A Construction for Super Pseudorandom Permutations from A Single Pseudorandom Function

Babak Sadeghiyan ^{*} Josef Pieprzyk [†]

Abstract

In this paper, we show how to construct a super pseudorandom permutation generator from a single pseudorandom function generator, based on DES-like permutations. First, we show $\psi(g, 1, f, g, 1, f)$, which consists of six rounds of DES-like permutations with two different pseudorandom functions and a fixed permutation, is super pseudorandom. Then, we show that with replacing a two-fold composition of one of the pseudorandom functions instead of the other one it is possible to construct a super pseudorandom permutation from a single pseudorandom function, where we need six rounds of DES-like permutations and six references to the pseudorandom function.

1 Introduction

Pseudorandom bit generators have many cryptographic applications. Classical pseudorandom bit generators are deterministic algorithms which generate binary strings that look like a truly random one. A pseudorandom bit generator passes a given test if the results of the test are similar for both the pseudorandom and a truly random one. If the statistics of pseudorandom generated strings are different from the statistics of truly random ones, the bit generator fails some statistical test. However, even if a generator passes all known statistical tests, it is sometimes possible to predict the next bit knowing some previous ones. The notion of unpredictability of the next bit was first introduced by Yao [6]. He showed that a generated string is indistinguishable from a random one, if and only if, knowing the first s bits of the string, predicting the $s + 1$ bit is difficult, in other words

^{*}Department of Computer Science, University College, University of New South Wales, Australian Defence Force Academy, Canberra, A.C.T. 2600, Australia.

[†]Department of Computer Science, University of Wollongong, Wollongong, N.S.W. 2500, Australia.

the next bit is unpredictable. Goldreich, Goldwasser and Micali introduced the notion of pseudorandom function generators [1] and showed how to construct a pseudorandom function generator from a pseudorandom bit generator adopting Yao's unpredictability property of the next bit.

Luby and Rackoff showed how to construct a pseudorandom invertible permutation generator with three pseudorandom function generators and application of three rounds of DES-like permutations [2] (this structure is notated as $\psi(h, g, f)$). A practical implication of their work is that a private key block cipher which can be proven to be secure against chosen plaintext attack can be constructed. Their result is quite astonishing since it is not based on any unproven hypothesis.

Later Pieprzyk [4] showed that it is possible to construct a pseudorandom permutation generator based on a single pseudorandom function and four rounds of DES-like permutations, i.e., $\psi(f^2, f, f, f)$ is pseudorandom and it is secure against a chosen plaintext attack. Luby and Rackoff also introduced the notion of super pseudorandomness, where the block cryptosystem is secure against a chosen plaintext/ciphertext attack. They suggested that $\psi(h, g, f, e)$ is super pseudorandom, which is a structure with four pseudorandom functions in four DES-like permutations. Recently, in [5] the necessary and sufficient conditions for the construction of super pseudorandom permutation generators based on DES-like permutations have been investigated and it has been suggested that $\psi(g, g, f, f)$ is super pseudorandom, which is a structure with two pseudorandom functions and four DES-like permutations.

It is a question of how to construct super pseudorandom permutations from a single pseudorandom function.

In this paper, we answer the above question and present a construction based on a single pseudorandom function which is super pseudorandom. We take advantage of the structure of the optimal perfect randomiser $\psi(g, 1, f, g, 1, f)$ presented in [3], where not only the output is independent from the input but also the two branches of the output are independent of each other. First, we show that the perfect randomiser is super pseudorandom. Then, we present a construction based on a single pseudorandom function, with replacing a two-fold composition of one of the pseudorandom functions instead of the other one, i.e., $\psi(f^2, 1, f, f^2, 1, f)$, which is indistinguishable from the randomiser. Finally, we show that the presented construction is super pseudorandom. Hence, it is possible to construct a super pseudorandom permutation from a single pseudorandom function, where we need six rounds of DES-like permutations and six references to the pseudorandom function.

2 Notations

The notation we use, is similar to [4]. The set of all integers is denoted by $\mathbb{N}$. Let $\Sigma = \{0, 1\}$ be the alphabet we consider. For $n \in \mathbb{N}$, Σ^n is the set of all 2^n binary strings of length n . The concatenation of two binary strings x, y is denoted by $x \parallel y$. The bit by bit exclusive-OR of x and y is denoted by $x \oplus y$. By $x \in_r S$ we mean that x is chosen from a set S uniformly at random. By f a function we mean a trasformation from Σ^n to Σ^n . The set of all functions on Σ^n is denoted by H_n , i.e., $H_n = \{f \mid f : \Sigma^n \rightarrow \Sigma^n\}$ and it consists of 2^{n2^n} elements. The composition of two functions f and g is defined as $f \circ g(x) = f(g(x))$. The i -fold composition of f is denoted by f^i . A function f is a permutation if it is a 1 to 1 and onto function. The set of all permutations on Σ^n is defined by P_n and it consists of $2^n!$ elements.

3 Preliminaries

This section provides the preliminary definitions and notions which are used throughout the paper.

Definition 1 We associate with a function $f \in H_n$ the DES-like permutation $D_{2n,f} \in P_{2n}$ as,

$$D_{2n,f}(L \parallel R) = (R \oplus f(L) \parallel L)$$

where R and L are n -bit strings, i.e., $R, L \in \Sigma^n$.

