Non-cryptographic Primitive for Pseudorandom Permutation

Tetsu Iwata[†], Tomonobu Yoshino[†], and Kaoru Kurosawa[†,‡]

[†] Department of Communications and Integrated Systems,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
tez@ss.titech.ac.jp
[‡] Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

Abstract. Four round Feistel permutation (like DES) is super-pseudorandom if each round function is *random* or a *secret* universal hash function. A similar result is known for five round MISTY type permutation. It seems that each round function must be at least either *random* or *secret* in both cases.
In this paper, however, we show that the second round permutation g in five round MISTY type permutation need not be cryptographic at all, i.e., no randomness nor secrecy is required. g has only to satisfy that $g(x) \oplus x \neq g(x') \oplus x'$ for any $x \neq x'$. This is the first example such that a non-cryptographic primitive is substituted to construct the minimum round super-pseudorandom permutation. Further we show efficient constructions of super-pseudorandom permutations by using above mentioned g.

Keywords: Block cipher, pseudorandomness, MISTY type permutation.

1 Introduction

1.1 Super-pseudorandomness

A secure block cipher should be indistinguishable from a truly random permutation. Consider an infinitely powerful distinguisher $\mathcal{D}$ which tries to distinguish a block cipher from a truly random permutation. It outputs 0 or 1 after making at most m queries to the given encryption and/or decryption oracles. We say that a distinguisher $\mathcal{D}$ is a pseudorandom distinguisher if it has oracle access to the encryption oracle. We also say that a distinguisher $\mathcal{D}$ is a super-pseudorandom distinguisher if it has oracle access to both the encryption oracle and the decryption oracle. Then a block cipher E is called pseudorandom if any pseudorandom distinguisher $\mathcal{D}$ cannot distinguish E from a truly random permutation. A block cipher E is called super-pseudorandom if any super-pseudorandom distinguisher $\mathcal{D}$ cannot distinguish E from a truly random permutation.

1.2 Previous works

The super-pseudorandomness of Feistel permutation (like DES) has been studied extensively so far. Let $\phi(f_1, f_2, f_3)$ denote the three round Feistel permutation such that the i-th round function is f_i. Similarly, let $\phi(f_1, f_2, f_3, f_4)$ denote the four round Feistel permutation.

Suppose that each f_i is a random function. Then Luby and Rackoff proved that $\phi(f_1, f_2, f_3)$ is pseudorandom and $\phi(f_1, f_2, f_3, f_4)$ is super-pseudorandom [4]. Lucks showed that the $\phi(h_1, f_2, f_3)$ is pseudorandom even if h_1 is an ϵ-XOR universal hash function [5]. Suppose that h_1 and h_4 are uniform ϵ-XOR universal hash functions. Then Naor and Reingold proved that $h_4 \circ \phi(f_2, f_3) \circ h_1$ is super-pseudorandom [8], and Ramzan and Reyzin showed that $\phi(h_1, f_2, f_3, h_4)$ is super-pseudorandom even if the distinguisher has oracle access to f_2 and f_3 [9].

On the other hand, let $\psi(p_1, p_2, p_3, p_4, p_5)$ denote the five round MISTY type permutation such that the i-th round permutation is p_i. Suppose that each p_i is a random permutation. Then Iwata et al. [3] and Gilbert and Minier [2] independently showed that $\psi(p_1, p_2, p_3, p_4, p_5)$ is super-pseudorandom. More than that, let h_i be a uniform ϵ-XOR universal permutation. Iwata et al. proved that

1. $\psi(h_1, h_2, p_3, p_4, h_5^{-1})$ is super-pseudorandom even if the distinguisher has oracle access to p_3, p_3^{-1}, p_4 and p_4^{-1}.
2. $\psi(h_1, p_2, p_3, p_4, h_5^{-1})$ is super-pseudorandom even if the distinguisher has oracle access to p_2, p_2^{-1}, p_3, p_3^{-1}, p_4 and p_4^{-1}.

1.3 Our contribution

Four round Feistel permutation (like DES) is super-pseudorandom if each round function is *random* or a *secret* universal hash function. A similar result is known for five round MISTY type permutation. It seems that each round function must be at least either *random* or *secret* in both cases.

In this paper, however, we show that the second round permutation g in five round MISTY type permutation need not be cryptographic at all, i.e., no randomness nor secrecy is required. g has only to satisfy that $g(x) \oplus x \neq g(x') \oplus x'$ for any $x \neq x'$. This is the first example such that a non-cryptographic primitive is substituted to construct the minimum round super-pseudorandom permutation. Further we show efficient constructions of super-pseudorandom permutations by using above mentioned g.

One might wonder if five rounds can be reduced to four rounds to obtain super-pseudorandomness of MISTY. However, it is not true because Sakurai and Zheng showed that the four round MISTY type permutation $\psi(p_1, p_2, p_3, p_4)$ is not super-pseudorandom [10].

More precisely, we prove that five round MISTY is super-pseudorandom if it is $\psi(h_1, g, p, p^{-1}, h_5^{-1})$, where g is the above mentioned permutation, h_1 is an ϵ-XOR universal permutation, h_5 is a uniform ϵ-XOR universal permutation, and p is a random permutation. Further, suppose that both h_1 and h_5 are *uniform*

ϵ-XOR universal permutations. Then we prove that it is super-pseudorandom even if the distinguisher has oracle access to p and p^{-1}.

