Round Security and Super-Pseudorandomness of MISTY Type Structure

Tetsu Iwata, Tomonobu Yoshino, Tomohiro Yuasa, and Kaoru Kurosawa

Department of Communication and Integrated Systems,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
{tez,kurosawa}@ss.titech.ac.jp

Abstract. The security of an iterated block cipher heavily depends on its structure as well as each round function. Matsui showed that MISTY type structure is faster and more robust than Feistel structure on linear cryptanalysis and differential cryptanalysis. On the other hand, Luby and Rackoff proved that the four round Feistel structure is super-pseudorandom if each round function f_i is a random function. This paper proves that the five round MISTY type structure is super-pseudorandom. We also characterize its round security.

1 Introduction

The security of an iterated block cipher heavily depends on its structure as well as each round function. There are some well known structures of iterated block ciphers, Feistel structure (for example, DES), MISTY type structure, IDEA type structure and etc. For Feistel structure, Nyberg and Knudsen [7] showed that if each round function is secure against linear cryptanalysis and differential cryptanalysis, then the whole block cipher is immune to both attacks. Matsui showed that MISTY type structure is faster and more robust than Feistel structure on linear cryptanalysis and differential cryptanalysis [4,5].

Pseudorandomness is also an important cryptographic criterion of iterated block ciphers. This approach studies the pseudorandomness of the block cipher by assuming that each round function is ideally random. We say that a block cipher is pseudorandom if it is secure against chosen plaintext attack, where the adversary has access only to the forward direction of the block cipher. It is said to be super-pseudorandom if it is secure under *both* chosen plaintext and chosen ciphertext attacks, where the adversary has access to *both* directions of the block cipher.

The super-pseudorandomness of Feistel structure has been studied extensively so far. Luby and Rackoff proved that the three round Feistel structure is pseudorandom and the four round Feistel structure is super-pseudorandom if each round function f_i is a random function [2]. Patarin gave an alternate proof [8,9]. Lucks showed that the three round Feistel structure is pseudorandom even if the first round function f_1 is an XOR-universal hash function (not

M. Matsui (Ed.): FSE 2001, LNCS 2355, pp. 233–247, 2002.
© Springer-Verlag Berlin Heidelberg 2002

necessarily random) [3]. Naor and Reingold showed that the four round Feistel structure is super-pseudorandom even if the first and the last round functions f_1 and f_4 are XOR-universal [6]. Finally, Ramzan and Reyzin showed that the four round Feistel structure is super-pseudorandom even if the adversary has oracle access to the second and the third round functions f_2 and f_3, but not super-pseudorandom if the adversary has oracle access to the first or the last round function, f_1 or f_4 [10].

However, only a little is known about the super-pseudorandomness of MISTY type structure. Sakurai and Zheng showed that the three round MISTY type structure is not pseudorandom, and the four round MISTY type structure is not super-pseudorandom [11]. On the other hand, it is not known if the five round MISTY type structure is super-pseudorandom [11].

This paper characterizes the *super*-pseudorandomness of the five round MISTY type structure. We prove that the five round MISTY type structure is *super*-pseudorandom even if:

1. The first, second and the last round functions, p_1, p_2 and p_5, are XOR-universal permutations. This holds even if the adversary has oracle access to the third and fourth round functions p_3 and p_4.
2. The first and the last round functions, p_1 and p_5, are XOR-universal. This holds even if the adversary has oracle access to the second, third and fourth round functions, p_2, p_3 and p_4.

We also show that it is not super-pseudorandom if the adversary is allowed to have oracle access to the first or the last round function, p_1 or p_5.

Intuitively, our results can be stated as follows. The five round MISTY type structure is super-pseudorandom if: (1) the first and the last rounds have secrecy and only weak randomness, (2) the third and fourth rounds have strong randomness and no secrecy, and (3) the second round has secrecy and only weak randomness, or no secrecy and strong randomness.

To derive our positive results, we use Patarin's approach [8,9] while Ramzan and Reyzin [10] used the approach of Naor and Reingold [6].

Related works: About pseudorandomness (but not super-pseudorandomness) Sugita showed that the four round MISTY type structure is pseudorandom [12], and the five round recursive MISTY type structure is pseudorandom [13].

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. If S is a probability space, then $s \xleftarrow{R} S$ denotes the process of picking an element from S according to the underlying probability distribution. (Unless otherwise specified,) The underlying distribution is assumed to be uniform.

Denote by F_n the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, which consists of $2^{n \cdot 2^n}$ in total. Similarly, denote by P_n the set of all permutations from $\{0,1\}^n$ to $\{0,1\}^n$, which consists of $(2^n)!$ in total. By a finite function (or permutation) family $\mathcal{F}$, we denote a set of functions with common domain and common range. We call a finite function (or permutation) family *keyed* if every function in it can be specified by a key sk. We denote the function given by sk as f_{sk}. We assume that given sk, it is possible to efficiently evaluate f_{sk} at any point (as well as f_{sk}^{-1} in case of a keyed permutation family). For a given keyed function family, a key can be any string from $\{0,1\}^s$, where s is known as "key length." For functions f and g, $g \circ f$ denotes the function $x \mapsto g(f(x))$.

2.2 Super-Pseudorandomness

We are now ready to define a secure block cipher, or what Luby and Rackoff called a super-pseudorandom permutation [2]. The super-pseudorandomness of a keyed permutation family $\mathcal{F}$ over $\{0,1\}^n$ captures its computational indistinguishability from P_n, where the adversary is given access to both directions of the permutation. In other words, it measures security of a block cipher against chosen plaintext and chosen ciphertext attacks.

Our adaptive adversary $\mathcal{M}$ is modeled as a Turing machine that has black-box access to some number k of oracles, each of which computes some specified function. If $(f_1, \ldots, f_k)$ is a k-tuple of functions, then $\mathcal{M}^{f_1,\ldots,f_k}$ denotes a k-oracle adversary who is given black-box access to each of the functions $f_1, \ldots, f_k$. The computational power of $\mathcal{M}$ is unlimited, but the total number of oracle calls is limited to a parameter m.