Definition 2 Having a sequence of functions $f_1, f_2, \dots, f_i \in H_n$, we define the composition of their DES-like permutations as $\psi \in P_{2n}$, where

$$\psi(f_i, \dots, f_2, f_1) = D_{2n,f_i} \circ D_{2n,f_{i-1}} \circ \dots \circ D_{2n,f_1}$$

Definition 3 Let $l(n)$ be a polynomial in n , a function generator $F = \{F_n : n \in \mathbb{N}\}$ is a collection of functions with the following properties:

- *Indexing:* Each F_n specifies for each k of length $l(n)$ a function $f_{n,k} \in H_n$.
- *Poly-time evaluation:* Given a key $k \in \Sigma^{l(n)}$, and a string $x \in \Sigma^n$, $f_{n,k}(x)$ can be computed in polynomial time in n .

Definition 4 An oracle circuit C_n is an acyclic circuit which contains Boolean gates of type AND, OR and NOT, and constant gates of type zero and one, and a particular kind of gates named oracle gates. Each oracle gate has an n -bit input and an n -bit output and it is evaluated using some function from H_n . The oracle circuit C_n has a single bit output.

Definition 5 The size of an oracle circuit C_n is the total number of connections between gates, Boolean gates, constant gates and oracle gates.

Definition 6 A distinguishing circuit family for a function generator F is an infinite family of circuits $\{C_{n_1}, C_{n_2}, \dots\}$, where $n_1 < n_2 < \dots$, such that for some pair of constants c_1 and c_2 and for each n there exist a circuit C_n such that:

- The size of C_n is less than or equal to n^{c_1} .
- Let $\text{Prob}\{C_n[H_n] = 1\}$ be the probability that the output bit of C_n is one when a function is randomly selected from H_n and used to evaluate oracle gates. Let $\text{Prob}\{C_n[F_n] = 1\}$ be the probability that the output bit of C_n is one when a key k of length $l(n)$ is randomly chosen and $f_{n,k}$ is used to evaluate the oracle gates.

The distinguishing probability for C_n is greater than or equal to $\frac{1}{n^{c_2}}$, that is,

$$|\text{Prob}\{C_n[H_n] = 1\} - \text{Prob}\{C_n[F_n] = 1\}| \geq \frac{1}{n^{c_2}}$$

Definition 7 A function generator F is pseudorandom if there is no distinguishing circuit family for F .

How to construct pseudorandom permutation from pseudorandom functions was first presented by Luby and Rackoff applying a DES-like structure. The following lemma is due to Luby and Rackoff and has been stated in [2] as the main lemma.

Lemma 1 Let $f_1, f_2, f_3 \in_r H_n$ be independent random functions and C_{2n} be an oracle circuit with $m < 2^n$ oracle gates, then

$$|\text{Prob}\{C_{2n}[P_{2n}] = 1\} - \text{Prob}\{C_{2n}[\psi(f_3, f_2, f_1)] = 1\}| \leq \frac{m^2}{2^n}$$

In other words, a block cryptosystem with three rounds of DES-like permutation and three different random functions is secure against chosen plaintext attack, when a cryptanalyst can ask for only a polynomial number of plaintexts. Later, Pieprzyk et al. considered the composition of Luby - Rackoff modules in [3]. They showed that the composition of two Luby - Rackoff modules where the intermediate layers are replaced with random permutations, would produce a pseudorandom permutation where not only the output is independent of the input but the two branches of output are also independent of each other. In [3], it was also suggested that the independency of output branches would still be held even if the intermediate layers are replaced with some fixed permutation. The following theorem is from [3], but is stated in a different word.

Theorem 1 Let $f_1, f_2, h_1, h_2 \in_r H_n$ be four different random functions. There is no distinguishing circuit for $\Psi_2 = \psi(h_2, 1, f_2) \circ \psi(h_1, 1, f_1)$, and it is also a perfect randomiser, i.e., for all oracle gates used by the distinguishing circuit, the outputs are independent from the inputs and are independent from each other.

When the block cryptosystem is secure against chosen plaintext / ciphertext attack, it is called super pseudorandom. This notion only applies for invertible permutations and is stated formally in three following definitions.

Definition 8 A permutation generator F is a function generator such that each function $f_{n,k}$ is 1 to 1 and onto. Let $\overline{F} = \{\overline{F}_n : n \in N\}$, where $\overline{F}_n = \{\overline{f}_{n,k} : k \in \Sigma^{l(n)}\}$, where $\overline{f}_{n,k}$ is the inverse function of $f_{n,k}$. F is called invertible if $\overline{F}$ is also a permutation generator.

Definition 9 A super distinguishing family of circuits for an invertible permutation generator F is an infinite family of circuits $\{SC_{n_1}, SC_{n_2}, \dots\}$, where $n_1 < n_2 < \dots$, where each circuit is an oracle circuit containing two types of oracle gates, normal and inverse, such that for some pair of constants c_1 and c_2 and for each n there exist a circuit SC_n such that:

- The size of SC_n is less than or equal to n^{c_1} .
- Let $\text{Prob}\{SC_n[P_n] = 1\}$ be the probability that the output bit of SC_n is one when a permutation p is randomly selected from P_n and p and $\overline{p}$ are used to evaluate normal and inverse oracle gates. Let $\text{Prob}\{SC_n[F_n] = 1\}$ be the probability that the output bit of SC_n is one when a key k of length $l(n)$ is randomly chosen and $f_{n,k}$ and $\overline{f}_{n,k}$ is used to evaluate the normal and inverse oracle gates respectively.

The distinguishing probability for SC_n is greater than or equal to $\frac{1}{n^{c_2}}$, that is,

$$|\text{Prob}\{SC_n[P_n] = 1\} - \text{Prob}\{SC_n[F_n] = 1\}| \geq \frac{1}{n^{c_2}}$$

Definition 10 A permutation generator F is super pseudorandom if there is no super distinguishing circuit family for F .