More than that, we study the case such that the third and the fourth round permutations are both p. In this case, we show that it is not super-pseudorandom nor pseudorandom if a distinguisher has oracle access to p. More formally, we show that for any fixed and public g, $\psi(p_1, g, p, p, p_5)$ is not pseudorandom if a distinguisher has oracle access to p.

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 $s \stackrel{R}{\leftarrow} S$ denotes the process of picking an element from S according to the underlying probability distribution. The underlying distribution is assumed to be uniform (unless otherwise specified).

Denote by F_n the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, which consists of $2^{n \cdot 2^n}$ functions in total. Similarly, denote by P_n the set of all permutations from $\{0,1\}^n$ to $\{0,1\}^n$, which consists of $(2^n)!$ permutations in total.

2.2 MISTY type permutation [6, 7]

Definition 2.1 (The basic MISTY type permutation). *Let $x \in \{0,1\}^{2n}$. For any permutation $p \in P_n$, define the basic MISTY type permutation $\psi_p \in P_{2n}$ as $\psi_p(x) \stackrel{\text{def}}{=} (x_R, p(x_L) \oplus x_R)$. Note that it is a permutation since $\psi_p^{-1}(x) = (p^{-1}(x_L \oplus x_R), x_L)$.*

Definition 2.2 (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 $\psi(p_1, \ldots, p_r) \stackrel{\text{def}}{=} \rho \circ \psi_{p_r} \circ \cdots \circ \psi_{p_1}$, where $\rho(x_L, x_R) = (x_R, x_L)$ for $x \in \{0,1\}^{2n}$.*

See Fig. 1 (the five round MISTY type permutation) for an illustration. Note that p_i in Fig. 1 is a permutation. For simplicity, the left and right swaps are omitted.

2.3 Uniform ϵ-XOR universal permutation

Our definitions follow from those given in [1, 3, 9, 11].

Definition 2.3. *Let H_n be a permutation family over $\{0,1\}^n$. Denote by $\#H_n$ the size of H_n.*

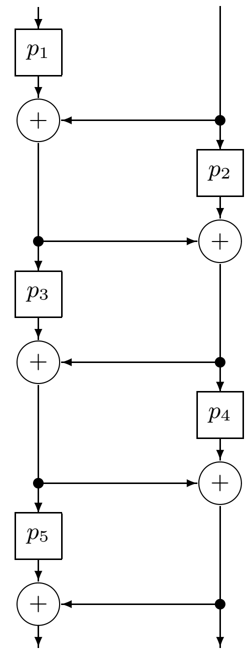

Fig. 1. MISTY type permutation

1. *H_n is a* uniform *permutation family if 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. *H_n is an* ϵ-XOR universal *permutation family if 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 $f_a(x) \stackrel{\text{def}}{=} a \cdot x$ over $\mathrm{GF}(2^n)$, where $a \neq 0$. Then $\{f_a(x)\}$ is a $\frac{1}{2^n-1}$-XOR universal permutation family.

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 a uniform $\frac{1}{2^n-1}$-XOR universal permutation family.

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

3 Improved super-pseudorandomness of MISTY type permutation

We say that a permutation g over $\{0,1\}^n$ is *XOR-distinct* if

$$g(x) \oplus x \neq g(x') \oplus x'$$

for any $x \neq x'$. Let $g(x) = a \cdot x$ over $\mathrm{GF}(2^n)$, where $a \neq 0, 1$. Then this g is clearly XOR-distinct.

In this section, we prove that $\psi(h_1, g, p, p^{-1}, h_5^{-1})$ is super-pseudorandom even if the second round permutation g is fixed and publicly known. g has only to be XOR-distinct. This means that the five round MISTY type permutation is super-pseudorandom even if the second round permutation has no randomness nor secrecy.

Let H_n^0 be an ϵ-XOR universal permutation family over $\{0,1\}^n$, and H_n^1 be a uniform ϵ-XOR universal permutation family over $\{0,1\}^n$. Define

$$\begin{cases} \mathrm{MISTY}_{2n}^{01} \stackrel{\mathrm{def}}{=} \{\psi(h_1, g, p, p^{-1}, h_5^{-1}) \mid p \in P_n, h_1 \in H_n^0, h_5 \in H_n^1\} \\ \mathrm{MISTY}_{2n}^{11} \stackrel{\mathrm{def}}{=} \{\psi(h_1, g, p, p^{-1}, h_5^{-1}) \mid p \in P_n, h_1, h_5 \in H_n^1\} \end{cases}$$

3.1 Super-pseudorandomness of MISTY_{2n}^{01}

Let $\mathcal{D}$ be a super-pseudorandom distinguisher for MISTY_{2n}^{01} which makes at most m queries in total. We consider two experiments, experiment 0 and experiment 1. In experiment 0, $\mathcal{D}$ has oracle access to ψ and ψ^{-1}, where ψ is randomly chosen from MISTY_{2n}^{01}. In experiment 1, $\mathcal{D}$ has oracle access to R and R^{-1}, where R is randomly chosen from P_{2n}.

