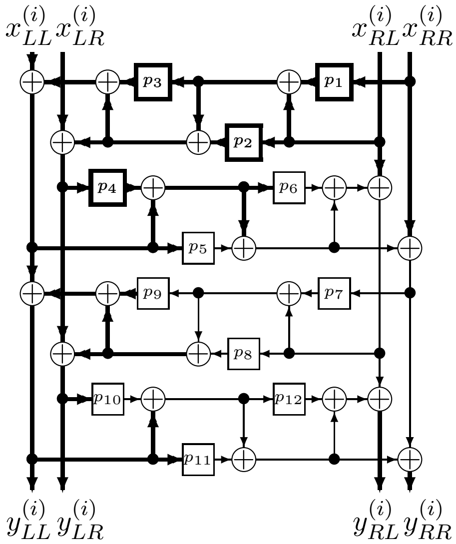

Fig. 5. $p_1, \ldots, p_4$ are fixed.

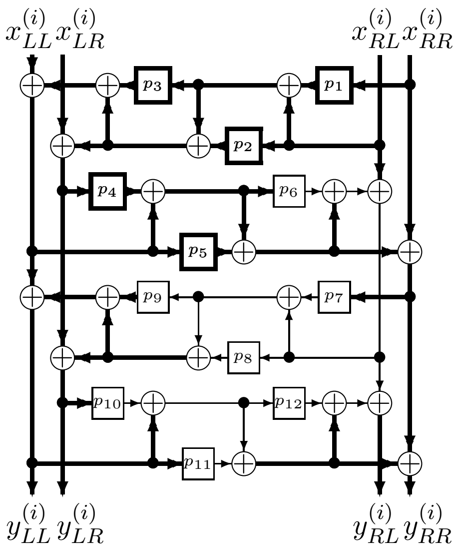

Fig. 6. p_5 is fixed.

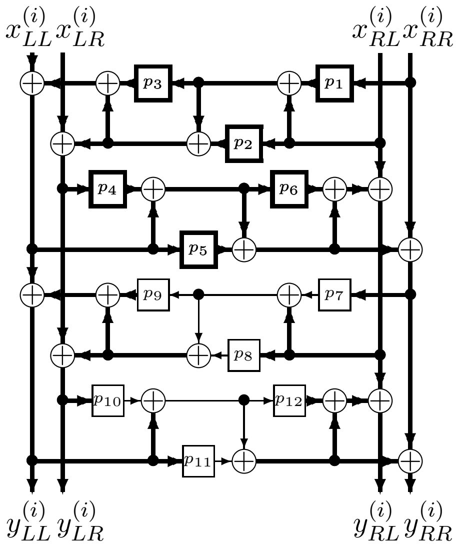

Fig. 7. p_6 is fixed.

Number of $(p_7, \ldots, p_{12})$**.** Now $p_1, \ldots, p_6$ are fixed in such a way that $\{I_7^{(i)}\}_{1\le i\le q}$ are distinct, $\{I_8^{(i)}\}_{1\le i\le q}$ are distinct, $\{O_9^{(i)}\}_{1\le i\le q}$ are distinct and $\{O_{12}^{(i)}\}_{1\le i\le q}$ are distinct. We know from our condition that $\{I_{10}^{(i)}\}_{1\le i\le q}$ are distinct and $\{I_{11}^{(i)}\}_{1\le i\le q}$ are distinct.

Then we have at least $\left(1 - \frac{q(q-1)}{2^n-1}\right) \cdot (2^n)! \cdot \{(2^n - q)!\}^2$ choice of (p_7, p_8, p_9) by applying Lemma 4.1. That is, $X_L^{(i)}$, $X_R^{(i)}$, $Y_L^{(i)} \oplus Y_R^{(i)}$, P_1, P_2 and P_3 in Lemma 4.1 correspond to $I_7^{(i)}$, $I_8^{(i)}$, $O_9^{(i)}$, p_7, p_8 and p_9 respectively.

Similarly, from Lemma 4.1 we have at least $\left(1 - \frac{q(q-1)}{2^n-1}\right) \cdot (2^n)! \cdot \{(2^n - q)!\}^2$ choice of (p_{10}, p_{11}, p_{12}). Note that $X_L^{(i)}$, $X_R^{(i)}$, $Y_L^{(i)} \oplus Y_R^{(i)}$, P_1, P_2 and P_3 in Lemma 4.1 correspond to $I_{10}^{(i)}$, $I_{11}^{(i)}$, $O_{12}^{(i)}$, p_{10}, p_{11} and p_{12} respectively.