If F is a super pseudorandom permutation generator, it is secure against a chosen plaintext/ciphertext attack where a cryptanalyst can interactively choose plain blocks and see their encryptions and choose encryptions and see their corresponding plaintext blocks.

4 Construction of Super Pseudorandom Permutations

Luby and Rackoff [2] suggested that, it is possible to make a super pseudorandom permutation with four independent random functions, i.e., if $f_1, f_2, f_3, f_4 \in H_n$ are independent random functions then $\psi(f_4, f_3, f_2, f_1)$ is a super pseudorandom permutation. It is a matter of question whether it is possible to build a super pseudorandom permutation with a single random functions.

First a definition for independent permutations is given, which would be used in the proof of Theorem 2.

Definition 11 A D -distinguishing family of circuits for two invertible pseudorandom permutation generators (Π_1, Π_2) is an infinite family of circuits $\{DC_{n_1}, DC_{n_2}, \dots\}$, where $n_1 < n_2 < \dots$, where each circuit is an oracle circuit containing two types of oracle gates, such that for some pair of constants c_1 and c_2 and for each n there exist a circuit DC_n such that:

- The size of DC_n is less than or equal to n^{c_1} .
- Let $\text{Prob}\{DC_n[P_n, P_n] = 1\}$ be the probability that the output bit of DC_n is 1, when two permutations p_1 and p_2 are chosen independently and randomly from P_n and are used to evaluate the two types of oracle gates of DC_n respectively. Let $\text{Prob}\{DC_n[\Pi_1, \Pi_2] = 1\}$ be the probability that the output bit of DC_n is one when a key k of length $l(n)$ is randomly chosen and $p_{1,k}$ and $p_{2,k}$ are used to evaluate the two types of oracle gates respectively.

The distinguishing probability for DC_n is greater than or equal to $\frac{1}{n^{c_2}}$, that is,

$$|\text{Prob}\{DC_n[P_n, P_n] = 1\} - \text{Prob}\{DC_n[\Pi_1, \Pi_2] = 1\}| \geq \frac{1}{n^{c_2}}$$

Definition 12 Two pseudorandom permutation generators Π_1 and Π_2 , are two independent permutation generators, if there is no D -distinguishing oracle circuit family for (Π_1, Π_2) .

Note that, the D -distinguishing oracle circuits are generalizations of the distinguishing circuits and the super distinguishing circuits, if two simple circuits be excluded. If there is no D -distinguishing circuit for a permutation generator $(\Pi_1 \text{ and } \Pi_1)$, then there is no distinguishing circuit family for Π_1 , provided that the D -distinguishing circuit is not an identity test, (e.g., giving an input to two types of oracles and comparing the outputs). Moreover, if there is no D -distinguishing circuit for a permutation generator Π_1 and its inverse $\bar{\Pi}_1$, then there is no super distinguishing circuit family for Π_1 provided that the D -distinguishing circuit is not an inversion test, (e.g., giving an input to one type of oracle and feeding the other type of oracle with this result and comparing the output with the original input).

4.1 Super Pseudorandomness of $\psi(h, 1, f, h, 1, f)$

To construct a super pseudorandom permutation generator based on a single pseudorandom function, we first show that $G_1 = \psi(h, 1, f) \circ \psi(h, 1, f)$ is a super pseudorandom permutation generator, then, we show that if h is substituted with f^2 , $G_1 = \psi(f^2, 1, f, f^2, 1, f)$ would remain super pseudorandom. To show that G_1 is a super pseudorandom permutation generator, we first show that $G_2 = \psi(h, 1, f, h, 1)$ and $G_3 = \psi(f, 1, h, f, 1)$ are not only pseudorandom but also two independent permutations. Then we show that G_1 is super pseudorandom.

Lemma 2 Let $h, f \in_r H_n$ be independent random functions and $G_2 = \psi(h, 1, f, h, 1)$ then

$$| \text{Prob}\{C_{2n}[G_2] = 1\} - \text{Prob}\{C_{2n}[P_{2n}] = 1\} | \leq \frac{m^2}{2^n} + \frac{m^2}{2^{2n}}$$

where C_{2n} is any polynomial size distinguishing circuit with $m < 2^n$ oracle gates.

Proof :

When the distinguisher examines an oracle, the input is a $2n$ bit string $(L \parallel R)$ and the output would also be a $2n$ bit string $(S \parallel T)$ where

$$\begin{aligned} S &= L \oplus R \oplus f(L \oplus h(L \oplus R)) \oplus h(R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R))) \\ T &= R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R)) \end{aligned}$$

For two different experiments, $(L_i \parallel R_i)$ should be different from $(L_j \parallel R_j)$, so either $L_i \neq L_j$ or $R_i \neq R_j$ or both are different. If there is no leakage of information from the input to the output, the distinguisher cannot make any sensible decision on the generator used to evaluate the oracle gates. The leakage of information happens when there are at least one pair of oracle gates such that their outputs are related to their inputs. Let X be a random variable notating the output of h , the random function in the second round of the DES-like structure of G_2 , and let Y be a random variable notating the output of f , the random function in the third round of DES-like structure of G_2 (see Figure 1).

Figure 1: Random variables X and Y in G_2

The leakage of information happens in two cases:

1. X is bad: it happens when there are a pair of oracle gates O_i, O_j with the input random variables $R_i \neq R_j$ and $L_i = L_j = L$ such that the random function h

collides. Hence, for this case we assume that $x_i = x_j = x$ where $x_i = h(L \oplus R_i)$ and $x_j = h(L \oplus R_j)$. It is obvious that if X is bad then always $T_i \oplus T_j = R_i \oplus R_j$. The probability that h collides in a pair of oracle gates among m oracles would be equal to $\frac{m(m-1)}{2} \frac{1}{2^n}$.