Define the advantage of $\mathcal{D}$ as follows.

$$\mathtt{Adv}(\mathcal{D}) \stackrel{\mathrm{def}}{=} |p_\psi - p_R|$$

where

$$\begin{cases} p_\psi \stackrel{\mathrm{def}}{=} \Pr(\mathcal{D}^{\psi,\psi^{-1}}(1^{2n}) = 1 \mid \psi \stackrel{R}{\leftarrow} \mathrm{MISTY}_{2n}^{01}) \\ p_R \stackrel{\mathrm{def}}{=} \Pr(\mathcal{D}^{R,R^{-1}}(1^{2n}) = 1 \mid R \stackrel{R}{\leftarrow} P_{2n}) \end{cases}$$

Lemma 3.1. *Fix $x^{(i)} \in \{0,1\}^{2n}$ and $y^{(i)} \in \{0,1\}^{2n}$ for $1 \le i \le m$ arbitrarily in such a way that $\{x^{(i)}\}_{1 \le i \le m}$ are all distinct and $\{y^{(i)}\}_{1 \le i \le m}$ are all distinct.*

Then the number of $\psi \in \mathrm{MISTY}_{2n}^{01}$ such that

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

is at least

$$(\#H_n^0)(\#H_n^1)(2^n - 2m)! \left(1 - 2\epsilon \cdot m(m-1) - \frac{2m^2}{2^n}\right) .$$

A proof is given in Appendix A.

Theorem 3.1. *For any super-pseudorandom distinguisher $\mathcal{D}$ that makes at most m queries in total,*

$$\mathtt{Adv}(\mathcal{D}) \le 2\epsilon \cdot m(m-1) + \frac{2m^2}{2^n} .$$

Proof. Let $\mathcal{O} = R$ or ψ. The super-pseudorandom distinguisher $\mathcal{D}$ has oracle access to $\mathcal{O}$ and $\mathcal{O}^{-1}$.

There are two types of queries $\mathcal{D}$ can make: either $(+, x)$ which denotes the query "what is $\mathcal{O}(x)$?", or $(-, y)$ which denotes the query "what is $\mathcal{O}^{-1}(y)$?" For the i-th query $\mathcal{D}$ makes to $\mathcal{O}$ or $\mathcal{O}^{-1}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{2n} \times \{0,1\}^{2n}$, where either $\mathcal{D}$'s query was $(+, x^{(i)})$ and the answer it got was $y^{(i)}$ or $\mathcal{D}$'s query was $(-, y^{(i)})$ and the answer it got was $x^{(i)}$. Define view v of $\mathcal{D}$ as $v = ((x^{(1)}, y^{(1)}), \ldots, (x^{(m)}, y^{(m)}))$.

Without loss of generality, we assume that $\{x^{(i)}\}_{1 \le i \le m}$ are all distinct, and $\{y^{(i)}\}_{1 \le i \le m}$ are all distinct.

Since $\mathcal{D}$ has unbounded computational power, $\mathcal{D}$ can be assumed to be deterministic. Therefore, the final output of $\mathcal{D}$ (0 or 1) depends only on v. Hence denote by $\mathcal{C}_{\mathcal{D}}(v)$ the final output of $\mathcal{D}$.

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

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

$$\begin{aligned} p_R &= \Pr_R(\mathcal{D}^{R,R^{-1}}(1^{2n}) = 1) \\ &= \frac{\#\{R \mid \mathcal{D}^{R,R^{-1}}(1^{2n}) = 1\}}{(2^{2n})!} \ . \end{aligned}$$

For each $v \in \boldsymbol{v}_{one}$, the number of R such that

$$R(x^{(i)}) = y^{(i)} \text{ for } 1 \le \forall i \le m \tag{2}$$

is exactly $(2^{2n} - m)!$. Therefore, we have

$$\begin{aligned} p_R &= \sum_{v \in \boldsymbol{v}_{one}} \frac{\#\{R \mid R \text{ satisfying (2)}\}}{(2^{2n})!} \\ &= N_{one} \cdot \frac{(2^{2n} - m)!}{(2^{2n})!} \ . \end{aligned}$$

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

$$\begin{aligned} p_\psi &= \Pr_{h_1,p,h_5}(\mathcal{D}^{\psi,\psi^{-1}}(1^{2n}) = 1) \\ &= \frac{\#\{(h_1,p,h_5) \mid \mathcal{D}^{\psi,\psi^{-1}}(1^{2n}) = 1\}}{(\#H_n^0)(2^n)!(\#H_n^1)} \ . \end{aligned}$$

Similarly to p_R, we have

$$p_\psi = \sum_{v \in \boldsymbol{v}_{one}} \frac{\#\left\{(h_1,p,h_5) \mid (h_1,p,h_5) \text{ satisfying (1)}\right\}}{(\#H_n^0)(2^n)!(\#H_n^1)} \ .$$

Then from Lemma 3.1, we obtain that

$$p_\psi \ge \sum_{v \in \boldsymbol{v}_{one}} \frac{(2^n - 2m)!\left(1 - 2\epsilon \cdot m(m-1) - \frac{2m^2}{2^n}\right)}{(2^n)!}$$

$$= N_{one}\frac{(2^n-2m)!}{(2^n)!}\left(1-2\epsilon\cdot m(m-1)-\frac{2m^2}{2^n}\right)$$
$$= p_R\frac{(2^{2n})!(2^n-2m)!}{(2^{2n}-m)!(2^n)!}\left(1-2\epsilon\cdot m(m-1)-\frac{2m^2}{2^n}\right) \quad .$$

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

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

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

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

Finally, (3) and (4) give $|p_\psi - p_R| \leq 2\epsilon\cdot m(m-1)+\frac{2m^2}{2^n}$.