Definition 2.1. (Advantage, sprp). *Let a block cipher $\mathcal{F}$ be a keyed permutation family over $\{0,1\}^n$ with key length s. Let $\mathcal{M}$ be a 2-oracle adversary. Then we define $\mathcal{M}$'s advantage as*

$$\mathtt{Adv}_{\mathcal{F}}^{\mathsf{sprp}}(\mathcal{M}) \stackrel{\text{def}}{=} |p_f - p_R|$$

where

$$\begin{cases} p_f \stackrel{\text{def}}{=} \Pr(\mathcal{M}^{f_{sk}, f_{sk}^{-1}}(1^n) = 1 \mid sk \xleftarrow{R} \{0,1\}^s) \\ p_R \stackrel{\text{def}}{=} \Pr(\mathcal{M}^{R, R^{-1}}(1^n) = 1 \mid R \xleftarrow{R} P_n) \end{cases}$$

Definition 2.2. (Super-pseudorandom permutation family). *A block cipher $\mathcal{F}$ is super-pseudorandom if $\mathtt{Adv}_{\mathcal{F}}^{\mathsf{sprp}}(\mathcal{M})$ is negligible for any 2-oracle adversary $\mathcal{M}$.*

2.3 MISTY Type Permutation [4,5]

Matsui proposed MISTY [4,5], which is faster and more robust than Feistel structure on linear cryptanalysis and differential cryptanalysis.

Definition 2.3. (The basic MISTY type permutation). *Let $x \in \{0,1\}^{2n}$. For any permutation $p \in P_n$, define the basic MISTY type permutation, $M_p \in P_{2n}$ as $M_p(x) \stackrel{\text{def}}{=} (x_R, p(x_L) \oplus x_R)$. Note that it is a permutation since $M_p^{-1}(x) = (p^{-1}(x_L \oplus x_R), x_L)$.*

Definition 2.4. (The r round MISTY type permutation, ψ). *Let $r \geq 1$ be an integer, $p_1, \ldots, p_r \in P_n$ be permutations. Define the r round MISTY type permutation $\psi(p_1, \ldots, p_r) \in P_{2n}$ as $\psi(p_1, \ldots, p_r) \stackrel{\text{def}}{=} \rho \circ M_{p_r} \circ \cdots \circ M_{p_1}$, where $\rho(x_L, x_R) = (x_R, x_L)$ for $x \in \{0,1\}^{2n}$.*

See Fig. 1 (the four round Feistel permutation) and Fig. 2 (the five round MISTY type permutation) for illustrations. Note that p_i in Fig. 2 is a permutation whereas f_i in Fig. 1 is just a function. For simplicity, the left and right swaps are omitted.

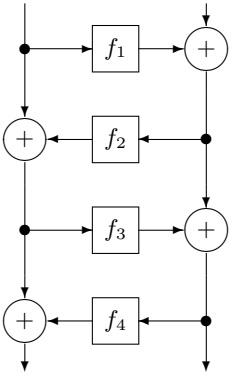

Fig. 1. Feistel permutation

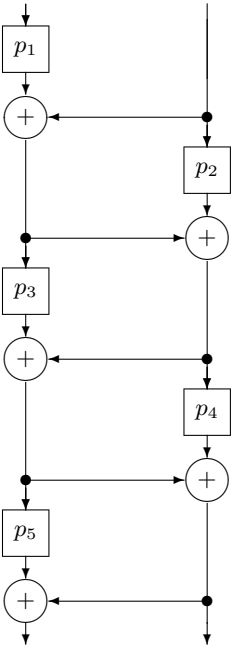

Fig. 2. MISTY type permutation

2.4 Round Security of the Five Round MISTY Type Permutation

The round security model of a block cipher was introduced by Ramzan and Reyzin [10]. In the round security model, the adversary is allowed to have oracle access to some subset K of round functions, and the advantage additionally depends on K.

Definition 2.5. (Round security of the five round MISTY type permutation). *Let p_i be a permutation drawn from a keyed permutation family $\mathcal{P}_i$ over $\{0,1\}^n$ with key length s_i, for $i = 1,\ldots,5$. Let $\psi(p_1,\ldots,p_5)$ be the five round MISTY type permutation, and Ψ be the set of $\psi(p_1,\ldots,p_5)$ with key length $s = s_1 + \cdots + s_5$ (the key sk for $\psi(p_1,\ldots,p_5)$ is simply the concatenation of keys for $p_1,\ldots,p_5$). Fix some subset $\mathcal{K} = \{\Pi^1,\ldots,\Pi^k\}$ of the set $\{\mathcal{P}_1,\mathcal{P}_1^{-1},\ldots,\mathcal{P}_5,\mathcal{P}_5^{-1}\}$, and let $\mathcal{M}$ be a $(k+2)$-oracle adversary. Let $K \stackrel{\text{def}}{=} \{\pi^1_{sk},\ldots,\pi^k_{sk}\}$, where $\pi^i_{sk} \in \Pi^i$ for $1 \le i \le k$. Then we define $\mathcal{M}$'s advantage as*

$$\mathtt{Adv}^{\mathsf{sprp}}_{\Psi;\mathcal{K}}(\mathcal{M}) \stackrel{\text{def}}{=} |p_\psi - p_R|$$

where

$$\begin{cases} p_\psi \stackrel{\text{def}}{=} \Pr(\mathcal{M}^{\psi_{sk},\psi^{-1}_{sk},\pi^1_{sk},\ldots,\pi^k_{sk}}(1^{2n}) = 1 \mid sk \xleftarrow{R} \{0,1\}^s) \\ p_R \stackrel{\text{def}}{=} \Pr(\mathcal{M}^{R,R^{-1},\pi^1_{sk},\ldots,\pi^k_{sk}}(1^{2n}) = 1 \mid R \xleftarrow{R} P_{2n}, sk \xleftarrow{R} \{0,1\}^s) \end{cases}$$

2.5 Uniform ϵ-XOR Universal Permutation

Our definition follows from those given in [1,10,14].

Definition 2.6. *Let H_n be a keyed permutation family over $\{0,1\}^n$. Denote by $\#H_n$ the size of H_n. H_n is* uniform ϵ-XOR universal *provided that the following two conditions are satisfied:*

1. *for any element $x \in \{0,1\}^n$ and any element $y \in \{0,1\}^n$, there exist exactly $\frac{\#H_n}{2^n}$ permutations $h \in H_n$ such that $h(x) = y$.*
2. *for any two distinct elements $x, x' \in \{0,1\}^n$ and any element $y \in \{0,1\}^n$, there exist at most $\epsilon \# H_n$ permutations $h \in H_n$ such that $h(x) \oplus h(x') = y$.*

Let $f_{a,b}(x) \stackrel{\text{def}}{=} a \cdot x + b$ over $\mathrm{GF}(2^n)$, where $a \neq 0$. Then $\{f_{a,b}(x)\}$ is uniform $\frac{1}{2^n-1}$-XOR universal.