2. Y is bad: it happens when there are a pair of oracle gates O_i, O_j with the input random variables $R_i = R_j = R$ and $L_i \neq L_j$ such that the random function f collides. Hence, for this case we assume that $y_i = y_j = y$ where $y_i = f(L_i \oplus h(L_i \oplus R))$ and $y_j = f(L_j \oplus h(L_j \oplus R))$. It is obvious that if Y is bad and also X is bad then always $T_i \oplus T_j = L_i \oplus L_j$. The probability that f collides and also h collides in a pair of oracle gates among m oracles would be equal to $\frac{m(m-1)}{2} \frac{1}{2^{2n}}$.

The probability that a distinguishing circuit for G_2 could be constructed would be equal to $\frac{m(m-1)}{2^{n+1}} + \frac{m(m-1)}{2^{2n+1}}$. On the other hand, when a permutation p is chosen randomly, the probability that p can satisfy the distinguishing circuit relation is $\frac{m}{2^n} + \frac{m}{2^{2n}}$. So, an upper bound on the probability of distinguishing would be

$$| \text{Prob}\{C_{2n}[P_{2n}] = 1\} - \text{Prob}\{C_{2n}[\psi(h, 1, f, h, 1)] = 1\} | \leq \frac{m^2}{2^n} + \frac{m^2}{2^{2n}}$$

□

Lemma 3 Let $h, f \in_r H_n$ be independent random functions and $G_3 = \psi(f, 1, h, f, 1)$, then

$$| \text{Prob}\{C_{2n}[G_3] = 1\} - \text{Prob}\{C_{2n}[P_{2n}] = 1\} | \leq \frac{m^2}{2^n} + \frac{m^2}{2^{2n}}$$

where C_{2n} is a distinguishing circuit with $m < 2^n$ oracle gates.

Proof : Since structure of G_3 is similar to the structure of G_2 except that the locations for g and f are replaced, a proof similar to the proof of Lemma 2 can be suggested for the probability of distinguishing of G_3 from a random permutation, and is omitted here. □

Note that when m is a polynomial in n , the probability of distinguishing G_2 or G_3 from a random permutation becomes less than 1 over any polynomial in n .

Lemma 4 Let $h, f \in_r H_n$ be independent random functions, and $G_2 = \psi(h, 1, f, h, 1)$ and $G_3 = \psi(f, 1, h, f, 1)$, then

$$| \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | \leq \frac{m^2}{2^{2n}}$$

where DC_{2n} is a D -distinguishing circuit with two types of oracle gates and $m < 2^n$ the number of oracle gates.

Proof : As the distinguisher has two types of oracle gates, one probability is calculated when two permutations are chosen independently and randomly from P_{2n} and are used to evaluate the oracle gates. The other probability is calculated when the distinguisher chooses f, h independently and randomly from H_n and uses them in the G_2 and G_3 structures, which are applied for the evaluation of the oracle gates. When the distinguisher examines an oracle, the input is a $2n$ bit string ($L \parallel R$) and the output would also be a $2n$ bit string ($S \parallel T$).

When G_2 is examined the output would be

$$\begin{aligned} S &= L \oplus R \oplus f(L \oplus h(L \oplus R)) \oplus h(R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R))) \\ T &= R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R)) \end{aligned}$$

and when G_3 is examined the output would be

$$\begin{aligned} S &= L \oplus R \oplus h(L \oplus f(L \oplus R)) \oplus f(R \oplus f(L \oplus R) \oplus h(L \oplus f(L \oplus R))) \\ T &= R \oplus f(L \oplus R) \oplus h(L \oplus f(L \oplus R)) \end{aligned}$$

As both G_2 and G_3 are pseudorandom, there is no leakage of information from their input to their output. The D -distinguisher could only make a decision if there were at least one pair of oracle gates such that their outputs were related to each other.

Let X_2 be a random variable notating the output of h , the random function in the second round of the DES-like structure of G_2 , and X_3 be a random variable notating the output of f , the random function in the second round of the DES-like structure of G_3 . Let Y_2 be a random variable notating the output of f , the random function in the third round of DES-like structure of G_2 , and Y_3 be a random variable notating the output of h , the random function in the third round of DES-like structure of G_3 (see Figure 2).

The distinguisher can make a sensible decision if any of the two following cases happens:

1. When there are a pair of oracle gates O_i, O_j such that the random functions f and h collide: Hence, for this case we assume that $x_{i,2} = x_{j,3} = x$ where $x_{i,2} = h(L_i \oplus R_i)$ and $x_{j,3} = f(L_j \oplus R_j)$ and $y_{i,2} = y_{j,3} = y$ where $y_{i,2} = f(L_i \oplus h(L_i \oplus R_i))$ and $y_{j,3} = h(L_j \oplus f(L_j \oplus R_j))$.

In this case, when the input random variables $R_i \neq R_j$ and $L_i = L_j = L$ then always $T_i \oplus T_j = R_i \oplus R_j$, and when the input random variables $R_i = R_j = R$ and $L_i \neq L_j$ then always $S_i \oplus S_j = L_i \oplus L_j$. The probability that f and h collide in a pair of oracle gates among m oracles would be equal to $\frac{m(m-1)}{2} \frac{1}{2^{2n}}$.

2. When there are a pair of oracle gates O_i, O_j such that the random function f collides and the random function h collides: For this case we assume that $x_{i,2} = y_{j,3}$ where $x_{i,2} = h(L_i \oplus R_i)$ and $y_{j,3} = h(L_j \oplus f(L_j \oplus R_j))$, and $y_{i,2} = x_{j,3}$ where $y_{i,2} = f(L_i \oplus h(L_i \oplus R_i))$ and $x_{j,3} = f(L_j \oplus R_j)$

Figure 2: X_3, Y_3 random variables in G_3 and X_2, Y_2 in G_2

In this case, when the input random variables $R_i \neq R_j$ and $L_i = L_j = L$ then always $T_i \oplus T_j = R_i \oplus R_j$. The probability that f collides and also h collides in a pair of oracle gates among m oracles would be equal to $\frac{m(m-1)}{2} \frac{1}{2^{2n}}$.

