Tatra Mt. Math. Publ. **20** (2000), 119–126

TATRA MOUNTAINS
Mathematical Publications

A REMARK TO LUBY–RACKOFF AND UELI M. MAURER PSEUDORANDOM GENERATORS

Otokar Grošek — Karol Nemoga — Ladislav Satko

ABSTRACT. There are two excellent papers among many others: while Luby and Rackoff's paper [M. Luby, C. Rackoff: *How to construct pseudorandom permutations from pseudorandom functions* SIAM J. Comput. **17** (1988), 373–386] treats pseudorandom permutation generators focusing on complexity theory, Maurer's paper [U. M. Maurer: *A simplified and generalized treatment of Luby–Rackoff*, Pseudorandom Permutation Generators, Lecture Notes in Comput. Sci., Vol. 658, Springer-Verlag, Berlin, 1993, pp. 239–255] is based on the relation between probability and complexity theory. One of the Maurer's result is that the famous Luby–Rackoff lemma can be assumed as a purely probabilistic result. In this paper we compare and generalize both approaches. We show that for arbitrary n, and given a general oracle circuit C_{2n} it is not possible to find Boolean function $g\colon (\{0,1\}^{2n})^k \to \{0,1\}$ and $x = (x_1,\dots,x_k)$, $x_i \in \{0,1\}^{2n}$ such that for all Boolean functions $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ the relation $C_{2n}(f) = g(f(x_1),\dots,f(x_k))$ is valid.

1. Preliminaries

Our terminology is similar to that of [2]. Let $\{0,1\}^n$ denote the set of binary strings of length n, let F^n denote the set of all 2^{n2^n} functions $\{0,1\}^n \to \{0,1\}^n$, and let P^n denote the subset of functions of F^n that are permutations of $\{0,1\}^n$, i.e., invertible or one-to-one. For $f_1, f_2 \in F^n$, $f_1 \circ f_2$ denotes the composition of f_1 and f_2, i.e., $(f_1 \circ f_2)(x) = f_2\bigl(f_1(x)\bigr)$. For two binary strings a and b, $a \bullet b$ denotes their concatenation, and when a and b have the same length, $a \oplus b$ denotes their bit-by-bit XOR.

Let L and R denote the left and right half of a $2n$-bit string $L \bullet R$, respectively and let for $f \in F^n$ the permutation $\overline{f} \in P^{2n}$ be defined as

$$\overline{f}(L \bullet R) = R \bullet \bigl[L \oplus f(R)\bigr]\,.$$

2000 Mathematics Subject Classification: 94A60, 11K45, 68P25.
Keywords: pseudorandom function, pseudorandom permutation, Luby–Rackoff permutation generator.

Supported by Grant VEGA 1/4289/97, 1/5123/99.

This corresponds to one round of DES. For a list of functions, $f_1,\dots,f_s \in F^n$, let the function (actually a permutation) $\psi(f_1,\dots,f_s)\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ be defined by

$$\psi(f_1,\dots,f_s) = \overline{f}_1 \circ \cdots \circ \overline{f}_s\,.$$

An oracle circuit C_{2n} is a circuit with oracle gates, i.e., gates with a $2n$-bit input and $2n$-bit output, where all oracle gates in a circuit evaluate the same fixed function from F^{2n} (for details see [2]).

Main Lemma of [2]. Let C_{2n} be an oracle circuit with k oracle gates such that no input value is repeated to an oracle gate. Then

$$\Big|\mathrm{Prob}\big[C_{2n}(f)=1\colon f \in_R \psi(F^n,F^n,F^n)\big] - \mathrm{Prob}\big[C_{2n}(f)=1\colon f \in_R F^{2n}\big]\Big| \le k^2/2^n\,,$$

where $\in_R$ denotes the uniform probability distribution on a set.

Let $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$ be a function taking as input k $2n$-bit strings. Then define

$$P_g = \mathrm{Prob}\big[g(r_1,\dots,r_k)=1\big]\,,$$

where $r_1,\dots,r_k$ are independent and randomly selected from $\{0,1\}^{2n}$.