We will use the phrase "h is an uniform ϵ-XOR universal permutation" to mean that "h is drawn uniformly from an uniform ϵ-XOR universal permutation family."

3 Round Security of MISTY Type Permutation

3.1 Negative Result

In this section, we show that $\psi(p_1,p_2,p_3,p_4,p_5)$ is not super-pseudorandom if the adversary is allowed to have oracle access to $\{p_1,p_1^{-1}\}$ or $\{p_5^{-1}\}$. This means that, we require secrecy in the first and the last rounds if the cipher is secure.

Theorem 3.1. *Let $p_1,p_2,p_3,p_4,p_5 \in P_n$ be random permutations. Let $\psi = \psi(p_1,p_2,p_3,p_4,p_5)$, and $R \in P_{2n}$ be a random permutation. Suppose that K contains at least one of $\{p_1,p_1^{-1}\}$ or $\{p_5^{-1}\}$. Then there exists an oracle adversary $\mathcal{M}$ such that*

$$\mathtt{Adv}^{\mathsf{sprp}}_{\Psi;\mathcal{K}}(\mathcal{M}) \ge 1 - \frac{2}{2^n} \ .$$

Proof. Let $\mathcal{O} = R$ or ψ. First, suppose that $\mathcal{M}$ has oracle access to $\mathcal{O}$, $\mathcal{O}^{-1}$, p_1 and p_1^{-1}. Consider the following $\mathcal{M}$:

1. Pick $X, A, A' \in \{0,1\}^n$ such that $A \neq A'$ arbitrarily.
2. Ask $(A, A \oplus X)$ to $\mathcal{O}^{-1}$ and obtain (C, D).
3. Ask $(A', A' \oplus X)$ to $\mathcal{O}^{-1}$ and obtain (C', D').
4. Ask C to p_1 and obtain E.
5. Ask C' to p_1 and obtain E'.
6. Ask $D \oplus D' \oplus E$ to p_1^{-1} and obtain F.
7. Ask $D \oplus D' \oplus E'$ to p_1^{-1} and obtain F'.
8. Ask (F', D) to $\mathcal{O}$ and obtain (S, T).
9. Ask (F, D') to $\mathcal{O}$ and obtain (S', T').
10. Output "1" if and only if $S \oplus T = S' \oplus T'$.

If $\mathcal{O} = \psi$, then X is the output of p_5 at step 2 and step 3. Hence the input to p_5 at step 2 is equal to that of step 3. Therefore, from step 4 and step 5, we have

$$p_2(D) \oplus D \oplus E \oplus p_3(D \oplus E) = p_2(D') \oplus D' \oplus E' \oplus p_3(D' \oplus E') \ . \qquad (1)$$

In step 8, the output of p_1 is equal to $D \oplus D' \oplus E'$ from step 7. Therefore, the input to p_5 is equal to $p_2(D) \oplus D' \oplus E' \oplus p_3(D' \oplus E')$ in step 8. Similarly, in step 9, the input to p_5 is equal to $p_2(D') \oplus D \oplus E \oplus p_3(D \oplus E)$. Then from eq.(1), we see that the inputs to p_5 are equal in step 8 and step 9. Hence we have $p_\psi = 1$.

If $\mathcal{O} = R$, we have $p_R \leq \frac{2}{2^n}$.

Next suppose that $\mathcal{M}$ has oracle access to $\mathcal{O}$, $\mathcal{O}^{-1}$ and p_5^{-1}. Consider the following $\mathcal{M}$:

1. Pick $X, B, B' \in \{0,1\}^n$ such that $B \neq B'$ arbitrarily.
2. Ask B to p_5^{-1} and obtain A.
3. Ask B' to p_5^{-1} and obtain A'.
4. Ask $(X, X \oplus B)$ to $\mathcal{O}^{-1}$ and obtain (C, D).
5. Ask $(A \oplus A' \oplus B \oplus B' \oplus X, A \oplus A' \oplus B \oplus X)$ to $\mathcal{O}^{-1}$ and obtain (C', D').
6. Ask (C, D') to $\mathcal{O}$ and obtain (E, F).
7. Ask (C', D) to $\mathcal{O}$ and obtain (E', F').
8. Ask $E \oplus F$ to p_5^{-1} and obtain H.
9. Ask $E' \oplus F'$ to p_5^{-1} and obtain H'.
10. Output "1" if and only if $H \oplus F = H' \oplus F'$.

If $\mathcal{O} = \psi$, then $A \oplus B \oplus X$ is the outputs of p_4 at step 4 and step 5. Then the input to p_4 at step 6 is equal to that of step 7. Hence we have $p_\psi = 1$.

If $\mathcal{O} = R$, we have $p_R \leq \frac{2}{2^n}$. □

3.2 Positive Result 1

Let $h_1, h_2, h_3 \in H_n$ be uniform ϵ-XOR universal permutations and $p \in P_n$ be a random permutation. Let $\psi = \psi(h_1, h_2, p, p, h_3^{-1})$, and $R \in P_{2n}$ be a random permutation. Define $K = \{p, p^{-1}\}$.

Lemma 3.1. *Let m_0 and m_1 be integers. Choose $x^{(i)} \in \{0,1\}^{2n}$ and $y^{(i)} \in \{0,1\}^{2n}$ for $1 \le i \le m_0$ arbitrarily in such a way that $x^{(i)}$ are all distinct and $y^{(i)}$ are all distinct. Choose $X^{(i)} \in \{0,1\}^n$ and $Y^{(i)} \in \{0,1\}^n$ for $1 \le i \le m_1$ arbitrarily in such a way that $X^{(i)}$ are all distinct and $Y^{(i)}$ are all distinct.*

Then the number of (h_1, h_2, p, h_3) such that

$$\left.\begin{array}{l} \psi(x^{(i)}) = y^{(i)} \text{ for } 1 \le \forall i \le m_0, \text{ and} \\ p(X^{(i)}) = Y^{(i)} \text{ for } 1 \le \forall i \le m_1 \end{array}\right\} \tag{2}$$

is at least

$$(\#H_n)^3(2^n - 2m_0 - m_1)! \left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n}\right) \ .$$

A proof is given in the next section.