The probability that a D -distinguishing circuit could be constructed for (G_2, G_3) would be equal to $\frac{m(m-1)}{2^{2n+1}} + \frac{m(m-1)}{2^{2n+1}}$. On the other hand, when two permutations p_1 and p_2 are chosen independently and randomly the probability that they can satisfy the distinguishing circuit relation would be $\frac{2m}{2^{2n}}$. So, an upper bound on the probability of distinguishing would be

$$|\text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} - \text{Prob}\{DC_{2n}[G_2, G_3] = 1\}| \leq \frac{m^2}{2^{2n}}$$

□

Theorem 2 Let $f_1, f_2 \in_r F_n$ be independently chosen pseudorandom functions, and $G_2 = \psi(f_2, 1, f_1, f_2, 1)$ and $G_3 = \psi(f_1, 1, f_2, f_1, 1)$. When

$$|\text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\}| < \frac{1}{n^{c_2}}$$

for any polynomial size D -distinguishing circuit and for any constant c_2 , then $G_1 = \psi(f_2, 1, f_1, f_2, 1, f_1)$ is a super pseudorandom permutation generator.

Proof: First, it is necessary to show that $G_3 = \psi(f_1, 1, f_2, f_1, 1)$ and $\bar{G}_1 = \psi(f_1, 1, f_2, f_1, 1, f_2)$ are independent of each other. In order to prove this claim, by contradiction assume that they are not independent, and there is a D -distinguishing circuit such that for a constant c_2

$$|\text{Prob}\{DC_{2n}[G_3, \bar{G}_1] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\}| > \frac{1}{n^{c_2}}$$

Without changing the inequality relation, we have,

$$| \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} + \\ \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | > \frac{1}{n^{c_2}}$$

then,

$$| \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} | + \\ | \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | > \frac{1}{n^{c_2}}$$

If $| \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | > \frac{1}{n^{c_2}}$, G_3 would not be pseudorandom, as the D -distinguishing circuit is not a test for identity. This contradicts Lemma 3. Furthermore, if $| \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_3, G_3] = 1\} | > \frac{1}{n^{c_2}}$, then the oracle circuit virtually distinguishes f_1 from a randomly chosen function. This also contradicts our assumption that f_1 is a pseudorandom function. Since both cases conclude to contradictions, then G_3 and $\overline{G}_1$ should be independent of each other, and there would be no D -distinguishing circuit for $(\overline{G}_1, G_3)$.

Considering the independency of G_2 and G_3 , it is given that

$$| \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | < \frac{1}{n^{c_2}}$$

Note that G_2 and G_3 are not inverse of each other, so the D -distinguishing circuit cannot be a test for inversion. Without changing the sign of inequality, the above relation can be expanded as,

$$| \text{Prob}\{DC_{2n}[G_1, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_1, \overline{G}_1] = 1\} + \\ \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} + \\ \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | < \frac{1}{n^{c_2}}$$

With reordering and separation of absolute values, we get:

$$|| \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} | - \\ | \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_1, \overline{G}_1] = 1\} | - \\ | \text{Prob}\{DC_{2n}[G_1, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} || < \frac{1}{n^{c_2}}$$

Since, it was assumed that G_2 and G_3 are two independent permutations, and so are G_3 and $\overline{G}_1$, then $| \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} |$ would be less than $\frac{1}{n^{c_2}}$, since

$$|| \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} | \leq \\ | \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | + \\ | \text{Prob}\{DC_{2n}[G_3, \overline{G}_1] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | < \frac{1}{n^{c_2}}$$

Hence

$$\begin{aligned} & | \text{Prob}\{DC_{2n}[G_1, \bar{G}_1] = 1\} - \text{Prob}\{DC_{2n}[P_n, P_n] = 1\} | + \\ & | \text{Prob}\{DC_{2n}[G_3, \bar{G}_1] = 1\} - \text{Prob}\{DC_{2n}[G_1, \bar{G}_1] = 1\} | < \frac{1}{n^2} \end{aligned}$$

So, each of the above absolute values would be less than $\frac{1}{n^2}$. In other words

$$| \text{Prob}\{DC_{2n}[G_1, \bar{G}_1] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | < \frac{1}{n^2}$$

Hence G_1 and $\bar{G}_1$ are independent of each other, and G_1 is a super pseudorandom permutation. $\square$

The above lemmas and theorem show that when the number of oracle gates m is a polynomial of n then the probability of making a circuit which distinguishes $G_2 = \psi(f_2, 1, f_1, f_2, 1)$ from $G_3 = \psi(f_1, 1, f_2, f_1, 1)$ is less than 1 over any polynomial in n , and the probability of making a super distinguishing circuit for $G_1 = \psi(f_2, 1, f_1) \circ \psi(f_2, 1, f_1)$ is also less than 1 over any polynomial in n . In other words, G_1 is secure against chosen plaintext / ciphertext attack if the cryptanalyst is permitted to access to only a polynomial number of queries.

4.2 Super Pseudorandomness of $\psi(f^2, 1, f, f^2, 1, f)$

In the above relations, an upper bound on the probabilities has been defined, where f_1 and f_2 are two independently chosen pseudorandom functions. In the following lemmas and theorem, we show that if f_2 is substituted with f_1^2 , there would be an increase of the upper bound of the above probabilities of distinguishing. Nevertheless, if the number of oracles would be limited to some polynomial in n , the corresponding probabilities of distinguishing would remain less than 1 over any polynomial in n .