Main Lemma of [1]. For every function $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$ and for every set of k arguments $x_1,\dots,x_k \in \{0,1\}^{2n}$

$$\Big|\mathrm{Prob}\big[g\big(f(x_1),\dots,f(x_k)\big)=1\colon f \in_R \psi(F^n,F^n,F^n)\big] - P_g\Big| \le k^2/2^n\,.$$

In his article [1] Maurer concludes that these lemmas are equivalent.

2. Counterexamples

In fact, to prove that two above mentioned approaches are equivalent it is possible to use the transferring lemma:

Lemma 1. *For every function $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$ and for every set of k arguments $x_1,\dots,x_k \in \{0,1\}^{2n}$ there exists an oracle circuit C_{2n} with k oracle gates such that*

$$C_{2n}(f) = g\big(f(x_1),\dots,f(x_k)\big)\,,$$

for all $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$.

Conversely, to any oracle circuit C_{2n} there exist a Boolean function $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$, and a k-tuple $(x_1,\dots,x_k) \in \big(\{0,1\}^{2n}\big)^k$ such that

$$C_{2n}(f) = g\big(f(x_1),\dots,f(x_k)\big)$$

is valid for all Boolean functions $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$.

As it was mentioned in [1], it is easy to prove that Maurer's lemma is an immediate consequence of the Luby–Rackoff's lemma. In fact, it is easy to prove the first part of Lema 1. Unfortunately, the second part of Lemma 1 is not true in general. To clarify the situation we give an equivalent formulation of this part of Lemma 1. At first we define some new sets.

Having oracle circuit C_{2n}, we separate by C_{2n} the set of all Boolean functions F^{2n} into two subsets corresponding to the image $\{0\}$ and $\{1\}$, respectively, as follows:

$$A_0 = \bigl\{f\colon f \in F^{2n},\ C_{2n}(f) = 0\bigr\},$$

and

$$A_1 = \bigl\{f\colon f \in F^{2n},\ C_{2n}(f) = 1\bigr\}.$$

For $x \in \bigl(\{0,1\}^{2n}\bigr)^k$, $x = (x_1, \dots, x_k)$, $x_i \in \{0,1\}^{2n}$ let

$$A_0^x = \bigl\{\bigl(f(x_1), \dots, f(x_k)\bigr)\colon f \in A_0\bigr\},$$

and

$$A_1^x = \bigl\{\bigl(f(x_1), \dots, f(x_k)\bigr)\colon f \in A_1\bigr\}.$$

THEOREM 1. *Let C_{2n} be an oracle circuit with k gates. Then the following two assertions are equivalent:*

(1) *There exist a function $g\colon \bigl(\{0,1\}^{2n}\bigr)^k \to \{0,1\}$ and a k-tuple $x = (x_1, \dots, x_k)$, $x_i \in \{0,1\}^{2n}$, such that for all Boolean functions $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$*

$$C_{2n}(f) = g\bigl(f(x_1), \dots, f(x_k)\bigr).$$

(2) *There exists a k-tuple x, $x \in \bigl(\{0,1\}^{2n}\bigr)^k$, such that*

$$A_0^x \cap A_1^x = \emptyset.$$

P r o o f. a) Let there exist g and x such that (1) holds and let $y \in A_0^x \cap A_1^x$. Then

$$\begin{aligned} y &= \bigl(f(x_1), \dots, f(x_k)\bigr) \quad \text{for some} \quad f \in A_0, \\ &= \bigl(h(x_1), \dots, h(x_k)\bigr) \quad \text{for some} \quad h \in A_1. \end{aligned}$$

It means that

$$\begin{aligned} &C_{2n}\bigl(f(x_1), \dots, f(x_k)\bigr) = g(y) = g\bigl(f(x_1), \dots, f(x_k)\bigr) = 1, \quad \text{and} \\ &C_{2n}\bigl(h(x_1), \dots, h(x_k)\bigr) = g(y) = g\bigl(h(x_1), \dots, h(x_k)\bigr) = 0, \end{aligned}$$

a contradiction.