Theorem 3.2. *For any 4-oracle adversary $\mathcal{M}$ that makes at most m queries in total,*

$$\mathtt{Adv}^{\mathsf{sprp}}_{\Psi;K}(\mathcal{M}) \le \epsilon \cdot m(3m-2) + \frac{4m^2}{2^n} \ .$$

Proof. Let $\mathcal{O} = R$ or ψ. The 4-oracle adversary $\mathcal{M}$ has oracle access to $\mathcal{O}$, $\mathcal{O}^{-1}$, p and p^{-1}. Assume that $\mathcal{M}$ makes m_0 queries to $\mathcal{O}$ or $\mathcal{O}^{-1}$, and m_1 queries to p or p^{-1}, where $m = m_0 + m_1$.

Let $q^{(1)}, \ldots, q^{(m_0)} \in \{0,1\}^{2n}$ be bit strings that $\mathcal{M}$ asks to $\mathcal{O}$ or $\mathcal{O}^{-1}$, and let $a^{(1)}, \ldots, a^{(m_0)} \in \{0,1\}^{2n}$ be the answers that $\mathcal{M}$ obtains. Let $Q^{(1)}, \ldots, Q^{(m_1)} \in \{0,1\}^n$ be bit strings that $\mathcal{M}$ asks to p or p^{-1}, and let $A^{(1)}, \ldots, A^{(m_1)} \in \{0,1\}^n$ be the answers that $\mathcal{M}$ obtains.

Let

$$(x^{(i)}, y^{(i)}) = \begin{cases} (q^{(i)}, a^{(i)}) & \text{if } \mathcal{O}(q^{(i)}) = a^{(i)} \\ (a^{(i)}, q^{(i)}) & \text{if } \mathcal{O}^{-1}(q^{(i)}) = a^{(i)} \end{cases} , \tag{3}$$

$$(X^{(i)}, Y^{(i)}) = \begin{cases} (Q^{(i)}, A^{(i)}) & \text{if } p(Q^{(i)}) = A^{(i)} \\ (A^{(i)}, Q^{(i)}) & \text{if } p^{-1}(Q^{(i)}) = A^{(i)} \end{cases} . \tag{4}$$

That is,

$$\mathcal{O}(x^{(i)}) = y^{(i)} \text{ for } 1 \le i \le m_0, \text{ and } p(X^{(i)}) = Y^{(i)} \text{ for } 1 \le i \le m_1 \ .$$

Without loss of generality, we assume that $x^{(i)}$ are all distinct, $y^{(i)}$ are all distinct, $X^{(i)}$ are all distinct and $Y^{(i)}$ are all distinct.

Suppose that $\mathcal{M}$ has obtained $a^{(1)}, \ldots, a^{(i)}$ and $A^{(1)}, \ldots, A^{(j)}$ from the oracles at some point. Then the next behavior of $\mathcal{M}$ is completely determined by $a^{(1)}, \ldots, a^{(i)}$ and $A^{(1)}, \ldots, A^{(j)}$. Therefore, the final output of $\mathcal{M}$ (0 or 1) depends only on $a \stackrel{\text{def}}{=} (a^{(1)}, \ldots, a^{(m_0)})$ and $A \stackrel{\text{def}}{=} (A^{(1)}, \ldots, A^{(m_1)})$. Hence denote by $\mathcal{C}_{\mathcal{M}}(a, A)$ the final output of $\mathcal{M}$.

Let $\mathcal{B} \stackrel{\text{def}}{=} \{(a, A) \mid \mathcal{C}_{\mathcal{M}}(a, A) = 1\}$ and $N \stackrel{\text{def}}{=} \#\mathcal{B}$.

Evaluation of p_R. From the definition of p_R, we have

$$p_R = \Pr_{R,p}(\mathcal{M}^{R,R^{-1},p,p^{-1}}(1^{2n}) = 1) = \frac{\#\{(R,p) \mid \mathcal{M}^{R,R^{-1},p,p^{-1}}(1^{2n}) = 1\}}{(2^{2n})!(2^n)!} \ .$$

We say that (R,p) is compatible with (a,A) if the (R,R^{-1}) oracles answer a and the (p,p^{-1}) oracles answer A. More precisely, (R,p) is compatible with (a,A) if

$$R(x^{(i)}) = y^{(i)} \text{ for } 1 \le i \le m_0 \text{ and } p(X^{(i)}) = Y^{(i)} \text{ for } 1 \le i \le m_1 \ , \qquad (5)$$

where $x^{(i)}, y^{(i)}, X^{(i)}, Y^{(i)}$ are defined by eq.(3) and eq.(4) from (a,A). For each $(a,A) \in \mathcal{B}$, the number of (R,p) which is compatible with (a,A) is exactly $(2^{2n} - m_0)!(2^n - m_1)!$. Therefore, we have

$$\begin{aligned} p_R &= \sum_{(a,A)\in\mathcal{B}} \frac{\#\{(R,p) \mid (R,p) \text{ is compatible with } (a,A)\}}{(2^{2n})!(2^n)!} \\ &= \sum_{(a,A)\in\mathcal{B}} \frac{\#\{(R,p) \mid (R,p) \text{ satisfying (5)}\}}{(2^{2n})!(2^n)!} \\ &= N \cdot \frac{(2^{2n} - m_0)!(2^n - m_1)!}{(2^{2n})!(2^n)!} \ . \end{aligned}$$

Evaluation of p_ψ. From the definition of p_ψ, we have

$$\begin{aligned} p_\psi &= \Pr_{h_1,h_2,p,h_3}(\mathcal{M}^{\psi,\psi^{-1},p,p^{-1}}(1^{2n}) = 1) \\ &= \frac{\#\{(h_1,h_2,p,h_3) \mid \mathcal{M}^{\psi,\psi^{-1},p,p^{-1}}(1^{2n}) = 1\}}{(\#H_n)^3(2^n)!} \ . \end{aligned}$$

Similarly to p_R, we have

$$p_\psi = \sum_{(a,A)\in\mathcal{B}} \frac{\#\{(h_1,h_2,p,h_3) \mid (h_1,h_2,p,h_3) \text{ satisfying (2)}\}}{(\#H_n)^3(2^n)!} \ .$$

Then from Lemma 3.1, we obtain that

$$\begin{aligned} p_\psi &\ge \sum_{(a,A)\in\mathcal{B}} \frac{(\#H_n)^3(2^n - 2m_0 - m_1)!\left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0+2m_1)}{2^n}\right)}{(\#H_n)^3(2^n)!} \\ &= N\frac{(2^n - 2m_0 - m_1)!}{(2^n)!}\left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n}\right) \\ &= p_R\frac{(2^{2n})!(2^n - 2m_0 - m_1)!}{(2^{2n} - m_0)!(2^n - m_1)!}\left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n}\right) \ . \end{aligned}$$