Lemma 5 *Let $f, h \in_r H_n$ and C_{2n} be a distinguishing circuit with $m < 2^n$ oracle gates, then*

$$| \text{Prob}\{C_{2n}[\psi(f^2, 1, f, f^2, 1)] = 1\} - \text{Prob}\{C_{2n}[\psi(h, 1, f, h, 1)] = 1\} | \leq \frac{2m^2}{2^n}$$

Proof : Since both f and h can be considered as two sequences of 2^n independent and uniformly distributed n -bit random variables, for an argument $a \in \Sigma^n$, $f(a)$ and $h(a)$ are two independent n -bit strings. When the input to an oracle is $(L \parallel R)$ and the oracle is evaluated with $\psi(h, 1, f, h, 1)$, each branches of the outputs, i.e., S and T , is always a sum of two random variables generated by the functions f and h . That is

$$\begin{aligned} S &= L \oplus R \oplus f(L \oplus h(L \oplus R)) \oplus h(R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R))) \\ T &= R \oplus h(L \oplus R) \oplus f(L \oplus h(L \oplus R)) \end{aligned}$$

Figure 3: X , Y and Z random variables in G_2 and G_2

where all the random variables $Y_i = f(L_i \oplus h(L_i \oplus R_i))$ are independent from random variables

$$X_j = h(L_j \oplus R_j)$$

$$Z_j = h(R_j \oplus h(L_j \oplus R_j) \oplus f(L_j \oplus h(L_j \oplus R_j)))$$

When the input to an oracle is $(L \parallel R)$ and the oracle is evaluated with $\psi(f^2, 1, f, f^2, 1)$, each branch of the output, i.e., S and T , is always a sum of two random variables generated by the function f . That is

$$S = L \oplus R \oplus f(L \oplus f^2(L \oplus R)) \oplus f^2(R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R)))$$

$$T = R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R))$$

If $R = 0$

$$S = L \oplus f(L \oplus f^2(L)) \oplus f^2(f^2(L) \oplus f(L \oplus f^2(L)))$$

$$T = f^2(L) \oplus f(L \oplus f^2(L))$$

If $L = 0$

$$S = R \oplus f^3(R) \oplus f^2(R \oplus f^2(R) \oplus f^3(R))$$

$$T = R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R))$$

If $L = 0$ and $R = 0$

$$S = f^3(0) \oplus f^2(f^2(0) \oplus f^3(0))$$

$$T = f^2(0) \oplus f^3(0)$$

When all the oracle gates are evaluated with $\psi(f^2, 1, f, f^2, 1)$ or all the oracle gates are evaluated with $\psi(h, 1, f, h, 1)$, a distinguisher generates "1" on its output with the same probability if all the random variables $Y_i = f(L_i \oplus f^2(L_i \oplus R_i))$ are independent from random variables

$$\begin{aligned} X_j &= f^2(L_j \oplus R_j) \\ Z_j &= f^2(R_j \oplus f^2(L_j \oplus R_j)) \oplus f(L_j \oplus f^2(L_j \oplus R_j)) \end{aligned}$$

In other words, a distinguisher with m oracle gates generates "1" on its output when there is one oracle gate O_i such that β_i the input value to the random function f is equal to either of

$$\beta_i = \begin{cases} f(L_j \oplus R_j) \\ f(R_j \oplus f^2(L_j \oplus R_j)) \oplus f(L_j \oplus f^2(L_j \oplus R_j)) \end{cases}$$

for some $j = 1, \dots, m$. The probability that in a given oracle the input to the f function takes a value equal to any of $2m$ internal random values in m oracle gates with different inputs is $\frac{2m}{2^n}$. The probability that a circuit distinguishes $\psi(f^2, 1, f, f^2, 1)$ from $\psi(h, 1, f, h, 1)$ is equal to the probability that two of the oracles generate dependant random variables. Hence

$$|\text{Prob}\{C_{2n}[\psi(f^2, 1, f, f^2, 1)] = 1\} - \text{Prob}\{C_{2n}[\psi(h, 1, f, h, 1)] = 1\}| \leq \frac{2m^2}{2^n}$$

The probability of distinguishing $\psi(h, 1, f, h, 1)$ from a random permutation was given in Lemma 2, as a result an upper bound on the overall probability of distinguishing $G_2 = \psi(f^2, 1, f, f^2, 1)$ from a random permutation is

$$|\text{Prob}\{C_{2n}[G_2] = 1\} - \text{Prob}\{C_{2n}[P_{2n}] = 1\}| \leq \frac{3m^2}{2^n} + \frac{m^2}{2^{2n}}$$

where $m < 2^n$ is the number of oracle gates. Hence, when the distinguisher is bounded by a polynomial number of oracle gates the probability of distinguishing $\psi(f^2, 1, f, f^2, 1)$ from a random permutation is less than 1 over any polynomial in n . $\square$

Lemma 6 Let $f, h \in_r H_n$ and C_{2n} be a distinguishing circuit with $m < 2^n$ oracle gates, then

$$|\text{Prob}\{C_{2n}[\psi(f, 1, f^2, f, 1)] = 1\} - \text{Prob}\{C_{2n}[\psi(f, 1, h, f, 1)] = 1\}| \leq \frac{2m^2}{2^n}$$