Completing the proof. To summarize, we have:

- at least $\left(1 - \frac{5}{2} \cdot \frac{q(q-1)}{2^n-1}\right) \cdot \{(2^n)!\}^4$ choice of $p_1, \ldots, p_4$,
- at least $(2^n)! - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot (2^n)!$ choice of p_5 when $p_1, \ldots, p_4$ are fixed,
- at least $(2^n)! - \frac{q(q-1)}{2^n-1} \cdot (2^n)!$ choice of p_6 when $p_1, \ldots, p_5$ are fixed, and
- at least $\left(1 - \frac{q(q-1)}{2^n-1}\right)^2 \cdot \{(2^n)!\}^2 \cdot \{(2^n - q)!\}^4$ choice of $p_7 \ldots, p_{12}$ when $p_1, \ldots, p_6$ are fixed.

Then, the number of $(p_1, \ldots, p_{12})$ which satisfy (2) is at least

$$\begin{aligned} &\left(1 - \frac{5}{2} \cdot \frac{q(q-1)}{2^n-1}\right) \cdot \left(1 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1}\right) \cdot \left(1 - \frac{q(q-1)}{2^n-1}\right)^3 \cdot \{(2^n)!\}^8 \cdot \{(2^n - q)!\}^4 \\ &\quad \ge \left(1 - \frac{6q(q-1)}{2^n-1}\right) \cdot \{(2^n)!\}^8 \cdot \{(2^n - q)!\}^4 \ . \end{aligned}$$

This concludes the proof of the lemma. Q.E.D.

4.2 Proof of Lemma 3.2

For any fixed i and j such that $1 \le i < j \le q$, the number of $\{y^{(i)}\}_{1\le i\le q}$ such that $y_{LL}^{(i)} = y_{LL}^{(j)}$ is at most $\frac{2^{3n}-1}{2^{4n}-(j-1)} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!} \le \frac{2^{3n}-1}{2^{4n}-(q-1)} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}$, since we have: $(2^{4n})(2^{4n}-1)\cdots(2^{4n}-(j-2))$ choice of $y^{(1)}, \dots, y^{(j-1)}$, which uniquely determines $y_{LL}^{(j)} = y_{LL}^{(i)}$; at most $2^{3n}-1$ choice of $y_{LR}^{(j)}, y_{RL}^{(j)}, y_{RR}^{(j)}$; and $(2^{4n}-j)(2^{4n}-j-1)\cdots(2^{4n}-(q-1))$ choice of $y^{(j+1)}, \dots, y^{(q)}$.

Similarly, for any fixed i and j such that $1 \le i < j \le q$, the number of $\{y^{(i)}\}_{1\le i\le q}$ such that $y_{LR}^{(i)} = y_{LR}^{(j)}$ is at most $\frac{2^{3n}-1}{2^{4n}-(q-1)} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}$.

Next, for any fixed i and j such that $1 \le i < j \le q$, the number of $\{y^{(i)}\}_{1\le i\le q}$ such that $x_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LL}^{(i)} \oplus y_{LR}^{(i)} = x_{LL}^{(j)} \oplus x_{LR}^{(j)} \oplus y_{LL}^{(j)} \oplus y_{LR}^{(j)}$ is at most $\frac{2^{3n}}{2^{4n}-(j-1)} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!} \le \frac{2^{3n}}{2^{4n}-(q-1)} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}$, since we have: $(2^{4n})(2^{4n}-1)\cdots(2^{4n}-(j-2))$ choice of $y^{(1)}, \dots, y^{(j-1)}$; 2^n choice of $y_{LR}^{(j)}$, which uniquely determines $y_{LL}^{(j)} = x_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LL}^{(i)} \oplus y_{LR}^{(i)} \oplus x_{LL}^{(j)} \oplus x_{LR}^{(j)} \oplus y_{LR}^{(j)}$; at most 2^{2n} choice of $y_{RL}^{(j)}, y_{RR}^{(j)}$; and $(2^{4n}-j)(2^{4n}-j-1)\cdots(2^{4n}-(q-1))$ choice of $y^{(j+1)}, \dots, y^{(q)}$.

Therefore, the number of $y^{(1)}, \dots, y^{(q)}$ such that

- $y_{LL}^{(i)} = y_{LL}^{(j)}$ for $1 \le \exists i < \exists j \le q$,
- $y_{LR}^{(i)} = y_{LR}^{(j)}$ for $1 \le \exists i < \exists j \le q$, or
- $x_{LL}^{(i)} \oplus x_{LR}^{(i)} \oplus y_{LL}^{(i)} \oplus y_{LR}^{(i)} = x_{LL}^{(j)} \oplus x_{LR}^{(j)} \oplus y_{LL}^{(j)} \oplus y_{LR}^{(j)}$ for $1 \le \exists i < \exists j \le q$

is at most $\binom{q}{2} \cdot \frac{3\cdot 2^{3n}-2}{2^{4n}-(q-1)} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n}-q)!\}}$, which is at most $\frac{3}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n}-q)!\}}$. Q.E.D.