3.2 Super-pseudorandomness of MISTY^{11}_{2n}

Let $\mathcal{D}$ be a super-pseudorandom distinguisher for MISTY^{11}_{2n}. $\mathcal{D}$ also has oracle access to p and p^{-1}, where p and p^{-1} are the third and fourth round permutations of MISTY^{11}_{2n} respectively. $\mathcal{D}$ makes at most m queries in total. We consider two experiments, experiment 0 and experiment 1. In experiment 0, $\mathcal{D}$ has oracle access to not only ψ and ψ^{-1}, but also p and p^{-1}, where ψ is randomly chosen from MISTY^{11}_{2n}. In experiment 1, $\mathcal{D}$ has oracle access to R, R^{-1}, p and p^{-1}, where R is randomly chosen from P_{2n} and p is randomly chosen from P_n.

Define the advantage of $\mathcal{D}$ as follows.

$$\mathtt{Adv}(\mathcal{D}) \stackrel{\text{def}}{=} |p_\psi - p_R|$$

where

$$\begin{cases} p_\psi \stackrel{\text{def}}{=} \Pr(\mathcal{D}^{\psi,\psi^{-1},p,p^{-1}}(1^{2n})=1 \mid \psi \stackrel{R}{\leftarrow} \mathrm{MISTY}^{11}_{2n}) \\ p_R \stackrel{\text{def}}{=} \Pr(\mathcal{D}^{R,R^{-1},p,p^{-1}}(1^{2n})=1 \mid R \stackrel{R}{\leftarrow} P_{2n}, p \stackrel{R}{\leftarrow} P_n) \end{cases}$$

Lemma 3.2. *Let m_0 and m_1 be integers. Fix $x^{(i)} \in \{0,1\}^{2n}$ and $y^{(i)} \in \{0,1\}^{2n}$ for $1 \leq i \leq m_0$ arbitrarily in such a way that $\{x^{(i)}\}_{1\leq i\leq m_0}$ are all distinct and $\{y^{(i)}\}_{1\leq i\leq m_0}$ are all distinct. Similarly, fix $X^{(i)} \in \{0,1\}^n$ and $Y^{(i)} \in \{0,1\}^n$ for $1 \leq i \leq m_1$ arbitrarily in such a way that $\{X^{(i)}\}_{1\leq i\leq m_1}$ are all distinct and $\{Y^{(i)}\}_{1\leq i\leq m_1}$ are all distinct.*

Then the number of $\psi \in \mathrm{MISTY}^{11}_{2n}$ such that

$$\psi(x^{(i)}) = y^{(i)} \text{ for } 1 \leq \forall i \leq m_0 \text{ and } p(X^{(i)}) = Y^{(i)} \text{ for } 1 \leq \forall i \leq m_1 \tag{5}$$

is at least

$$(\#H^1_n)^2(2^n-2m_0-m_1)!\left(1-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n}\right) \quad .$$

A proof is given in Appendix B.

Theorem 3.2. *For any super-pseudorandom distinguisher $\mathcal{D}$ that also has oracle access to p and p^{-1} and makes at most m queries in total,*

$$\mathtt{Adv}(\mathcal{D}) \leq 2\epsilon \cdot m(m-1) + \frac{6m^2}{2^n} \ .$$

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

There are four types of queries $\mathcal{D}$ can make: either $(+, x)$ which denotes the query "what is $\mathcal{O}(x)$?", $(-, y)$ which denotes the query "what is $\mathcal{O}^{-1}(y)$?", $(+, X)$ which denotes the query "what is $p(X)$?", or $(-, Y)$ which denotes the query "what is $p^{-1}(Y)$?" For the i-th query $\mathcal{D}$ makes to $\mathcal{O}$ or $\mathcal{O}^{-1}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{2n} \times \{0,1\}^{2n}$, where either $\mathcal{D}$'s query was $(+, x^{(i)})$ and the answer it got was $y^{(i)}$ or $\mathcal{D}$'s query was $(-, y^{(i)})$ and the answer it got was $x^{(i)}$. Similarly for the i-th query $\mathcal{D}$ makes to p or p^{-1}, define the query-answer pair $(X^{(i)}, Y^{(i)}) \in \{0,1\}^n \times \{0,1\}^n$, where either $\mathcal{D}$'s query was $(+, X^{(i)})$ and the answer it got was $Y^{(i)}$ or $\mathcal{D}$'s query was $(-, Y^{(i)})$ and the answer it got was $X^{(i)}$. Define view v and V of $\mathcal{D}$ as $v = ((x^{(1)}, y^{(1)}), \ldots, (x^{(m_0)}, y^{(m_0)}))$ and $V = ((X^{(1)}, Y^{(1)}), \ldots, (X^{(m_1)}, Y^{(m_1)}))$. Without loss of generality, we assume that $\{x^{(i)}\}_{1 \leq i \leq m_0}$ are all distinct, $\{y^{(i)}\}_{1 \leq i \leq m_0}$ are all distinct, $\{X^{(i)}\}_{1 \leq i \leq m_1}$ are all distinct and $\{Y^{(i)}\}_{1 \leq i \leq m_1}$ are all distinct.

Then similarly to the proof of Theorem 3.1, denote by $\mathcal{C}_{\mathcal{D}}(v, V)$ the final output of $\mathcal{D}$.

Let $(\boldsymbol{v}, \boldsymbol{V})_{one} \stackrel{\text{def}}{=} \{(v, V) \mid \mathcal{C}_{\mathcal{D}}(v, V) = 1\}$ and $N_{one} \stackrel{\text{def}}{=} \#(\boldsymbol{v}, \boldsymbol{V})_{one}$.