Proof : A proof similar to the proof of Lemma 5 can be given here. When the input to an oracle is $(L \parallel R)$ and the oracle is evaluated with $\psi(f, 1, f^2, f, 1)$, each branch of the output, i.e., S and T , is always a sum of two random variables generated by the function f . That is

$$\begin{aligned} S &= L \oplus R \oplus f^2(L \oplus f(L \oplus R)) \oplus f(R \oplus f(L \oplus R) \oplus f^2(L \oplus f(L \oplus R))) \\ T &= R \oplus f(L \oplus R) \oplus f^2(L \oplus f(L \oplus R)) \end{aligned}$$

If $R = 0$

$$\begin{aligned} S &= L \oplus f^2(L \oplus f(L)) \oplus f(f(L) \oplus f^2(L \oplus f(L))) \\ T &= f(L) \oplus f^2(L \oplus f(L)) \end{aligned}$$

If $L = 0$

$$\begin{aligned} S &= R \oplus f^3(R) \oplus f(R \oplus f(R) \oplus f^3(R)) \\ T &= R \oplus f(R) \oplus f^3(R) \end{aligned}$$

If $L = 0$ and $R = 0$

$$\begin{aligned} S &= f^3(0) \oplus f(f(0) \oplus f^3(0)) \\ T &= f(0) \oplus f^3(0) \end{aligned}$$

When all the oracle gates are evaluated with $\psi(f, 1, f^2, f, 1)$ or all the oracle gates are evaluated with $\psi(f, 1, h, f, 1)$, a distinguisher generates "1" on its output with the same probability if all the random variables $Y_i = f^2(L_i \oplus f(L_i \oplus R_i))$ are independent from random variables

$$\begin{aligned} X_j &= f(L_j \oplus R_j) \\ Z_j &= f(R_j \oplus f(L_j \oplus R_j) \oplus f^2(L_j \oplus f(L_j \oplus R_j))) \end{aligned}$$

In other words, a distinguisher with m oracle gates generates "1" on its output when there is one oracle gate O_i such that β_i , the input value to the random function f , is equal to $f(L_j \oplus f(L_j \oplus R_j))$ for some $j = 1, \dots, m$. As in each oracle, f have been used in two different layers, the probability that in a given oracle, β_i the input to the f functions takes a value equal to any of m internal random values Y_i , i.e., output of f^2 layer in m oracle gates with different inputs, is $\frac{2m}{2^n}$. The probability that a circuit distinguishes $\psi(f, 1, f^2, f, 1)$ from $\psi(f, 1, h, f, 1)$ is equal to the probability that two of the oracles generate dependant random variables. Hence

$$|\text{Prob}\{C_{2n}[\psi(f, 1, f^2, f, 1)] = 1\} - \text{Prob}\{C_{2n}[\psi(f, 1, h, f, 1)] = 1\}| \leq \frac{2m^2}{2^n}$$

The probability of distinguishing $\psi(f, 1, h, f, 1)$ from a random permutation was given in Lemma 3, as a result an upper bound on the overall probability of distinguishing $\mathcal{G}_3 = \psi(f, 1, f^2, f, 1)$ from a random permutation is

$$|\text{Prob}\{C_{2n}[\mathcal{G}_3] = 1 - \text{Prob}\{C_{2n}[P_{2n}] = 1\}| \leq \frac{3m^2}{2^n} + \frac{m^2}{2^{2n}}$$

where $m \leq 2^n$ is the number of oracle gates. Hence, when the distinguisher is bounded by a polynomial number of oracle gates the probability of distinguishing $\psi(f, 1, f^2, f, 1)$ from a random permutation is less than 1 over any polynomial in n . $\square$

Theorem 3 Let $f \in F_n$ be a pseudorandom function, then $\mathcal{G}_1 = \psi(f^2, 1, f, f^2, 1, f)$ is a super pseudorandom permutation.

Proof Sketch: To prove that $\mathcal{G}_1$ is a super pseudorandom permutation generator, we first show that $\mathcal{G}_2 = \psi(f^2, 1, f, f^2, 1)$ and $\mathcal{G}_3 = (f, 1, f^2, f, 1)$ are independent of each other. As it was shown in Lemma 5 and Lemma 6, in a D -distinguishing circuit when the input to an oracle is $(L \parallel R)$ and the oracle is evaluated with $\psi(f^2, 1, f, f^2, 1)$, the output is

$$\begin{aligned} S &= L \oplus R \oplus f(L \oplus f^2(L \oplus R)) \oplus f^2(R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R))) \\ T &= R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R)) \end{aligned}$$

and when the oracle is evaluated with $\psi(f, 1, f^2, f, 1)$, the output is

$$\begin{aligned} S' &= L \oplus R \oplus f^2(L \oplus f(L \oplus R)) \oplus f(R \oplus f(L \oplus R) \oplus f^2(L \oplus f(L \oplus R))) \\ T' &= R \oplus f(L \oplus R) \oplus f^2(L \oplus f(L \oplus R)) \end{aligned}$$

The six random variables involved are:

$$\begin{aligned} X_2 &= f^2(L \oplus R) \\ Y_2 &= f(L \oplus f^2(L \oplus R)) \\ Z_2 &= f^2(R \oplus f^2(L \oplus R) \oplus f(L \oplus f^2(L \oplus R))) \end{aligned}$$

and

$$\begin{aligned} X_3 &= f(L \oplus R) \\ Y_3 &= f^2(L \oplus f(L \oplus R)) \\ Z_3 &= f(R \oplus f(L \oplus R) \oplus f^2(L \oplus f(L \oplus R))) \end{aligned}$$