Since $\frac{(2^{2n})!(2^n-2m_0-m_1)!}{(2^{2n}-m_0)!(2^n-m_1)!} \geq 1$ (This can be shown easily by an induction on m_0), we have

$$\begin{aligned} p_\psi &\geq p_R \left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n}\right) \\ &\geq p_R - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n} \\ &\geq p_R - \epsilon \cdot m(3m - 2) - \frac{4m^2}{2^n} \ . \end{aligned} \tag{6}$$

Applying the same argument to $1 - p_\psi$ and $1 - p_R$ yields that

$$1 - p_\psi \geq 1 - p_R - \epsilon \cdot m(3m - 2) - \frac{4m^2}{2^n} \ . \tag{7}$$

Finally, (6) and (7) give $|p_\psi - p_R| \leq \epsilon \cdot m(3m - 2) + \frac{4m^2}{2^n}$. □

3.3 Positive Result 2

Let $h_1, h_2 \in H_n$ be uniform ϵ-XOR-universal permutations, $p_1, p_2, p_3 \in P_n$ be random permutations, $\psi = \psi(h_1, p_1, p_2, p_3, h_2^{-1})$, and $R \in P_{2n}$ be a random permutation. Define $K = \{p_1, p_1^{-1}, p_2, p_2^{-1}, p_3, p_3^{-1}\}$.

Lemma 3.2. *Let m_0, m_1, m_2, m_3 be integers such that $m = m_0 + m_1 + m_2 + m_3$. Choose $x^{(i)} \in \{0,1\}^{2n}$ and $y^{(i)} \in \{0,1\}^{2n}$ for $1 \leq i \leq m_0$ arbitrarily in such a way that $x^{(i)}$ are all distinct and $y^{(i)}$ are all distinct. Similarly, for $1 \leq l \leq 3$, choose $X_l^{(i)} \in \{0,1\}^n$ and $Y_l^{(i)} \in \{0,1\}^n$ for $1 \leq i \leq m_l$ arbitrarily in such a way that $X_l^{(i)}$ are all distinct, $Y_l^{(i)}$ are all distinct and*

$$X_1^{(i)} \oplus Y_1^{(i)} \neq X_1^{(j)} \oplus Y_1^{(j)} \text{ for } l = 1 \text{ and } 1 \leq \forall i < \forall j \leq m_1 \ .$$

Then the number of $(h_1, p_1, p_2, p_3, h_2)$ such that

$$\left.\begin{array}{l} \psi(x^{(i)}) = y^{(i)} \text{ for } 1 \leq \forall i \leq m_0, \\ p_1(X_1^{(i)}) = Y_1^{(i)} \text{ for } 1 \leq \forall i \leq m_1, \\ p_2(X_2^{(i)}) = Y_2^{(i)} \text{ for } 1 \leq \forall i \leq m_2, \text{ and} \\ p_3(X_3^{(i)}) = Y_3^{(i)} \text{ for } 1 \leq \forall i \leq m_3 \end{array}\right\} \tag{8}$$

is at least

$$\begin{aligned} &(2^n - m_1)!(2^n - m_2 - m_0)!(2^n - m_3 - m_0)! \\ &\quad (\#H_n)^2 \left(1 - 2\epsilon \cdot m_0(m_0 - 1) - \frac{m_0(2m - 1)}{2^n}\right) \ . \end{aligned}$$

A proof is similar to that of Lemma 3.1.

Theorem 3.3. *For any 8-oracle adversary $\mathcal{M}$ that makes at most m queries in total,*

$$\mathtt{Adv}^{\mathsf{sprp}}_{\Psi;\mathcal{K}}(\mathcal{M}) \le 2\epsilon \cdot m(m-1) + \frac{m(3m-2)}{2^n} \quad .$$

Proof. Let $\mathcal{O} = R$ or ψ. The 8-oracle adversary $\mathcal{M}$ has oracle access to $\mathcal{O}$, $\mathcal{O}^{-1}$, p_1, p_1^{-1}, p_2, p_2^{-1}, p_3 and p_3^{-1}. Assume that $\mathcal{M}$ makes m_0 queries to $\mathcal{O}$ or $\mathcal{O}^{-1}$ and m_l queries to p_l or p_l^{-1} for $1 \le l \le 3$, where $m = m_0 + m_1 + m_2 + m_3$.

Let $q^{(1)}, \ldots, q^{(m_0)} \in \{0,1\}^{2n}$ be bit strings that $\mathcal{M}$ asks to $\mathcal{O}$ or $\mathcal{O}^{-1}$, and let $a^{(1)}, \ldots, a^{(m_0)} \in \{0,1\}^{2n}$ be the answers that $\mathcal{M}$ obtains. For $1 \le l \le 3$, let $Q_l^{(1)}, \ldots, Q_l^{(m_l)} \in \{0,1\}^n$ be bit strings that $\mathcal{M}$ asks to p_l or p_l^{-1}, and let $A_l^{(1)}, \ldots, A_l^{(m_l)} \in \{0,1\}^n$ be the answers that $\mathcal{M}$ obtains.

Let

$$(x^{(i)}, y^{(i)}) = \begin{cases} (q^{(i)}, a^{(i)}) & \text{if } \mathcal{O}(q^{(i)}) = a^{(i)} \\ (a^{(i)}, q^{(i)}) & \text{if } \mathcal{O}^{-1}(q^{(i)}) = a^{(i)} \end{cases} \tag{9}$$

$$(X_l^{(i)}, Y_l^{(i)}) = \begin{cases} (Q_l^{(i)}, A_l^{(i)}) & \text{if } p_l(Q_l^{(i)}) = A_l^{(i)} \\ (A_l^{(i)}, Q_l^{(i)}) & \text{if } p_l^{-1}(Q_l^{(i)}) = A_l^{(i)} \end{cases} \tag{10}$$

for $1 \le l \le 3$. That is, $\mathcal{O}(x^{(i)}) = y^{(i)}$ for $1 \le i \le m_0$ and $p_l(X_l^{(i)}) = Y_l^{(i)}$ for $1 \le l \le 3$ and $1 \le i \le m_l$.

Without loss of generality, we assume that $x^{(i)}$ are all distinct, $y^{(i)}$ are all distinct, $X_l^{(i)}$ are all distinct and $Y_l^{(i)}$ are all distinct, for $1 \le l \le 3$.