b) Let there exists $\overline{x} = (\overline{x}_1, \dots, \overline{x}_k)$ such that $A_0^{\overline{x}} \cap A_1^{\overline{x}} = \emptyset$. Then we define a function $g\colon \left(\{0,1\}^{2n}\right)^k \to \{0,1\}$ such that

$$g(x) = \begin{cases} 0\,, & x \in A_0^{\overline{x}}\,,\\ 1\,, & x \in A_1^{\overline{x}}\,,\\ 0\,, & \text{otherwise}\,. \end{cases} \tag{1}$$

Hence, if $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$, $f \in A_1$, for our oracle circuit with k gates we have

$$C_{2n}(f) = 1 = g\big(f(\overline{x}_1), \dots, f(\overline{x}_k)\big)\,.$$

Similarly if $f \in A_0$, then

$$C_{2n}(f) = 0 = g\big(f(\overline{x}_1), \dots, f(\overline{x}_k)\big)\,.$$

□

In fact the first assertion of the Theorem 1 is the second part of Lemma 1. The second assertion is an equivalent statement which enables construction of counterexamples.

In the following two examples we show that given an oracle circuit C_{2n} it is not possible to find a Boolean function $g\colon \left(\{0,1\}^{2n}\right)^k \to \{0,1\}$ and a k-tuple $x = (x_1, \dots, x_k)$, $x_i \in \{0,1\}^{2n}$ such that for all Boolean functions $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$

$$C_{2n}(f) = g\big(f(x_1), \dots, f(x_k)\big)\,.$$

EXAMPLE 1. Let $n = 1$ and $k = 2$. Consider the oracle circuit C_2 according to Figure 1.

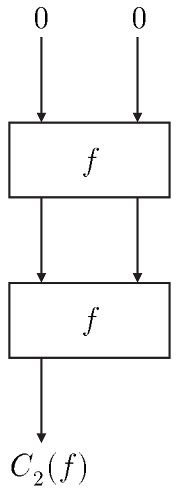

FIGURE 1. Oracle circuit C_2.

For the Boolean function $f\colon \{0,1\}^2 \longrightarrow \{0,1\}^2$, $f=(f_1,f_2)$ the circuit C_2 gives the value

$$C_2(f) = f_1\big(f_1(0,0), f_2(0,0)\big)\,.$$

It is easy to divide all Boolean functions $f\colon \{0,1\}^2 \longrightarrow \{0,1\}^2$ in two sets A_0, A_1 (see Table 1, 2), where $\bullet$ stands for arbitrary value 0 or 1. A_1 is the complement of A_0 in F^2.

TABLE 1. Set A_0.

x_1x_2	f_1f_2	f_1f_2	f_1f_2	f_1f_2
0 0	0 0	0 1	1 0	1 1
0 1	$\bullet\,\bullet$	0 $\bullet$	$\bullet\,\bullet$	$\bullet\,\bullet$
1 0	$\bullet\,\bullet$	$\bullet\,\bullet$	0 $\bullet$	$\bullet\,\bullet$
1 1	$\bullet\,\bullet$	$\bullet\,\bullet$	$\bullet\,\bullet$	0 $\bullet$

TABLE 2. Set A_1.

x_1x_2	f_1f_2	f_1f_2	f_1f_2
0 0	0 1	1 0	1 1
0 1	1 $\bullet$	$\bullet\,\bullet$	$\bullet\,\bullet$
1 0	$\bullet\,\bullet$	1 $\bullet$	$\bullet\,\bullet$
1 1	$\bullet\,\bullet$	$\bullet\,\bullet$	1 $\bullet$

