Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 13/1999

Otakar Grošek
Karol Nemoga
Ladislav Satko

A remark to Luby-Rackoff and Ueli M. Maurer pseudorandom generators

August 13, 1999

PREPRINT SERIES

A Remark to Luby–Rackoff and Ueli M. Maurer Pseudorandom Generators

Otokar Grošek [*]
Department of Mathematics
Slovak University of Technology
812 19 Bratislava, Slovakia
e-mail: grosek@elf.stuba.sk

and

Karol Nemoga [†]
Institute of Mathematics
Slovak Academy of Sciences
814 73 Bratislava, Slovakia
e-mail: nemoga@savba.sk

and

Ladislav Satko [‡]
Department of Mathematics
Slovak University of Technology
812 19 Bratislava, Slovakia
e-mail: satko@kmat.elf.stuba.sk

[*]This work was supported by VEGA grant 1/4289/97
[†]This work was supported by VEGA grant 1/5123/99
[‡]This work was supported by VEGA grant 1/4289/97

Abstract

There are two excellent papers among many others: while Luby and Rackoff's paper [?] treats pseudorandom permutation generators focusing on complexity theory, Maurer's paper [?] 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 $g : (\{0,1\}^{2n})^k \to \{0,1\}$ and $x = (x_1, \ldots, x_k), x_i \in \{0,1\}^{2n}$ such that for all Boolean functions $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ the relation $C_{2n}(f) = g(f(x_1), \ldots, f(x_k))$ is valid.

Key words: Pseudorandom function, Pseudorandom permutation, Luby–Rackoff permutation generator.

1. Preliminaries

Our terminology is similar to that of [?]. 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., $(f_1 \circ f_2)(x) = f_2(f_1(x))$. 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 $L \bullet R$ and let for $f \in F^n$ the permutation $\bar{f} \in P^{2n}$ be defined as

$$\bar{f}(L \bullet R) = R \bullet [L \oplus f(R)].$$

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

$$\psi(f_1, \ldots, f_s) = \bar{f}_1 \circ \ldots \circ \bar{f}_s.$$

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 in F^{2n} (for details see [?]).

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

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

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

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

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

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

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

$$\left|\mathrm{Prob}[g(f(x_1), \ldots, f(x_k)) = 1 : f \in_R \psi(F^n, F^n, F^n)] - P_g]\right| \leq k^2/2^n.$$

In his article [?] 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 a transferring lemma:

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

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

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

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

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

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

As it was mentioned in [?] 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:

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

and

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

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

$$A_0^x = \{(f(x_1), \ldots, f(x_k)) : f \in A_0\},$$

and

$$A_1^x = \{(f(x_1), \ldots, f(x_k)) : f \in A_1\}.$$

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

1. *There exist function $g : (\{0,1\}^{2n})^k \to \{0,1\}$ and $x = (x_1, \ldots, x_k), x_i \in \{0,1\}^{2n}$ such that for all Boolean functions $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$*

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

2. *There exists x, $x \in (\{0,1\}^{2n})^k$ such that*

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

Proof.
a) Let there exist g and x such that 1. holds and let $y \in A_0^x \cap A_1^x$. Then

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

It means that

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

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

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

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

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

Similarly if $f \in A_0$, then

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

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
`http://www.mat.savba.sk/preprints`

Latest preprints of the series:

13/1999 *Otakar Grošek, Karol Nemoga, Ladislav Satko*: A remark to Luby-Rackoff and Ueli M. Maurer pseudorandom generators

12/1999 *Beloslav Riečan*: On the sum of observables in product MV algebras

11/1999 *Peter Eliaš*: A hierarchy of thin sets related to the boundedness of trigonometric series

10/1999 *Miloslav Duchoň, Peter Maličký*: On Herglotz theorem in partially ordered vector spaces

9/1999 *Ján Jakubík*: Torsion classes of specker lattice ordered groups

8/1999 *Ján Jakubík*: Graph automorphisms and cells of lattices

7/1999 *Miloslav Duchoň, Peter Maličký*: Positive linear maps on trigonometric polynomials

6/1999 *Miloslav Duchoň, Anna Kolesárová*: Fourier transforms of vector-valued measures on a certain compact semigroup

5/1999 *Miroslav Ploščica*: Separation properties in congruence lattices of lattices

4/1999 *Georges Chevalier, Anatolij Dvurečenskij, Karl Svozil*: Piron's and Bell's geometric lemmas and Gleason's theorem