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

$$\begin{aligned} p_R &= \Pr_{R,p}(\mathcal{D}^{R,R^{-1},p,p^{-1}}(1^{2n}) = 1) \\ &= \frac{\#\{(R,p) \mid \mathcal{D}^{R,R^{-1},p,p^{-1}}(1^{2n}) = 1\}}{(2^{2n})!(2^n)!} \ . \end{aligned}$$

For each $(v, V) \in (\boldsymbol{v}, \boldsymbol{V})_{one}$, the number of (R, p) such that

$$R(x^{(i)}) = y^{(i)} \text{ for } 1 \leq \forall i \leq m_0 \text{ and } p(X^{(i)}) = Y^{(i)} \text{ for } 1 \leq \forall i \leq m_1 \qquad (6)$$

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

$$\begin{aligned} p_R &= \sum_{(v,V) \in (\boldsymbol{v}, \boldsymbol{V})_{one}} \frac{\#\{(R,p) \mid (R,p) \text{ satisfying (6)}\}}{(2^{2n})!(2^n)!} \\ &= N_{one} \cdot \frac{(2^{2n} - m_0)!}{(2^{2n})!} \cdot \frac{(2^n - m_1)!}{(2^{2n})!} \ . \end{aligned}$$

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

$$p_\psi = \Pr_{h_1,p,h_5}(\mathcal{D}^{\psi,\psi^{-1},p,p^{-1}}(1^{2n}) = 1)$$

$$= \frac{\#\{(h_1,p,h_5) \mid \mathcal{D}^{\psi,\psi^{-1},p,p^{-1}}(1^{2n})=1\}}{(\#H_n^1)^2(2^n)!} \ .$$

Similarly to p_R, we have

$$p_\psi = \sum_{(v,V)\in(\boldsymbol{v},\boldsymbol{V})_{one}} \frac{\#\,\{(h_1,p,h_5) \mid (h_1,p,h_5) \text{ satisfying (5)}\}}{(\#H_n^1)^2(2^n)!} \ .$$

Then from Lemma 3.2, we obtain that

$$\begin{aligned}
p_\psi &\geq \sum_{(v,V)\in(\boldsymbol{v},\boldsymbol{V})_{one}} \frac{(2^n-2m_0-m_1)!\left(1-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n}\right)}{(2^n)!} \\
&= N_{one}\frac{(2^n-2m_0-m_1)!}{(2^n)!}\left(1-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n}\right) \\
&= p_R\frac{(2^{2n})!(2^n-2m_0-m_1)!}{(2^{2n}-m_0)!(2^n-m_1)!}\left(1-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n}\right) \ .
\end{aligned}$$

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

$$\begin{aligned}
p_\psi &\geq p_R\left(1-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n}\right) \\
&\geq p_R-2\epsilon\cdot m_0(m_0-1)-\frac{4m_0m_1}{2^n}-\frac{2m_0^2}{2^n} \\
&\geq p_R-2\epsilon\cdot m(m-1)-\frac{6m^2}{2^n} \ . \qquad (7)
\end{aligned}$$

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

$$1-p_\psi \geq 1-p_R-2\epsilon\cdot m(m-1)-\frac{6m^2}{2^n} \ . \qquad (8)$$

Finally, (7) and (8) give $|p_\psi-p_R| \leq 2\epsilon\cdot m(m-1)+\frac{6m^2}{2^n}$.

4 Negative result

Let g be a fixed and publicly known XOR-distinct permutation. In Theorem 3.2, we showed that $\psi(h_1,g,p,p^{-1},h_5^{-1})$ is super-pseudorandom even if the distinguisher has oracle access to p and p^{-1}, where h_1 and h_5 are uniform ϵ-XOR universal permutations, and p is a random permutation.

One might think that $\psi(h_1,g,p,p,h_5^{-1})$ is super-pseudorandom even if the distinguisher has oracle access to p and p^{-1}. In this section, however, we show that this is not true. We can distinguish $\psi(h_1,g,p,p,h_5^{-1})$ from a random permutation with advantage very close to 1.

More generally, let $p_1, p_2, p, p_5 \in P_n$ be random permutations and $\psi = \psi(p_1, p_2, p, p, p_5)$. We prove that ψ is not pseudorandom if the distinguisher has oracle access to p_2, p_2^{-1} and p. This proof implies that for any fixed and public g, $\psi(p_1, g, p, p, p_5)$ is not super-pseudorandom nor pseudorandom if the distinguisher has oracle access to p.

Define the advantage of $\mathcal{D}$ as follows.

$$\mathtt{Adv}(\mathcal{D}) \stackrel{\mathrm{def}}{=} |p_\psi - p_R|$$

where

$$\begin{cases} p_\psi \stackrel{\mathrm{def}}{=} \Pr(\mathcal{D}^{\psi, p_2, p_2^{-1}, p}(1^{2n}) = 1 \mid p_1, p_2, p, p_5 \stackrel{R}{\leftarrow} P_n, \psi = \psi(p_1, p_2, p, p, p_5)) \\ p_R \stackrel{\mathrm{def}}{=} \Pr(\mathcal{D}^{R, p_2, p_2^{-1}, p}(1^{2n}) = 1 \mid R \stackrel{R}{\leftarrow} P_{2n}, p_2, p \stackrel{R}{\leftarrow} P_n) \end{cases}$$