5 A six round KASUMI type permutation is super-pseudorandom

Theorem 5.1 *For $1 \le i \le 18$, let $p_i \in P_n$ be a random permutation. Let $\psi = \psi(p_1, \dots, p_{18})$ be a six round KASUMI type permutation, $R \in P_{4n}$ be a random permutation, and $\Psi \stackrel{\mathrm{def}}{=} \{\psi \mid \psi = \psi(p_1, \dots, p_{18}), p_i \in P_n \text{ for } 1 \le i \le 18\}$.*

Then for any adversary $\mathcal{A}$ that makes at most q queries in total,

$$\mathtt{Adv}_{\Psi}^{\mathsf{sprp}}(\mathcal{A}) \le \frac{9q(q-1)}{2^n-1} \quad .$$

Proof. Let $\mathcal{O}$ be either R or ψ. The adversary $\mathcal{A}$ has oracle access to $\mathcal{O}$ and $\mathcal{O}^{-1}$.

There are two types of queries $\mathcal{A}$ can make: either $(+, x)$ or $(-, y)$. For the i-th query $\mathcal{A}$ makes to $\mathcal{O}$ or $\mathcal{O}^{-1}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{4n} \times \{0,1\}^{4n}$, where either $\mathcal{A}$'s query was $(+, x^{(i)})$ and the answer it got was $y^{(i)} = \mathcal{O}(x^{(i)})$ or $\mathcal{A}$'s query was $(-, y^{(i)})$ and the answer it got was $x^{(i)} = \mathcal{O}^{-1}(y^{(i)})$. Define view v of $\mathcal{A}$ as $v = \langle (x^{(1)}, y^{(1)}), \dots, (x^{(q)}, y^{(q)}) \rangle$.

Since $\mathcal{A}$ has unbounded computational power, $\mathcal{A}$ can be assumed to be deterministic. This implies that there exists a function $\mathcal{C}_{\mathcal{A}}$ such that

$$\begin{cases} \mathcal{C}_{\mathcal{A}}(x^{(1)}, y^{(1)}, \dots, x^{(i-1)}, y^{(i-1)}) = \text{either } (+, x^{(i)}) \text{ or } (-, y^{(i)}) \text{ for } 1 \le i \le q \text{ and} \\ \mathcal{C}_{\mathcal{A}}(v) = \mathcal{A}\text{'s final output.} \end{cases}$$

Let $\boldsymbol{v}_{one} \stackrel{\mathrm{def}}{=} \{v \mid \mathcal{C}_{\mathcal{A}}(v) = 1\}$ and $N_{one} \stackrel{\mathrm{def}}{=} \#\boldsymbol{v}_{one}$.

Evaluation of p_R. We first evaluate $p_R \stackrel{\text{def}}{=} \Pr(R \stackrel{R}{\leftarrow} P_{4n} : \mathcal{A}^{R,R^{-1}} = 1)$. We have $p_R = N_{one} \cdot \frac{(2^{4n}-q)!}{(2^{4n})!}$ as was done in the proof of Theorem 3.1

Evaluation of p_ψ. We evaluate $p_\psi \stackrel{\text{def}}{=} \Pr(\psi \stackrel{R}{\leftarrow} \Psi : \mathcal{A}^{\psi,\psi^{-1}} = 1)$. Note that "$\psi \stackrel{R}{\leftarrow} \Psi$" is equivalent to "$p_i \stackrel{R}{\leftarrow} P_n$ for $1 \le i \le 18$ and then let $\psi \leftarrow \psi(p_1, \dots, p_{18})$." We have $p_\psi = \frac{\#\{(p_1,\dots,p_{18}) | \mathcal{A}^{\psi,\psi^{-1}}=1\}}{\{(2^n)!\}^{18}}$.

We have the following lemma. A proof of this lemma is given in Section 6.

Lemma 5.1 (Main Lemma for $\psi(p_1, \dots, p_{18})$) *For any fixed possible view*

$$v = \langle (x^{(1)}, y^{(1)}), \dots, (x^{(q)}, y^{(q)}) \rangle \ ,$$

the number of $(p_1, \dots, p_{18})$ *such that*

$$\psi(x^{(i)}) = y^{(i)} \textit{ for } 1 \le \forall i \le q \tag{25}$$

is at least $\left(1 - \frac{9q(q-1)}{2^n-1}\right) \cdot \{(2^n)!\}^{14} \cdot \{(2^n - q)!\}^4$.