Define $a \stackrel{\text{def}}{=} (a^{(1)}, \ldots, a^{(m_0)})$ and $A_l \stackrel{\text{def}}{=} (A_l^{(1)}, \ldots, A_l^{(m_l)})$ for $1 \le l \le 3$. Then, similarly to the proof of Theorem 3.2, we can denote by $\mathcal{C}_{\mathcal{M}}(a, A_1, A_2, A_3)$ the output of $\mathcal{M}$ (0 or 1). Let

$$\begin{cases} \mathcal{B}_1 \stackrel{\text{def}}{=} \{(a, A_1, A_2, A_3) \mid \mathcal{C}_{\mathcal{M}}(a, A_1, A_2, A_3) = 1\}, \\ N \stackrel{\text{def}}{=} \#\mathcal{B}_1, \text{ and} \\ \mathcal{B}_2 \stackrel{\text{def}}{=} \{(a, A_1, A_2, A_3) \mid \mathcal{C}_{\mathcal{M}}(a, A_1, A_2, A_3) = 1 \text{ and} \\ \qquad\qquad 1 \le \forall i < \forall j \le m_1, X_1^{(i)} \oplus Y_1^{(i)} \ne X_1^{(j)} \oplus Y_1^{(j)}\}. \end{cases}$$

Evaluation of p_R. From the definition of p_R, we have

$$\begin{aligned} p_R &= \Pr_{R,p_1,p_2,p_3}(\mathcal{M}^{R,R^{-1},p_1,p_1^{-1},p_2,p_2^{-1},p_3,p_3^{-1}}(1^{2n}) = 1) \\ &= \frac{\#\{(R,p_1,p_2,p_3) \mid \mathcal{M}^{R,R^{-1},p_1,p_1^{-1},p_2,p_2^{-1},p_3,p_3^{-1}}(1^{2n}) = 1\}}{(2^{2n})!\,((2^n)!)^3} \quad . \end{aligned}$$

Since the number of (R, p_1, p_2, p_3) such that

$$\left.\begin{array}{l} R(x^{(i)}) = y^{(i)} \text{ for } 1 \le \forall i \le m_0, \\ p_1(X_1^{(i)}) = Y_1^{(i)} \text{ for } 1 \le \forall i \le m_1, \\ p_2(X_2^{(i)}) = Y_2^{(i)} \text{ for } 1 \le \forall i \le m_2, \text{ and} \\ p_3(X_3^{(i)}) = Y_3^{(i)} \text{ for } 1 \le \forall i \le m_3 \end{array}\right\} \tag{11}$$

is exactly $(2^{2n} - m_0)!(2^n - m_1)!(2^n - m_2)!(2^n - m_3)!$, we have

$$p_R = \sum_{(a,A_1,A_2,A_3)\in\mathcal{B}_1} \frac{\#\{(R,p_1,p_2,p_3) \mid (R,p_1,p_2,p_3) \text{ satisfying (11)}\}}{(2^{2n})!((2^n)!)^3}$$
$$= N \cdot \frac{(2^{2n}-m_0)!(2^n-m_1)!(2^n-m_2)!(2^n-m_3)!}{(2^{2n})!((2^n)!)^3} \quad .$$

Define C be the total number of possible (a, A_1, A_2, A_3). Then

$$C = \frac{(2^{2n})!}{(2^{2n}-m_0)!}\frac{(2^n)!}{(2^n-m_1)!}\frac{(2^n)!}{(2^n-m_2)!}\frac{(2^n)!}{(2^n-m_3)!} \quad .$$

Therefore we have $p_R = \frac{N}{C}$.

Evaluation of p_ψ. From the definition of p_ψ, we have

$$p_\psi = \Pr_{h_1,p_1,p_2,p_3,h_2}(\mathcal{M}^{\psi,\psi^{-1},p_1,p_1^{-1},p_2,p_2^{-1},p_3,p_3^{-1}}(1^{2n}) = 1)$$
$$= \frac{\#\{(h_1,p_1,p_2,p_3,h_2) \mid \mathcal{M}^{\psi,\psi^{-1},p_1,p_1^{-1},p_2,p_2^{-1},p_3,p_3^{-1}}(1^{2n}) = 1\}}{(\#H_n)^2((2^n)!)^3} \quad .$$

Then

$$p_\psi \geq \sum_{(a,A_1,A_2,A_3)\in\mathcal{B}_2} \frac{\#\{(h_1,p_1,p_2,p_3,h_2) \mid (h_1,p_1,p_2,p_3,h_2) \text{ satisfying (8)}\}}{(\#H_n)^2((2^n)!)^3} \quad .$$

Now we want to evaluate $\#\mathcal{B}_2$. Fix any i and j such that $1 \leq i < j \leq m_1$. Then the number of $A_1 = (A_1^{(1)}, \ldots, A_1^{(m_1)})$ which satisfies $X_1^{(i)} \oplus Y_1^{(i)} = X_1^{(j)} \oplus Y_1^{(j)}$ is exactly $\frac{1}{2^n-1}\frac{(2^n)!}{(2^n-m_1)!}$, since we have 2^n choice of $A_1^{(i)}$ which uniquely determines $A_1^{(j)}$ according to the relation $X_1^{(i)} \oplus Y_1^{(i)} = X_1^{(j)} \oplus Y_1^{(j)}$, and other bit strings, $A_1^{(l)}$ where $l \neq i, j$, can be arbitrarily, we have $\frac{(2^n-2)!}{(2^n-m_1)!}$ choice. Since we have $\binom{m_1}{2}$ choice of (i,j), the number of (a, A_1, A_2, A_3) which satisfy

$$1 \leq \exists i < \exists j \leq m_1, X_1^{(i)} \oplus Y_1^{(i)} = X_1^{(j)} \oplus Y_1^{(j)}$$

is at most $\binom{m_1}{2}\frac{C}{2^n-1}$, which is upper bounded by $\frac{m_1(m_1-1)}{2^n}C$. Then it is clear that $\#\mathcal{B}_2 \geq N - \frac{m_1(m_1-1)}{2^n}C$.