Theorem 4.1. *There exists a pseudorandom distinguisher $\mathcal{D}$ that has oracle access to p_2, p_2^{-1} and p and makes 6 queries in total,*

$$\mathtt{Adv}(\mathcal{D}) \geq 1 - \frac{2}{2^n} \ .$$

Proof. Let $\mathcal{O} = R$ or ψ. Our distinguisher $\mathcal{D}$ has oracle access to $\mathcal{O}$, p_2, p_2^{-1} and p. Consider the following $\mathcal{D}$:

1. Ask $(0, \ldots, 0) \in \{0,1\}^n$ to p_2^{-1} and obtain A.
2. Pick $X, A' \in \{0,1\}^n$ such that $A \neq A'$ arbitrarily.
3. Ask (X, A) to $\mathcal{O}$ and obtain (Y, B).
4. Ask $A \oplus A'$ to p_2 and obtain C.
5. Ask $A' \oplus B$ to p and obtain D.
6. Ask $A' \oplus B \oplus C$ to p and obtain E.
7. Ask $(X, A \oplus A')$ to $\mathcal{O}$ and obtain (Z, F).
8. Output "1" if and only if $F = A' \oplus B \oplus C \oplus D \oplus E$.

If $\mathcal{O} = \psi$, then B is the input to p in both third round and fourth round at step 3 since $p_2(A) = (0, \ldots, 0)$. Therefore we have $p_1(X) \oplus A = B$. Now the input to p in the third round at step 7 is $p_1(X) \oplus A \oplus A'$ which is equivalent to $A' \oplus B$. Next the input to p in the fourth round at step 7 is $A' \oplus B \oplus C$ since $p_2(A \oplus A') = C$. Then we always have $F = A' \oplus B \oplus C \oplus D \oplus E$ at step 8. Hence we have $p_\psi = 1$.

If $\mathcal{O} = R$, we have $p_R = \frac{2^n}{2^{2n}-1} \leq \frac{2}{2^n}$.

Corollary 4.1. *For any fixed and public g, $\psi(p_1, g, p, p, p_5)$ is not super-pseudorandom if the distinguisher has oracle access to p.*

Proof. From the proof of Theorem 4.1.

5 Conclusion

In this paper, we proposed more efficient constructions of super-pseudorandom permutations based on the five round MISTY type permutation than those given in [3] .

In particular, we showed that the second round permutation g need not be cryptographic at all, i.e., no randomness nor secrecy is required.

More precisely, let p and p_i be random permutations, then we proved that

1. $\psi(h_1, g, p, p^{-1}, h_5^{-1})$ is super-pseudorandom, where h_1 is an ϵ-XOR universal permutation, g is a (publicly known and fixed) XOR-distinct permutation, and h_5 is a uniform ϵ-XOR universal permutation (Theorem 3.1),
2. $\psi(h_1, g, p, p^{-1}, h_5^{-1})$ is super-pseudorandom, even if the adversary has oracle access to p and p^{-1}, where h_1 and h_5 are uniform ϵ-XOR universal permutations, and g is a (publicly known and fixed) XOR-distinct permutation (Theorem 3.2),
3. but $\psi(p_1, p_2, p, p, p_5)$ is *not* pseudorandom *nor* super-pseudorandom, if the adversary has oracle access to p_2, p_2^{-1} and p (Theorem 4.1).

References

1. J. L. Carter and M. N. Wegman. Universal classes of hash functions. *JCSS,* vol. 18, no. 2, pp. 143–154, 1979.
2. H. Gilbert and M. Minier. New results on the pseudorandomness of some block cipher constructions. Pre-proceedings of *Fast Software Encryption, FSE 2001,* pp. 260–277 (to appear in LNCS, Springer-Verlag).
3. T. Iwata, T. Yoshino, T. Yuasa and K. Kurosawa. Round security and super-pseudorandomness of MISTY type structure. Pre-proceedings of *Fast Software Encryption, FSE 2001*, pp. 245–259 (to appear in LNCS, Springer-Verlag).
4. 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.
5. S. Lucks. Faster Luby-Rackoff ciphers. *Fast Software Encryption, FSE '96, LNCS 1039,* pp. 189–203, Springer-Verlag.
6. 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.
7. M. Matsui. New block encryption algorithm MISTY. *Fast Software Encryption, FSE '97, LNCS 1267,* pp. 54–68, Springer-Verlag.
8. M. Naor and O. Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revised. *J. Cryptology,* vol. 12, no. 1, pp. 29–66, Springer-Verlag, 1999.
9. Z. Ramzan and L. Reyzin. On the round security of symmetric-key cryptographic primitives. *Advances in Cryptology — CRYPTO 2000, LNCS 1880,* pp. 376–393, Springer-Verlag, 2000.
10. 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.
11. M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *JCSS,* vol. 22, no. 3, pp. 265–279, 1981.

Appendix A. Proof of Lemma 3.1

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

Number of h_1. First, for any fixed i and j such that $1 \le i < j \le m$:

– if $x_L^{(i)} = x_L^{(j)}$, then there exists no h_1 such that

$$h_1(x_L^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus x_R^{(j)} \tag{9}$$

since $x_L^{(i)} = x_L^{(j)}$ implies $x_R^{(i)} \ne x_R^{(j)}$;

– if $x_L^{(i)} \ne x_L^{(j)}$, then the number of h_1 which satisfies (9) is at most $\epsilon \# H_n^0$ since h_1 is an ϵ-XOR universal permutation.