Then from Lemma 5.1, we have

$$\begin{aligned}
p_\psi &= \sum_{v \in \boldsymbol{v}_{one}} \frac{\#\{(p_1, \dots, p_{18}) \mid (p_1, \dots, p_{18}) \text{ satisfying } (25)\}}{\{(2^n)!\}^{18}} \\
&\ge \sum_{v \in \boldsymbol{v}_{one}} \left(1 - \frac{9q(q-1)}{2^n - 1}\right) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \\
&\ge N_{one} \cdot \left(1 - \frac{9q(q-1)}{2^n - 1}\right) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \\
&= p_R \cdot \left(1 - \frac{9q(q-1)}{2^n - 1}\right) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n} - q)!\}} \ .
\end{aligned}$$

Since $\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \cdot \frac{\{(2^{4n})!\}}{\{(2^{4n}-q)!\}} \ge 1$, $p_\psi \ge p_R \cdot \left(1 - \frac{9q(q-1)}{2^n-1}\right) \ge p_R - \frac{9q(q-1)}{2^n-1}$. Applying the same argument to $1-p_\psi$ and $1-p_R$ yields that $1-p_\psi \ge 1-p_R-\frac{9q(q-1)}{2^n-1}$ and we have $|p_\psi - p_R| \le \frac{9q(q-1)}{2^n-1}$.

Q.E.D.

From Theorem 5.1, it is straightforward to show that $\psi = \psi(p_1, \dots, p_{18})$ is super-pseudorandom even if each p_i is a pseudorandom permutation. Note that we do *not* need the super-pseudorandomness of p_i to derive this result, since KASUMI type permutation does *not* use p_i^{-1} in both encryption and decryption. That is, we can "simulate" both ψ and ψ^{-1} *without* using p_i^{-1}.

6 Proof of Lemma 5.1

For $1 \le i \le q$ and $1 \le j \le 18$, let $I_j^{(i)}$ denote the input to p_i when the input to ϕ is $x^{(i)}$ and the output is $y^{(i)}$. Similarly, let $O_j^{(i)}$ denote the output of p_i when the input to ϕ is $x^{(i)}$ and the output is $y^{(i)}$.

Initially, $x^{(1)}, \dots, x^{(q)}, y^{(1)}, \dots, y^{(q)}$ are fixed. See Fig. 8.

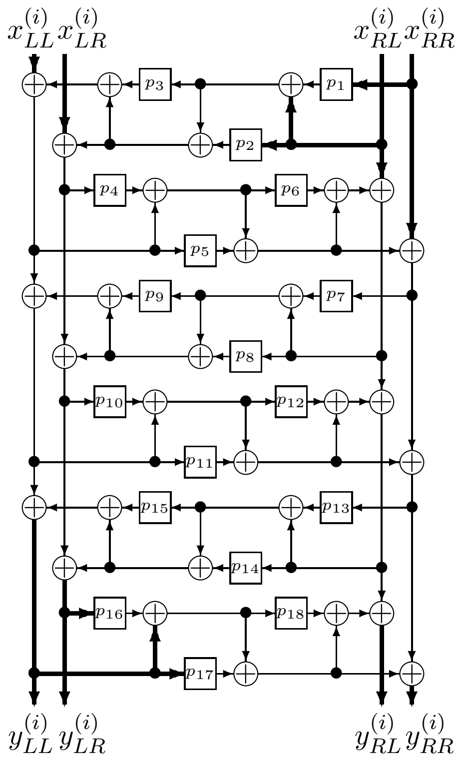

Fig. 8. $x^{(i)}$ and $y^{(i)}$ are fixed.

Number of $(p_1, \dots, p_4)$**.** From Lemma 4.2, the number of $(p_1, \dots, p_4)$ such that:

- $I_6^{(i)} \neq I_6^{(j)}$, and $I_6^{(i)} \oplus x_{RR}^{(i)} \neq I_6^{(j)} \oplus x_{RR}^{(j)}$ for $1 \leq \forall i < \forall j \leq q$

is at least $\{(2^n)!\}^4 - \frac{2q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4$. Note that Lemma 4.2 holds for any possible view, and it is irrelevant from the condition on $y^{(i)}$ in Lemma 3.1. Fix $(p_1, \dots, p_4)$ which satisfy these two conditions arbitrarily.

