ON THE POSSIBILITY OF DESIGN AND THE ALGORITHMIC
FOR THE FAST VLSI-RANDOMNESS SOURCES

C. Glowacz
DEPT. OF COMPUTER SCIENCE
UNIVERSITY OF BONN

M. Karpinski*
DEPT. OF COMPUTER SCIENCE
UNIVERSITY OF BONN

H.T. Vierhaus
GMD RESEARCH INSTITUTE
/E.I.S PROJECT
5205 ST. AUGUSTIN 1

SUMMARY

1. Design of Fast Randomized Algorithms.

The latest developments in the design of fast parallel algorithms lead to the fundamental
new insight into the growing importance of randomness (cf. [F 79], [KUW 85], [MVV 87],
[MS 82], [Fu 87]) as the computational resource. The randomization makes some algorithmic
solutions possible for problems for which no deterministic solutions are known or possible. The
randomization not only becomes widely applicable in combinatorial optimization algorithms
but also in algorithmic coding theory, computer algebra, number theory ([AH 87]), encryption
techniques, protocols, smart-card design, etc. All these applications assume the availability of
a source of randomness in form of the bit sequence random generators working as rapidly as
needed. These generators must not only be fast but also random (not pseudo-random, although
sometimes pseudo-randomness is enough, cf. [B 87]), i.e. capable of producing unbiased and
totally unpredictable bit sequences. The existence of such sources is an open question even
if one accepts the modern Physics postulate on the existence of 'truly random' elementary
processes. The model of imperfect but available physical sources of randomness, still good
enough for all algorithmic applications, was recently developed in a series of papers by
Vazirani and Santha [V 85], [SV 86], [V 87]. We base our development on models of slightly-random
([V 85]) and semi-random sources ([SV 86]).

*Supported in part by Leibniz Center for Research in Computer Science and the DFG Grant KA 673/2-1
We apply the phase-jitter of a free-running oscillator connected via an EXOR tree structure, and subsequently apply decoding techniques from the theory of BCH codes. The design is just being applied for the randomized combinatorial optimization chip (joint project of the University of Bonn and GMD-E.I.S.), which comprises the randomized MAXIMUM MATCHING subroutine. The details will be described in the full paper.

2. VLSI-Source of Randomness.

The conventional sources of pseudo-random numbers are not always suitable for algorithmic or cryptographic applications. In the number of applications the generation of "truly random" seeds of random numbers occurs to be necessary and the pseudo-random bit sequence generators ([BM82]) are not a proper substitution for it (cf. [RS85]). As proposed by [FMC85], the phase-jitter of a free-running oscillator can be used for random number generation. This basic approach was considerably modified using a relaxation-type oscillator at 100 MHz (see Figure 1). It can be shown that the exploitable phase jitter from such an oscillator exceeds that from a feedback-gate oscillator by far at comparable demands in silicon area (see Figure 2). Analog sources were also considered and showed inferior performance due to limitations of available technology with respect to power dissipation and gain-bandwidth product.

As shifts of MOS threshold voltages will cause an inescapable bias in the oscillator output, an equal probability of 0 and 1 values over a long time requires further processing. This can be done by connecting several independent sources via an EXOR tree structure. We used a more area economical approach devised by Vazirani [V87] instead and were able to prove its correctness for the first time. The main method we apply is on-chip implementation of BCH codes. Thus 127 independent oscillators were separately implemented on one chip using analog design techniques for optimum isolation and VDD/VSS decoupling.

The chip design (see Figure 3) finally yields 8 independent sources of truly random bits with negligible algorithmic bias. The pattern rate is controllable from the outside. True randomness is expected up to pattern rates of 100 KB per second, but the basic circuit design allows for an exploitation of rates up to 2 MB per second. By comparison, the AT&T LSI chip [FMC85] works with 4 B per second rates, which gives our design speed-up of order 25000. As an illustration in usual algorithmic applications, one needs a number of bits proportional to the square of the size of the input.

The chip was designed using 2.5 micron n-well CMOS technology (of Fraunhofer-Institut IMS, Duisburg, Germany) and contains about 9000 transistors using 18 smm of silicon area (see Figure 4). This includes an overhead for interfacing not necessary if the design's kernel is used in further applications where the random number generation and use of random bits take place on the same chip. Optimum testability for CMOS specific faults was implemented using novel scan-path elements with stuck-open testability (see Figure 5) (cf. also [Wi87], [GMKMV88]). The chip seems to be the first VLSI-design of this type for the fast, parallel, and 'provably good' on-chip random bit generation. It may find main applications in the design of fast random number generators for the randomized VLSI algorithms and potentially also in cryptography.
References


Figure 1: Relaxation Oscillator: Circuit-Diagram
Figure 3: Structure of the Chip
Figure 4: Layout of the Chip
Figure 5: Testable Scan-Path D-Latch