Therefore, the number of h_1 such that

$$h_1(x_L^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus x_R^{(j)} \text{ for } 1 \le \exists i < \exists j \le m \tag{10}$$

is at most $\epsilon \binom{m}{2} \# H_n^0$.

Next, for any fixed i and j such that $1 \le i < j \le m$:

– if $x_L^{(i)} = x_L^{(j)}$, then there exists no h_1 such that

$$h_1(x_L^{(i)}) \oplus g(x_R^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus g(x_R^{(j)}) \oplus x_R^{(j)} \tag{11}$$

since $x_L^{(i)} = x_L^{(j)}$ implies $x_R^{(i)} \ne x_R^{(j)}$, and our XOR-distinct g guarantees $g(x_R^{(i)}) \oplus x_R^{(i)} \ne g(x_R^{(j)}) \oplus x_R^{(j)}$;

– if $x_L^{(i)} \ne x_L^{(j)}$, then the number of h_1 which satisfies (11) is at most $\epsilon \# H_n^0$ since h_1 is an ϵ-XOR universal permutation.

Therefore, the number of h_1 such that

$$h_1(x_L^{(i)}) \oplus g(x_R^{(i)}) \oplus x_R^{(i)} = h_1(x_L^{(j)}) \oplus g(x_R^{(j)}) \oplus x_R^{(j)} \text{ for } 1 \le \exists i < \exists j \le m \tag{12}$$

is at most $\epsilon \binom{m}{2} \# H_n^0$.

Then, from (10) and (12), the number of h_1 such that

$$\left.\begin{array}{l} h_1(x_L^{(i)}) \oplus x_R^{(i)} \ne h_1(x_L^{(j)}) \oplus x_R^{(j)} \text{ for } 1 \le \forall i < \forall j \le m, \text{ and} \\ h_1(x_L^{(i)}) \oplus g(x_R^{(i)}) \oplus x_R^{(i)} \ne h_1(x_L^{(j)}) \oplus g(x_R^{(j)}) \oplus x_R^{(j)} \text{ for } 1 \le \forall i < \forall j \le m \end{array}\right\} \tag{13}$$

is at least $\# H_n^0 - 2\epsilon \binom{m}{2} \# H_n^0$. Fix h_1 which satisfies (13) arbitrarily. This implies that $I_3^{(1)}, \dots, I_3^{(m)}$ and $O_4^{(1)}, \dots, O_4^{(m)}$ are fixed in such a way that:

– $I_3^{(i)} \ne I_3^{(j)}$ for $1 \le \forall i < \forall j \le m$, and

– $O_4^{(i)} \neq O_4^{(j)}$ for $1 \leq \forall i < \forall j \leq m$.

Number of h_5. Similarly, the number of h_5 such that

$$\left.\begin{array}{l} h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq h_5(y_L^{(j)} \oplus y_R^{(j)}) \oplus y_R^{(j)} \text{ for } 1 \leq \forall i < \forall j \leq m, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus O_4^{(i)} \neq h_5(y_L^{(j)} \oplus y_R^{(j)}) \oplus O_4^{(j)} \text{ for } 1 \leq \forall i < \forall j \leq m, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus O_4^{(i)} \neq O_4^{(j)} \text{ for } 1 \leq \forall i, \forall j \leq m, \text{ and} \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq I_3^{(j)} \text{ for } 1 \leq \forall i, \forall j \leq m, \end{array}\right\} \quad (14)$$

is at least $\#H_n^1 - 2\epsilon\binom{m}{2}\#H_n^1 - \frac{2m^2\#H_n^1}{2^n}$. Fix h_5 which satisfies (14) arbitrarily. This implies that $O_3^{(1)}, \ldots, O_3^{(m)}$ and $I_4^{(1)}, \ldots, I_4^{(m)}$ are fixed in such a way that:

– $I_4^{(i)} \neq I_4^{(j)}$ for $1 \leq \forall i < \forall j \leq m$,
– $O_3^{(i)} \neq O_3^{(j)}$ for $1 \leq \forall i < \forall j \leq m$,
– $O_3^{(i)} \neq O_4^{(j)}$ for $1 \leq \forall i, \forall j \leq m$, and
– $I_4^{(i)} \neq I_3^{(j)}$ for $1 \leq \forall i, \forall j \leq m$.

Number of p. Now h_1 and h_5 are fixed in such a way that

$$I_3^{(1)}, \ldots, I_3^{(m)}, I_4^{(1)}, \ldots, I_4^{(m)}$$

(which are inputs to p) are all distinct and

$$O_3^{(1)}, \ldots, O_3^{(m)}, O_4^{(1)}, \ldots, O_4^{(m)}$$

(which are corresponding outputs of p) are all distinct. In other words, for p, the above $2m$ input-output pairs are determined. The other $2^n - 2m$ input-output pairs are undetermined. Therefore we have $(2^n - 2m)!$ possible choice of p for any such fixed h_1 and h_5.

To summarize, we have:

– at least $\#H_n^0 - 2\epsilon\binom{m}{2}\#H_n^0$ choice of h_1,
– at least $\#H_n^1 - 2\epsilon\binom{m}{2}\#H_n^1 - \frac{2m^2\#H_n^1}{2^n}$ choice of h_5 when h_1 is fixed, and
– $(2^n - 2m)!$ choice of p when h_1 and h_5 are fixed.