Number of $(p_{13}, p_{16}, p_{17}, p_{18})$**.** From Lemma 4.2, the number of $(p_{13}, p_{16}, p_{17}, p_{18})$ such that:

- $I_{15}^{(i)} \neq I_{15}^{(j)}$, and $I_{15}^{(i)} \oplus y_{LR}^{(i)} \neq I_{15}^{(j)} \oplus y_{LR}^{(j)}$ for $1 \leq \forall i < \forall j \leq q$

is at least $\{(2^n)!\}^4 - \frac{2q(q-1)}{2^n-1} \cdot \{(2^n)!\}^4$. We have used the symmetry of KASUMI type permutation. That is, $x_{LL}^{(i)}$, $x_{LR}^{(i)}$, $x_{RL}^{(i)}$, $x_{RR}^{(i)}$, p_1, p_2, p_3, p_4 and $I_6^{(i)}$ in Lemma 4.2 corresponds to $y_{RL}^{(i)}$, $y_{RR}^{(i)}$, $y_{LL}^{(i)}$, $y_{LR}^{(i)}$, p_{16}, p_{17}, p_{18}, p_{13} and $I_{15}^{(i)}$ respectively. Fix $(p_{13}, p_{16}, p_{17}, p_{18})$ which satisfy these two conditions arbitrarily. See Fig. 9.

Number of p_5**.** For any fixed i and j such that $1 \leq i < j \leq q$, the number of p_5 such that $p_5(I_5^{(i)}) \oplus I_6^{(i)} \oplus x_{RR}^{(i)} = p_5(I_5^{(j)}) \oplus I_6^{(j)} \oplus x_{RR}^{(j)}$, which is equivalent to $I_7^{(i)} = I_7^{(j)}$, is at most $\frac{\{(2^n)!\}^4}{2^n-1}$ since $I_6^{(i)} \oplus x_{RR}^{(i)} \neq I_6^{(j)} \oplus x_{RR}^{(j)}$. Then the number of p_5 such that

- $I_7^{(i)} \neq I_7^{(j)}$ for $1 \leq \forall i < \forall j \leq q$

is at least $(2^n)! - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any p_5 which satisfy the above condition.

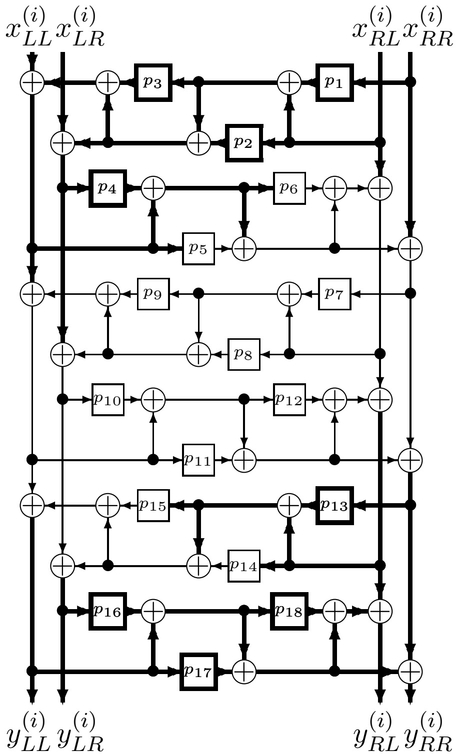

Fig. 9. $p_1, \ldots, p_4, p_{13}, p_{16}, p_{17}, p_{18}$ are fixed.

Number of p_{14}. Similar to the case p_5, for any fixed i and j such that $1 \le i < j \le q$, the number of p_{14} such that $p_{14}(I_{14}^{(i)}) \oplus I_{15}^{(i)} \oplus y_{LR}^{(i)} = p_{14}(I_{14}^{(j)}) \oplus I_{15}^{(j)} \oplus y_{LR}^{(j)}$, which is equivalent to $I_{10}^{(i)} = I_{10}^{(j)}$, is at most $\frac{\{(2^n)!\}^4}{2^n-1}$ since $I_{15}^{(i)} \oplus y_{LR}^{(i)} \ne I_{15}^{(j)} \oplus y_{LR}^{(j)}$. Then the number of p_{14} such that

- $I_{10}^{(i)} \ne I_{10}^{(j)}$ for $1 \le \forall i < \forall j \le q$

is at least $(2^n)! - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any p_{14} which satisfy the above condition. See Fig. 10.

Number of p_6. For any fixed i and j such that $1 \le i < j \le q$, the number of p_6 which satisfies $p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_5^{(i)} \oplus x_{RL}^{(i)} = p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_5^{(j)} \oplus x_{RL}^{(j)}$, which is equivalent to $I_8^{(j)} = I_8^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \ne I_6^{(j)}$.

Similarly, the number of p_6 which satisfies $p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_5^{(i)} \oplus x_{RL}^{(i)} \oplus I_{14}^{(i)} \oplus I_7^{(i)} \oplus I_{13}^{(i)} = p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_5^{(j)} \oplus x_{RL}^{(j)} \oplus I_{14}^{(j)} \oplus I_7^{(j)} \oplus I_{13}^{(j)}$, which is equivalent to $O_{12}^{(i)} = O_{12}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \ne I_6^{(j)}$.