By an exhaustive search it is easy to see that $A_0^x \cap A_1^x \neq \emptyset$ for all $x \in \{0,1\}^4$. For example, if $x=(0,0,0,1)$, then

$$\begin{aligned} A_1^x &= \big\{(0,1,1,\bullet),\ (1,0,\bullet,\bullet),\ (1,1,\bullet,\bullet)\big\}\,,\\ A_0^x &= \big\{(0,0,\bullet,\bullet),\ (0,1,0,\bullet),\ (1,0,\bullet,\bullet),(1,1,\bullet,\bullet)\big\}\,,\\ A_0^x \cap A_1^x &= \big\{(1,0,\bullet,\bullet),\ (1,1,\bullet,\bullet)\big\}\,. \end{aligned}$$

where, e.g., $(0,1,1,\bullet)$ stands for all f such that $f(0,0)=(0,1)$, and $f(0,0)=(1,\bullet)$.

Hence, due to Theorem 1 there does not exist a function g, and x, $x=(x_1,x_2)$, such that $C_2(f) = g\big(f(x_1), f(x_2)\big)$ for all f.

In the next Example we extend this approach to a general case.

EXAMPLE 2. Let us consider the oracle circuit C_{2n} according to Figure 2.

Then for $f=(h_1,\dots,h_{2n})$, $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ we have

$$C_{2n}(f) = h_1\big(h_1(0,\dots,0),\dots,h_{2n}(0,\dots,0)\big)\,.$$

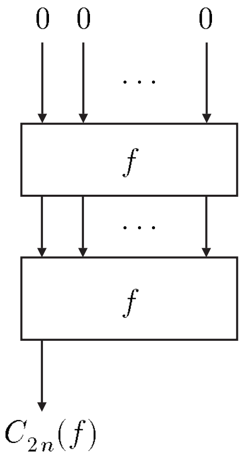

FIGURE 2. Oracle cirenit C_{2n}.

Similarly as in Example 1 we define sets A_0, A_1 (see Table 3, 4). Let $x \in \{0,1\}^{2n}$, $x \neq (0,\dots,0)$.

TABLE 3. Set A_0.

$x_1 \dots x_{2n}$	$h_1 \dots h_{2n}$	$h_1 h_2 \dots h_{2n}$	$h_1 h_2 \dots h_{2n}$
$0 \dots 0$	$0 \dots 0$	x	$\dots$
$0 \dots 1$	$\bullet \dots \bullet$	$\bullet\bullet \dots \bullet$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
x	$\bullet \dots \bullet$	$0 \bullet \dots \bullet$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

TABLE 4. Set A_1.

$x_1 \dots x_{2n}$	$h_1 h_2 \dots h_{2n}$	$h_1 h_2 \dots h_{2n}$
$0 \dots 0$	x	$\dots$
$\vdots$	$\vdots$	$\vdots$
x	$1 \bullet \dots \bullet$	$\dots$
$\vdots$	$\vdots$	$\vdots$

Functions corresponding to the column with x in the first row of the set A_0 we denote by H_x. Thus

$$H_x = \{f \in A_0 : f(0,\dots,0) = x\}.$$

Similarly

$$H'_x = \{f \in A_1 : f(0,\dots,0) = x\}.$$

Next we show that for any g and x, $C_{2n}(f) \neq g\big(f(x_1),\dots,f(x_k)\big)$. Due to Theorem 1 it is sufficient to prove that for all $y \in \big(\{0,1\}^{2n}\big)^k$, $y = (y_1,\dots,y_k)$, $y_i \in \{0,1\}^{2n}$ we have $A_0^y \cap A_1^y \neq \emptyset$.

Let $x \in \{0,1\}^{2n}$, and $x \neq y_i$ for all $i = 1,\dots,k$. Such x does exist because of $k < 2^{2n}$. Then by definition of H_x and H'_x there exist functions $f \in H_x$, $f' \in H'_x$ such that

$$f(y_i) = x = f'(y_i).$$

Using the same notation for arguments as in Example 1 we have $(x,\dots,x) \in A_0^y \cap A_1^y$ and thus $A_0^y \cap A_1^y$ is nonempty.