Then the number of $\psi \in \mathrm{MISTY}_{2n}^{01}$ which satisfy (1) is at least

$$\begin{aligned} &(\#H_n^0)(\#H_n^1)(2^n - 2m)!\left(1 - 2\epsilon\binom{m}{2}\right)\left(1 - 2\epsilon\binom{m}{2} - \frac{2m^2}{2^n}\right) \\ &\geq (\#H_n^0)(\#H_n^1)(2^n - 2m)!\left(1 - 2\epsilon \cdot m(m-1) - \frac{2m^2}{2^n}\right) \end{aligned}$$

This concludes the proof of the lemma.

Appendix B. Proof of Lemma 3.2

We use the same definition of $I_3^{(i)}$, $O_3^{(i)}$, $I_4^{(i)}$ and $O_4^{(i)}$ as in the proof of Lemma 3.1.

Number of h_1. First, similarly to the proof of Lemma 3.1, the number of h_1 such that

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

is at least $\#H_n^1 - 2\epsilon\binom{m_0}{2}\#H_n^1 - \frac{2m_0m_1\#H_n^1}{2^n}$. Fix h_1 which satisfies (15) arbitrarily. This implies that $I_3^{(1)}, \ldots, I_3^{(m_0)}$ and $O_4^{(1)}, \ldots, O_4^{(m_0)}$ are fixed in such a way that:

- $I_3^{(i)} \neq I_3^{(j)}$ for $1 \leq \forall i < \forall j \leq m_0$,
- $I_3^{(i)} \neq X^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$,
- $O_4^{(i)} \neq O_4^{(j)}$ for $1 \leq \forall i < \forall j \leq m_0$, and
- $O_4^{(i)} \neq Y^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$.

Number of h_5. Similarly, the number of h_5 such that

$$\left.\begin{array}{l} h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq h_5(y_L^{(j)} \oplus y_R^{(j)}) \oplus y_R^{(j)} \text{ for } 1 \leq \forall i < \forall j \leq m_0, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq X^{(j)} \text{ for } 1 \leq \forall i \leq m_0 \text{ and } 1 \leq \forall j \leq m_0, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus O_4^{(i)} \neq h_5(y_L^{(j)} \oplus y_R^{(j)}) \oplus O_4^{(j)} \text{ for } 1 \leq \forall i < \forall j \leq m_0, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus O_4^{(i)} \neq Y^{(j)} \text{ for } 1 \leq \forall i \leq m_0 \text{ and } 1 \leq \forall j \leq m_0, \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus O_4^{(i)} \neq O_4^{(j)} \text{ for } 1 \leq \forall i, \forall j \leq m_0, \text{ and} \\ h_5(y_L^{(i)} \oplus y_R^{(i)}) \oplus y_R^{(i)} \neq I_3^{(j)} \text{ for } 1 \leq \forall i, \forall j \leq m_0, \end{array}\right\} \tag{16}$$

is at least $\#H_n^1 - 2\epsilon\binom{m_0}{2}\#H_n^1 - \frac{2m_0m_1\#H_n^1}{2^n} - \frac{2m_0^2\#H_n^1}{2^n}$. Fix h_5 which satisfies (16) arbitrarily. This implies that $O_3^{(1)}, \ldots, O_3^{(m_0)}$ and $I_4^{(1)}, \ldots, I_4^{(m_0)}$ are fixed in such a way that:

- $I_4^{(i)} \neq I_4^{(j)}$ for $1 \leq \forall i < \forall j \leq m_0$,
- $I_4^{(i)} \neq X^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$,
- $O_3^{(i)} \neq O_3^{(j)}$ for $1 \leq \forall i < \forall j \leq m_0$,
- $O_3^{(i)} \neq Y^{(j)}$ for $1 \leq \forall i \leq m_0$ and $1 \leq \forall j \leq m_1$,
- $O_3^{(i)} \neq O_4^{(j)}$ for $1 \leq \forall i, \forall j \leq m_0$, and
- $I_4^{(i)} \neq I_3^{(j)}$ for $1 \leq \forall i, \forall j \leq m_0$.

Number of p. Now h_1 and h_5 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. Then we have $(2^n - 2m_0 - m_1)!$ possible choice of p for any such fixed h_1 and h_5.

To summarize, we have:

- at least $\#H_n^1 - 2\epsilon\binom{m_0}{2}\#H_n^1 - \frac{2m_0m_1\#H_n^1}{2^n}$ choice of h_1,
- at least $\#H_n^1 - 2\epsilon\binom{m_0}{2}\#H_n^1 - \frac{2m_0m_1\#H_n^1}{2^n} - \frac{2m_0^2\#H_n^1}{2^n}$ choice of h_5 when h_1 is fixed, and
- $(2^n - 2m_0 - m_1)!$ choice of p when h_1 and h_5 are fixed.

Then the number of $\psi \in \mathrm{MISTY}_{2n}^{11}$ which satisfy (5) is at least

$$\begin{aligned}
&(\#H_n^1)^2(2^n - 2m_0 - m_1)! \\
&\qquad \times \left(1 - 2\epsilon\binom{m_0}{2} - \frac{2m_0m_1}{2^n}\right)\left(1 - 2\epsilon\binom{m_0}{2} - \frac{2m_0m_1}{2^n} - \frac{2m_0^2}{2^n}\right) \\
&\quad \geq (\#H_n^1)^2(2^n - 2m_0 - m_1)!\left(1 - 2\epsilon \cdot m_0(m_0 - 1) - \frac{4m_0m_1}{2^n} - \frac{2m_0^2}{2^n}\right)
\end{aligned}$$

This concludes the proof of the lemma.