Define

$$D \stackrel{\text{def}}{=} \left(1 - 2\epsilon \cdot m_0(m_0-1) - \frac{m_0(2m-1)}{2^n}\right) \quad .$$

Then from Lemma 3.2, we have

$$p_\psi \geq \sum_{(a,A_1,A_2,A_3)\in\mathcal{B}_2} \frac{(2^n-m_1)!(2^n-m_2-m_0)!(2^n-m_3-m_0)!}{((2^n)!)^3}D$$
$$\geq \left(N - \frac{m_1(m_1-1)}{2^n}C\right)\frac{(2^n-m_1)!(2^n-m_2-m_0)!(2^n-m_3-m_0)!}{((2^n)!)^3}D$$
$$= \left(p_R - \frac{m_1(m_1-1)}{2^n}\right)D \cdot C\frac{(2^n-m_1)!(2^n-m_2-m_0)!(2^n-m_3-m_0)!}{((2^n)!)^3} \quad .$$

Since $C\frac{(2^n-m_1)!(2^n-m_2-m_0)!(2^n-m_3-m_0)!}{((2^n)!)^3} = \frac{(2^{2n})!(2^n-m_2-m_0)!(2^n-m_3-m_0)!}{(2^{2n}-m_0)!(2^n-m_2)!(2^n-m_3)!} \geq 1$ (This can be shown easily by an induction on m_0), we have

$$\begin{aligned} p_\psi &\geq \left(p_R - \frac{m_1(m_1-1)}{2^n}\right)\left(1 - 2\epsilon \cdot m_0(m_0-1) - \frac{m_0(2m-1)}{2^n}\right) \\ &\geq p_R - 2\epsilon \cdot m_0(m_0-1) - \frac{m_0(2m-1)}{2^n} - \frac{m_1(m_1-1)}{2^n} \\ &\geq p_R - 2\epsilon \cdot m(m-1) - \frac{m(3m-2)}{2^n} \ . \end{aligned}$$

Then we have

$$|p_\psi - p_R| \leq 2\epsilon \cdot m(m-1) + \frac{m(3m-2)}{2^n}$$

by applying the same argument as was used in Theorem 3.2. □

4 Proof of Lemma 3.1

In ψ, we denote by $I_3 \in \{0,1\}^n$, the input to p in the third round, and denote by $O_3 \in \{0,1\}^n$, the output of it. Similarly, $I_4, O_4 \in \{0,1\}^n$ are the input and output of p in the fourth round, respectively.

Number of h_1. First,

- if $x_L^{(i)} = x_L^{(j)}$, then there exists no h_1 which satisfies
$$h_1(x_L^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus x_R^{(j)} \tag{12}$$
since $x_L^{(i)} = x_L^{(j)}$ implies $x_R^{(i)} \neq x_R^{(j)}$.
- if $x_L^{(i)} \neq x_L^{(j)}$, then the number of h_1 which satisfies (12) is at most $\epsilon \# H_n$ from Definition 2.6.

Therefore, the number of h_1 which satisfies

$$1 \leq \exists i < \exists j \leq m_0, h_1(x_L^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus x_R^{(j)} \tag{13}$$

is at most $\epsilon\binom{m_0}{2}\#H_n$.

Next, the number of h_1 which satisfies

$$h_1(x_L^{(i)}) \oplus x_R^{(i)} = X^{(j)}$$

is exactly $\frac{\#H_n}{2^n}$ from Definition 2.6. Therefore, the number of h_1 which satisfies

$$1 \leq \exists i \leq m_0, 1 \leq \exists j \leq m_1, \ \ h_1(x_L^{(i)}) \oplus x_R^{(i)} = X^{(j)} \tag{14}$$

is at most $\frac{m_0 m_1 \# H_n}{2^n}$.

Then, from (13) and (14), the number of h_1 which satisfies

$$\left.\begin{array}{l} 1 \leq \forall i < \forall j \leq m_0, \ \ h_1(x_L^{(i)}) \oplus x_R^{(i)} \neq h_1(x_L^{(j)}) \oplus x_R^{(j)}, \text{ and} \\ 1 \leq \forall i \leq m_0, 1 \leq \forall j \leq m_1, \ \ h_1(x_L^{(i)}) \oplus x_R^{(i)} \neq X^{(j)} \end{array}\right\} \tag{15}$$

is at least $\#H_n - \epsilon\binom{m_0}{2}\#H_n - \frac{m_0 m_1 \#H_n}{2^n}$. Fix h_1 which satisfies (15) arbitrarily. This implies that $I_3^{(1)}, \ldots, I_3^{(m_0)}$ are fixed in such a way that $I_3^{(1)}, \ldots, I_3^{(m_0)}$ are distinct, and $I_3^{(i)} \neq X^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$.

Number of h_2. Similarly, the number of h_2 which satisfies

$$\left.\begin{array}{l} 1 \leq \forall i < \forall j \leq m_0,\ \ h_2(x_R^{(i)}) \oplus I_3^{(i)} \neq h_2(x_R^{(j)}) \oplus I_3^{(j)}, \\ 1 \leq \forall i \leq m_0, 1 \leq \forall j \leq m_1,\ \ h_2(x_R^{(i)}) \oplus I_3^{(i)} \neq X^{(j)}, \\ 1 \leq \forall i, \forall j \leq m_0,\ \ h_2(x_R^{(i)}) \oplus I_3^{(i)} \neq I_3^{(j)},\ \text{and} \\ 1 \leq \forall i, \forall j \leq m_0,\ \ h_2(x_R^{(i)}) \oplus I_3^{(i)} \neq y_R^{(j)} \end{array}\right\} \tag{16}$$

is at least $\#H_n - \epsilon\binom{m_0}{2}\#H_n - \frac{m_0 m_1 \#H_n}{2^n} - \frac{2m_0^2 \#H_n}{2^n}$. Fix h_2 which satisfies (16) arbitrarily. This implies that $I_4^{(1)}, \ldots, I_4^{(m_0)}$ are fixed in such a way that:

- $I_4^{(1)}, \ldots, I_4^{(m_0)}$ are distinct,
- $I_4^{(i)} \neq X^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$, and
- $I_4^{(i)} \neq I_3^{(j)}$ and $I_4^{(i)} \neq y_R^{(j)}$ for $1 \leq \forall i, \forall j \leq m_0$.