S, T, S' and T' are always a sum of two random variables generated by the function f . If a random variable in a output branch of an oracle becomes dependent on a random variable in any output branch of another oracle, the other random variables are always independent of each other. For example, if X_2 be equal to X_3 , the probability that Y_2 be equal to Y_3 is $\frac{1}{2^n}$. Likewise, if $Y_2 = Y_3$, the probability that $Z_2 = Z_3$ is $\frac{1}{2^n}$. Hence, the probability of dependency of two branches is equal to $\frac{1}{2^n}$, which is equal to the dependency of two output branches in two different oracle gates when instead of f^2 an independent random function such as h was applied. Here, we calculate an upper bound on the independency probability. As it was shown earlier in Lemma 5 that $\psi(f^2, 1, f, f^2, 1)$ and $\psi(h, 1, f, h, 1)$ are indistinguishable from each other, and it was shown in Theorem 2 that $\psi(h, 1, f, h, 1)$ and $\psi(f, 1, h, f, 1)$ are independent of each other, and it was shown in Lemma 6 that $\psi(f, 1, h, f, 1)$ and $\psi(f, 1, f^2, f, 1)$ are indistinguishable from each other. The probability that there would be a D -distinguishing circuit for $\mathcal{G}_2$ and $\mathcal{G}_3$ can be written as:

$$|\text{Prob}\{DC_{2n}[\mathcal{G}_2, \mathcal{G}_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\}| < \frac{1}{n^{c_2}}$$

The above probability statement can be expanded as,

$$\begin{aligned} & | \text{Prob}\{DC_{2n}[\mathcal{G}_2, \mathcal{G}_3] = 1\} - \text{Prob}\{DC_{2n}[\mathcal{G}_2, G_3] = 1\} \\ & + \text{Prob}\{DC_{2n}[\mathcal{G}_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} \\ & + \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | \end{aligned}$$

where $G_2 = \psi(h, 1, f, h, 1)$ and $G_3 = \psi(f, 1, h, f, 1)$. With reordering and separation of absolute values, we get:

$$\begin{aligned} & | | \text{Prob}\{DC_{2n}[\mathcal{G}_2, \mathcal{G}_3] = 1\} - \text{Prob}\{DC_{2n}[\mathcal{G}_2, G_3] = 1\} | \\ & + | \text{Prob}\{DC_{2n}[\mathcal{G}_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} | \\ & + | \text{Prob}\{DC_{2n}[G_2, G_3] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} || \end{aligned}$$

If the sum of the above probabilities is less than 1 over any polynomial in n , then $\mathcal{G}_2$ and $\mathcal{G}_3$ would essentially be independent of each other according to the definition. When $f, h \in H_n$, with applying procedures similar to the proofs of Lemma 5, Lemma 6 and Lemma 3, it can be shown that the first term is less than $\frac{2m^2}{2^n}$, and the second term is less than $\frac{2m^2}{2^n}$, and the third term is less than $\frac{m^2}{2^n} + \frac{m^2}{2^{2n}}$, respectively. So, the sum of these three probabilities, makes a bound on the probability for making a D -distinguishing circuit with m oracle gates for $\mathcal{G}_2$ and $\mathcal{G}_3$, which is $\frac{5m^2}{2^n} + \frac{m^2}{2^{2n}}$. When there are a polynomial number of oracle gates, i.e., m is a polynomial in n , then

$$| \text{Prob}\{DC_{2n}[\mathcal{G}_3, \mathcal{G}_2] = 1\} - \text{Prob}\{DC_{2n}[P_{2n}, P_{2n}] = 1\} | < \frac{1}{n^c}$$

With applying a proof similar to the proof of Theorem 2, it can be shown that when $\mathcal{G}_2$ and $\mathcal{G}_3$ are independent, $\mathcal{G}_1$ is super pseudorandom. $\square$

5 Conclusions and Open Problems

We have shown that it is possible to construct a super pseudorandom permutation generators applying a single pseudorandom function. We took advantage of the structure of optimal perfect randomizer, presented in [3]. We first showed that $\psi(h, 1, f, h, 1, f)$ is a super pseudorandom permutation. Then, we showed that by substituting f^2 instead of h , the probability of making a distinguisher still would remain less than 1 over any polynomial in n . Although, such a block cryptosystem is less than practical, it can be seen as an attempt towards a construction of practical ones which are provably secure against chosen plaintext / ciphertext attack without relying on any unproven hypothesis. If a cryptosystem is super pseudorandom it can be applied as a hashing algorithm, where it is assured that a cryptanalyst cannot find a collision without trying at least 2^n different messages. Two open problems can be posed from the result of this paper. The structure applies 6

rounds of DES-like permutations. The first open problem is whether the proposed structure is an optimal structure, and whether any other structure can be suggested which needs less number of rounds. It can be seen that $\psi(f, f^2, f, f, f)$ is a good candidate, but we have not got a justification for this claim yet. The second open problem is whether the proposed structure can be adopted to improve the quality of existing cryptosystems such as DES or LOKI against differential cryptanalysis without a need for redesigning their S boxes.

ACKNOWLEDGMENT

We would like to thank Professor Jennifer Seberry and Mr. Andy Quaine for their attention and support.

References

- [1] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.
- [2] Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.
- [3] J. Pieprzyk and B. Sadeghiyan. Optimal perfect randomizers. In *Abstracts of ASIACRYPT '91*, pages 130–135, 1991.
- [4] Josef Pieprzyk. How to Construct Pseudorandom Permutations from Single Pseudorandom Functions. In *Advances in Cryptology - EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 140–150. Springer-Verlag, 1991.
- [5] B. Sadeghiyan and J. Pieprzyk. On necessary and sufficient conditions for the construction of super pseudorandom permutations. In *Abstracts of ASIACRYPT '91*, pages 117–123, 1991.
- [6] A. C. Yao. Theory and applications of trapdoor functions. In *the 23rd IEEE Symposium on the Foundations of Computer Science*, pages 80–91, 1982.