3/1999 *Jarmila Hedlíková*: Relatively orthomodular lattices

2/1999 *Anatolij Dvurečenskij, Pekka Lahti, Kari Ylinen*: Some remarks on the moment problem

1/1999 *Anatolij Dvurečenskij*: Loomis-Sikorski theorem for σ-complete MV-algebras and ℓ-groups

27/1998 *Martin Kochol*: Cubic graphs without a Petersen minor have nowhere-zero 5-flows

26/1998 *Anatolij Dvurečenskij, Ferdinand Chovanec, Eva Rybáriková*: D-homomorphisms and atomic σ-complete Boolean D-posets

25/1998 *Anatolij Dvurečenskij*: Commutative BCK-algebras with product

24/1998 *Anatolij Dvurečenskij, Antonio Di Nola*: Product MV-algebras

23/1998 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Dedekind complete commutative BCK-algebras

22/1998 *Anatolij Dvurečenskij*: Ideals of commutative BCK-algebras

21/1998 *Anatolij Dvurečenskij, Beloslav Riečan*: Weakly divisible MV-algebras and product

20/1998 *Ivan Korec*: Definability of addition and multiplication from Pascal's triangle modulo n and number-theoretical functions

(continued on inside back cover)

19/1998 *Roberto Giuntini, Sylvia Pulmannová*: Ideals and congruences in effect algebras and QMV algebras

18/1998 *Ivan Korec*: Definability of exact arithmetical operations from approximate ones

17/1998 *Georges Chevalier, Sylvia Pulmannová*: Some ideal lattices in partial abelian monoids

16/1998 *Anatolij Dvurečenskij*: On categorical equivalences of commutative BCK-algebras

15/1998 *Ivan Korec*: Definability of addition and multiplication from some quadratic forms $ax^2 + cy^2$

14/1998 *Beloslav Riečan*: On the L^p space of observables on product MV algebras

13/1998 *Beloslav Riečan*: On the strong law of large numbers on some ordered structures

12/1998 *Ladislav Mišík, jr., Tibor Žáčik*: A simplified formula for calculation of metric dimension of converging sequences

11/1998 *Beloslav Riečan*: On the joint distribution of observables

10/1998 *Beloslav Riečan*: On the product MV algebras

9/1998 *Roman Frič*: A Stone-type duality and its applications to probability

8/1998 *Roman Frič*: Ring of maps: sequential convergence and completion

7/1998 *Roman Frič, Ján Jakubík*: Sequential convergences on Boolean algebras defined by systems of maximal filters

6/1998 *Roman Frič*: Categorical reflections on fields of events and probability

5/1998 *Beloslav Riečan*: On the probability theory and fuzzy sets

4/1998 *Ivan Korec*: Definability of arithmetical operations from binary quadratic forms

3/1998 *Beloslav Riečan*: On the conditional expectation of observables in MV algebras of fuzzy sets

2/1998 *Beloslav Riečan*: On the conditional probability on MV algebras

1/1998 *Paula B. Cohen, Robin L. Hudson, K. R. Parthasarathy, S. Pulmannová*: Hall's transformation via quantum stochastic calculus

13/1997 *Ivan Korec*: Real-time generation of primes by a one-dimensional cellular automaton with 9 states

12/1997 *Ivan Korec*: Arithmetical operations strongest with respect to the first order definability

11/1997 *Otokar Grošek, Karol Nemoga, Marcel Zanechal*: Why use bijective S-boxes in GOST-algorithm

10/1997 *Beloslav Riečan*: On the L^p space of observables

9/1997 *Ladislav Mišík Jr., Tibor Žáčik*: A formula for calculation of metric dimension of converging sequences

8/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Commutative *BCK*-algebras and lattice ordered groups

7/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: On representations of commutative BCK-algebras

6/1997 *Sylvia Pulmannová, Karl Svozil*: Ideals in ortholattices, Bell inequalities and simultaneously definite properties

5/1997 *Camille Debiève, Miloslav Duchoň, Beloslav Riečan*: Moment problem in some ordered vector spaces

4/1997 *Miloslav Duchoň, Beloslav Riečan*: On the Kurzweil–Stieltjes integral in ordered spaces

3/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Remarks on representations of minimal clans

2/1997 *Ivan Korec*: Elementary definability from Pascal's triangle modulo p and the set of e-th powers