Then, the number of p_6 which satisfies

- $I_8^{(i)} \ne I_8^{(j)}$ and $O_{12}^{(i)} \ne O_{12}^{(j)}$ for $1 \le \forall i < \forall j \le q$

is at least $(2^n)! - \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any p_6 which satisfy the above condition.

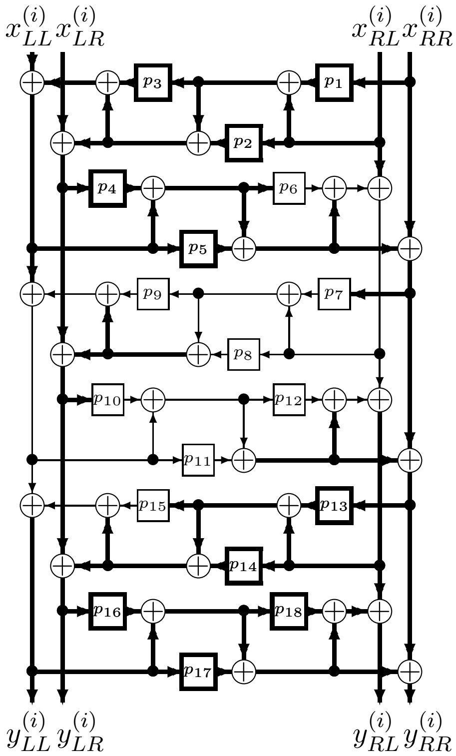

Fig. 10. p_5 and p_{14} are fixed.

Number of p_{15}. For any fixed i and j such that $1 \leq i < j \leq q$, the number of p_{15} which satisfies $p_{15}(I_{15}^{(i)}) \oplus I_{15}^{(i)} \oplus O_{14}^{(i)} \oplus y_{LL}^{(i)} = p_{15}(I_{15}^{(j)}) \oplus I_{15}^{(j)} \oplus O_{14}^{(j)} \oplus y_{LL}^{(j)}$, which is equivalent to $I_{11}^{(i)} = I_{11}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{15}^{(i)} \neq I_{15}^{(j)}$.

Similarly, the number of p_{15} which satisfies $p_{15}(I_{15}^{(i)}) \oplus I_{15}^{(i)} \oplus O_{14}^{(i)} \oplus y_{LL}^{(i)} \oplus I_4^{(i)} \oplus I_{10}^{(i)} \oplus I_5^{(i)} = p_{15}(I_{15}^{(j)}) \oplus I_{15}^{(j)} \oplus O_{14}^{(j)} \oplus y_{LL}^{(i)} \oplus I_4^{(j)} \oplus I_{10}^{(j)} \oplus I_5^{(j)}$, which is equivalent to $O_9^{(i)} = O_9^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{15}^{(i)} \neq I_{15}^{(j)}$.

Then, the number of p_{15} which satisfies

- $I_{11}^{(i)} \neq I_{11}^{(j)}$ and $O_9^{(i)} \neq O_9^{(j)}$ for $1 \leq \forall i < \forall j \leq q$

is at least $(2^n)! - \frac{q(q-1)}{2^n-1} \cdot (2^n)!$. Fix any p_{15} which satisfy the above condition. See Fig. 11.

Number of $(p_7, \ldots, p_{12})$. Now $p_1, \ldots, p_6, p_{13}, \ldots, p_{15}$ are fixed in such a way that $\{I_7^{(i)}\}_{1\leq i\leq q}$ are distinct, $\{I_8^{(i)}\}_{1\leq i\leq q}$ are distinct, $\{O_9^{(i)}\}_{1\leq i\leq q}$ are distinct, $\{I_{10}^{(i)}\}_{1\leq i\leq q}$ are distinct, $\{I_{11}^{(i)}\}_{1\leq i\leq q}$ are distinct and $\{O_{12}^{(i)}\}_{1\leq i\leq q}$ are distinct. Then, by applying Lemma 4.1 twice, we have at least $\left(1 - \frac{q(q-1)}{2^n-1}\right)^2 \cdot \{(2^n)!\}^2 \cdot \{(2^n - q)!\}^4$ choice of $(p_7, \ldots, p_{12})$.