Number of h_3. Similarly, the number of h_3 which satisfies

$$\left.\begin{array}{l} 1 \leq \forall i < \forall j \leq m_0,\ \ h_3(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq h_3(y_L^{(j)} \oplus y_R^{(j)}) \oplus y_R^{(j)}, \\ 1 \leq \forall i < \forall j \leq m_0,\ \ h_3(y_L^{(i)} \oplus y_R^{(i)}) \oplus I_4^{(i)} \neq h_3(y_L^{(j)} \oplus y_R^{(j)}) \oplus I_4^{(j)}, \\ 1 \leq \forall i \leq m_0, 1 \leq \forall j \leq m_1,\ \ h_3(y_L^{(i)} \oplus y_R^{(i)}) \oplus I_4^{(i)} \neq Y^{(j)}, \\ 1 \leq \forall i \leq m_0, 1 \leq \forall j \leq m_1,\ \ h_3(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq Y^{(j)},\ \text{and} \\ 1 \leq \forall i, \forall j \leq m_0,\ \ h_3(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq h_3(y_L^{(j)} \oplus y_R^{(j)}) \oplus I_4^{(j)} \end{array}\right\} \tag{17}$$

is at least $\#H_n - 2\epsilon\binom{m_0}{2}\#H_n - \frac{2m_0 m_1 \#H_n}{2^n} - \epsilon m_0^2 \#H_n$. Fix h_3 which satisfies (17) arbitrarily. This implies that $O_4^{(1)}, \ldots, O_4^{(m_0)}$ and $O_3^{(1)}, \ldots, O_3^{(m_0)}$ are fixed in such a way that:

- $O_4^{(1)}, \ldots, O_4^{(m_0)}$ are distinct,
- $O_3^{(1)}, \ldots, O_3^{(m_0)}$ are distinct,
- $O_3^{(i)} \neq Y^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$,
- $O_4^{(i)} \neq Y^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$, and
- $O_4^{(i)} \neq O_3^{(j)}$ for $1 \leq \forall i, \forall j \leq m_0$.

Number of p. Now h_1, h_2 and h_3 are fixed in such a way that

$$I_3^{(1)}, \ldots, I_3^{(m_0)}, I_4^{(1)}, \ldots, I_4^{(m_0)}, X^{(1)}, \ldots, X^{(m_1)}$$

(which are inputs to p) are all distinct and

$$O_3^{(1)}, \ldots, O_3^{(m_0)}, O_4^{(1)}, \ldots, O_4^{(m_0)}, Y^{(1)}, \ldots, Y^{(m_1)}$$

(which are corresponding outputs of p) are all distinct. In other words, for p, the above $2m_0 + m_1$ input-output pairs are determined. The other $2^n - 2m_0 - m_1$

input-output pairs are undetermined. Therefore we have $(2^n - 2m_0 - m_1)!$ possible choices of p for any such fixed (h_1, h_2, h_3).

Then the number of (h_1, h_2, p, h_3) which satisfy (2) is at least

$$
\begin{aligned}
&(\#H_n)^3(2^n - 2m_0 - m_1)! \left(1 - \epsilon\binom{m_0}{2} - \frac{m_0 m_1}{2^n}\right) \\
&\quad \times \left(1 - \epsilon\binom{m_0}{2} - \frac{m_0 m_1}{2^n} - \frac{2m_0^2}{2^n}\right)\left(1 - 2\epsilon\binom{m_0}{2} - \frac{2m_0 m_1}{2^n} - \epsilon m_0^2\right) \\
&\quad \geq (\#H_n)^3(2^n - 2m_0 - m_1)! \left(1 - \epsilon \cdot m_0(3m_0 - 2) - \frac{2m_0(m_0 + 2m_1)}{2^n}\right)
\end{aligned}
$$

This concludes the proof of the lemma. □

5 Conclusion

In this paper, we proved that:

1. $\psi(p_1, p_2, p_3, p_4, p_5)$ is not super-pseudorandom if the adversary is allowed to have oracle access to $\{p_1, p_1^{-1}\}$ or $\{p_5^{-1}\}$ (Theorem 3.1).
2. $\psi(h_1, h_2, p, p, h_3^{-1})$ is super-pseudorandom even if the adversary has oracle access to p and p^{-1} (Theorem 3.2).
3. $\psi(h_1, p_1, p_2, p_3, h_2^{-1})$ is super-pseudorandom even if the adversary has oracle access to p_1, p_1^{-1}, p_2, p_2^{-1}, p_3 and p_3^{-1} (Theorem 3.3).

The following concrete questions remain to be tackled.

- Is it possible to distinguish $\psi(p_1, p_2, p_3, p_4, p_5)$ from P_{2n} with access to only one of $\{p_1, p_1^{-1}, p_5\}$?
- For example, is $\psi(h_1, p_1, p_1, p_2, h_2^{-1})$ secure when the adversary has oracle access to p_1, p_1^{-1}, p_2 and p_2^{-1} ?

References

1. J.L.Carter and M.N.Wegman. Universal classes of hash functions. *JCSS*, vol. 18, No. 2, pages 143–154, 1979.
2. M.Luby and C.Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, vol. 17, No. 2, pages 373–386, April 1988.
3. S.Lucks. Faster Luby-Rackoff ciphers. *Fast Software Encryption, FSE '96, LNCS* 1039, pages 189–203, Springer-Verlag.
4. M.Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. *Fast Software Encryption, FSE '96, LNCS* 1039, pages 206–218, Springer-Verlag.
5. M.Matsui. New block encryption algorithm MISTY. *Fast Software Encryption, FSE '97, LNCS* 1267, pages 54–68, Springer-Verlag.
6. M.Naor and O.Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revised. *J. Cryptology*, vol. 12, No. 1, pages 29–66, Springer-Verlag, 1999.

7. K.Nyberg and L.R.Knudsen. Provable security against a differential attacks. *J. Cryptology*, vol. 8, No. 1, pages 27–37, Springer-Verlag, 1995.
8. J.Patarin. Pseudorandom permutations based on the DES scheme. *Proceedings of Eurocode '90, LNCS* 514, pages 193–204, Springer-Verlag, 1990.
9. J.Patarin. New results of pseudorandom permutation generators based on the DES scheme. *Advances in Cryptology — CRYPTO '91, LNCS* 576, pages 301–312, Springer-Verlag, 1991.
10. Z.Ramzan and L.Reyzin. On the round security of symmetric-key cryptographic primitives. *Advances in Cryptology — CRYPTO 2000, LNCS* 1880, pages 376–393, Springer-Verlag, 2000.
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, pages 19–24, April 1997.
12. M.Sugita. Pseudorandomness of a block cipher MISTY. *Technical report of IEICE*, ISEC 96-9, pages 13–21, 1996.
13. M.Sugita. Pseudorandomness of block ciphers MISTY1. *Technical report of IEICE*, ISEC 97-19, pages 53–64, 1997.
14. M.N.Wegman and J.L.Carter. New hash functions and their use in authentication and set equality. *JCSS*, vol. 22, No. 3, pages 265–279, 1981.