It yields that for arbitrary n, and given a general oracle circuit C_{2n} it is not possible to find a Boolean function $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$ and a k-tuple $x = (x_1,\dots,x_k)$, $x_i \in \{0,1\}^{2n}$ such that for all Boolean functions $f\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$

$$C_{2n}(f) = g\big(f(x_1),\dots,f(x_k)\big).$$

Thus, by counterexample, the second part of Lemma 1 is false, and it is not possible to prove the Luby–Rackoff Lemma from Maurer's Lemma using transferring Lemma 1.

3. A generalization of distinguishability

Our discussion from Section 1 leads to the following generalization. We define undistinguishability according to Luby and Rackoff by oracle circuits, and undistinguishability according to Maurer by Boolean functions, for two general classes of functions from F^{2n}.

Definition 1. Let T_1, T_2 be two classes of Boolean functions, $T_1, T_2 \subseteq F^{2n}$. Then T_1, T_2 are said to be *LR-undistinguishable*, $\mathrm{UD}_2(T_1,T_2)_{n,k}$, if for all oracle circuits C_{2n} with no repeated input values and k oracle gates there holds

$$\Big|\mathrm{Prob}\big[C_{2n}(f) = 1\colon f \in_R T_1\big] - \mathrm{Prob}\big[C_{2n}(f) = 1\colon f \in_R T_2\big]\Big| \leq \frac{k^2}{2^n}.$$

Definition 2. Let T_1, T_2 be two classes of Boolean functions, $T_1, T_2 \subseteq F^{2n}$. Then T_1, T_2 are said to be *M-undistinguishable*, $\mathrm{UD}_M(T_1,T_2)_{n,k}$, if for all Boolean functions $g\colon \big(\{0,1\}^{2n}\big)^k \to \{0,1\}$, and every set of k arguments $x_1,\dots,x_k$ with no repeated values we have

$$\left|\operatorname{Prob}\left[g\left(f(x_1),\dots,f(x_k)\right)=1\colon f\in_R T_1\right]-\operatorname{Prob}\left[g\left(f(x_1),\dots,f(x_k)\right)=1\colon f\in_R T_2\right]\right| \le \frac{k^2}{2^n}\,.$$

As an immediate consequence of the first part of Lemma 1 we have:

THEOREM 2. *If two classes $T_1, T_2 \subseteq \{0,1\}^{2n}$ are LR-undistinguishable then T_1 and T_2 are M-undistinguishable, i.e.,*

$$\mathrm{UD}_{LR}(T_1,T_2)_{n,k} \Longrightarrow \mathrm{UD}_M(T_1,T_2)_{n,k}\,.$$

The counterexamples given above do not prove that M-undistinguishability does not imply LR-undistinguishability. Nevertheless we think that the next conjecture is valid:

CONJECTURE 1. *There exist two classes T_1, T_2 of functions from F^{2n} such that*

$$\mathrm{UD}_M(T_1,T_2)_{n,k} \not\Longrightarrow \mathrm{UD}_{LR}(T_1,T_2)_{n,k}\,.$$

REFERENCES

[1] MAURER, U. M.: *A simplified and generalized treatment of Luby–Rackoff Pseudorandom Permutation Generators*, in: Lecture Notes in Comput. Sci., Vol. 658, Springer-Verlag, Berlin, 1993, pp. 239–255.

[2] LUBY, M.—RACKOFF, C.: *How to construct pseudorandom permutations from pseudorandom functions*, SIAM J. Comput. **17** (1988), 373–386.

Received February 25, 2000

Otokar Grošek, Ladislav Satko
Department of Mathematics
Faculty of Electrical Engineering
and Computer Science
Slovak University of Technology
Ilkovičova 3
SK–812 19 Bratislava
SLOVAKIA

E-mail: grosek@kmat.elf.stuba.sk
satko@kmat.elf.stuba.sk

Karol Nemoga
Mathematical Institute
Slovak Academy of Sciences
Štafánikova 49
SK–814 73 Bratislava
SLOVAKIA

E-mail: nemoga@mat.savba.sk