Completing the proof. To summarize, we have:

- at least $\left(1 - \frac{2q(q-1)}{2^n-1}\right)^2 \cdot \{(2^n)!\}^8$ choice of $p_1, \ldots, p_4, p_{13}, p_{16}, p_{17}$ and p_{18},

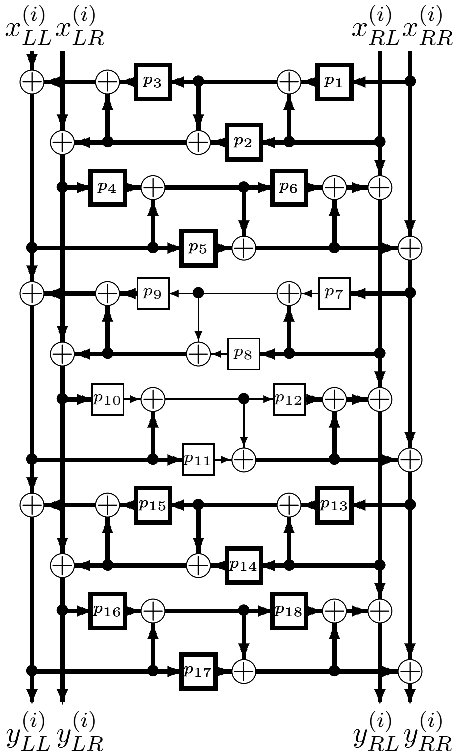

Fig. 11. p_6 and p_{15} are fixed.

- at least $\{(2^n)!\}^2 \cdot \left(1 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1}\right)^2$ choice of (p_5, p_{14}) when $p_1, \ldots, p_4$, p_{13}, p_{16}, p_{17} and p_{18} are fixed,
- at least $\{(2^n)!\}^2 \cdot \left(1 - \frac{q(q-1)}{2^n-1}\right)^2$ choice of (p_6, p_{15}) when $p_1, \ldots, p_5$, p_{13}, p_{14}, p_{16}, p_{17} and p_{18} are fixed,
- at least $\left(1 - \frac{q(q-1)}{2^n-1}\right)^2 \cdot \{(2^n)!\}^2 \cdot \{(2^n-q)!\}^4$ choice of $p_7 \ldots, p_{12}$ when $p_1, \ldots, p_6, p_{13}, \ldots, p_{18}$ are fixed.

Then the number of $(p_1, \cdots, p_{18})$ which satisfy (2) is at least

$$\begin{aligned}&\left(1 - \frac{2q(q-1)}{2^n-1}\right)^2 \cdot \left(1 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1}\right)^2 \cdot \left(1 - \frac{q(q-1)}{2^n-1}\right)^4 \cdot \{(2^n)!\}^{14} \cdot \{(2^n-q)!\}^4 \\ &\quad \geq \left(1 - \frac{9q(q-1)}{2^n-1}\right) \cdot \{(2^n)!\}^8 \cdot \{(2^n-q)!\}^4 \ .\end{aligned}$$

This concludes the proof of the lemma. Q.E.D.

7 Conclusion

In this paper, we showed that a four round KASUMI type permutation is pseudorandom (Theorem 3.1). We proved that the advantage is at most $\frac{15}{2} \cdot \frac{q(q-1)}{2^n-1}$. We also showed that a six round KASUMI type permutation is super-pseudorandom (Theorem 5.1). We proved that the advantage is at most $\frac{9q(q-1)}{2^n-1}$.

It is an important open question to prove (or disprove) the super-pseudorandomness of the five round KASUMI type permutation. We conjecture that it *is* super-pseudorandom.

References

[1] `http://www.3gpp.org/`.

[2] 3GPP TS 35.202 v 3.1.1. Specification of the 3GPP confidentiality and integrity algorithms, Document 2: KASUMI specification. Available at `http://www.3gpp.org/tb/other/algorithms.htm`.

[3] Evaluation report (version 2.0). Specification of the 3GPP confidentiality and integrity algorithms, Report on the evaluation of 3GPP confidentiality and integrity algorithms. Available at `http://www.3gpp.org/tb/other/algorithms.htm`.

[4] M. Blunden and A. Escott. Related key attacks on reduced round KASUMI. *Fast Software Encryption, FSE 2001, LNCS 2355,* pp. 277–285, Springer-Verlag, 2002.

[5] T. Iwata, T. Yagi, and K. Kurosawa. On the pseudorandomness of KASUMI type permutations. *The Eighth Australasian Conference on Information Security and Privacy, ACISP 2003, LNCS, 2727,* pp. 130–141, Springer-Verlag, 2003.

[6] J. S. Kang, S. U. Shin, D. Hong, and O. Yi. Provable security of KASUMI and 3GPP encryption mode $f8$. *Advances in Cryptology — ASIACRYPT 2001, LNCS 2248,* pp. 255–271, Springer-Verlag, 2001.

[7] J. S. Kang, O. Yi, D. Hong, and H. Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. *Information Security and Privacy, The 6th Australasian Conference, ACISP 2001, LNCS 2119,* pp. 60–73, Springer-Verlag, 2001.

[8] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.,* vol. 17, no. 2, pp. 373–386, April 1988.

[9] M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. *Fast Software Encryption, FSE '96, LNCS 1039,* pp. 206–218, Springer-Verlag.

[10] M. Matsui. New block encryption algorithm MISTY. *Fast Software Encryption, FSE '97, LNCS 1267,* pp. 54–68, Springer-Verlag.

[11] K. Sakurai and Y. Zheng. On non-pseudorandomness from block ciphers with provable immunity against linear cryptanalysis. *IEICE Trans. Fundamentals,* vol. E80-A, no. 1, pp. 19–24, April 1997.

A Flaws in the proof of [6]

Kang et al. claimed that:

- the four round MISTY type permutation is pseudorandom for adaptive adversaries [6, Theorem 1] and
- the four round KASUMI type permutation is pseudorandom for adaptive adversaries [6, Theorem 3].

In this section, we show that both proofs are wrong. In what follows, we use the same notation as in [6].

A.1 Flaws on Theorem 1

On advantage. In [6, Proof of Theorem 1, p.262], it is stated that

$$\left|\Pr(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin \mathrm{BAD}(f_1, f_2)) - \Pr(T_{\mathcal{P}_{n+m}} = \sigma)\right| \leq \varepsilon_{n,m,q} \ ,$$

and then

$$\sum_{\sigma \in \Theta} \Pr(\sigma \notin \mathrm{BAD}(f_1, f_2)) \cdot \left|\Pr(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin \mathrm{BAD}(f_1, f_2)) - \Pr(T_{\mathcal{P}_{n+m}} = \sigma)\right| \leq \varepsilon_{n,m,q} \ ,$$

where $\varepsilon_{n,m,q} = \{2^{n+m}(2^n - 1)(2^m - 1) \cdots (2^n - q + 1)(2^m - q + 1)\}^{-1}$.

However, we can only say that there are at most $1/\varepsilon_{n,m,q}$ σ such that $\sigma \in \Theta$. This implies only that

$$\sum_{\sigma \in \Theta} \Pr(\sigma \notin \mathrm{BAD}(f_1, f_2)) \cdot \left|\Pr(T_{\Lambda_{n+m}} = \sigma \mid \sigma \notin \mathrm{BAD}(f_1, f_2)) - \Pr(T_{\mathcal{P}_{n+m}} = \sigma)\right| \leq 1$$

and $ADV_{\mathcal{D}} < 1$. Hence it does not prove that $ADV_{\mathcal{D}}$ is negligible.

On collision. In [6, Lemma 4, p.261], it is stated that

$$\Pr(f_3(L_2^{(i)}) = y_L^{(i)} \oplus \overline{R_2^{(i)}} \text{ for } 1 \leq \forall i \leq q) = \frac{(2^n - q)!}{(2^n)!}, \tag{26}$$

where:

- f_3 is a random permutation over $\{0,1\}^n$,
- $L_2^{(i)}$ is a fixed n-bit string such that $L_2^{(i)} \neq L_2^{(j)}$ for $1 \leq \forall i < \forall j \leq q$,
- $y_L^{(i)}$ is a fixed n-bit string such that $y_L^{(i)} \neq y_L^{(j)}$ for $1 \leq \forall i < \forall j \leq q$, and
- $\overline{R_2^{(i)}}$ is a fixed n-bit string such that $\overline{R_2^{(i)}} \neq \overline{R_2^{(j)}}$ for $1 \leq \forall i < \forall j \leq q$.

However eq.(26) does not hold because in general, $y_L^{(i)} \oplus \overline{R_2^{(i)}} \neq y_L^{(j)} \oplus \overline{R_2^{(j)}}$ does not hold even if $y_L^{(i)} \neq y_L^{(j)}$ and $\overline{R_2^{(i)}} \neq \overline{R_2^{(j)}}$. For example, $y_L^{(i)} = 0^n, y_L^{(j)} = 10^{n-1}, \overline{R_2^{(i)}} = 0^n, \overline{R_2^{(j)}} = 10^{n-1}$.

Exactly the same problem occurs in the analysis of f_4 in [6, Lemma 4, p.261].

A.2 Flaws on Theorem 3

In [6, p.266] it is stated that "Theorem 3 is proved straightforwardly by the similar process in the proof of Theorem 1." However, the proof of Theorem 1 is wrong as shown above. Therefore, the proof of Theorem 3 is also wrong. (In addition, the proof of Lemma 6 is wrong similarly to above.)