THE
PLab
RESEARCH
GROUP

Institut für Mathematik
Universität Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg

Stefan Wegenkittl

The pLAB Picturebook

Load Tests

For the SG100 Security Generator

Report 08, February 1998-04-01

PLab - REPORTS

The pLAB Picturebook:
Load Test
For the SG100 Security Generator

Stefan Wegenkittl
Dept. Of Mathematics
University of Salzburg, Austria[*]

February 1998

Abstract

This report gives the empirical results of the SG100 Security Generator in the Load Test.

Keywords: pseudorandom number generation, empirical tests, stochastic simulation

1 Introduction

The test setup for the Load Test is described in the Picturebook, Part I, [4]. This report is part of a growing collection of test results for various pseudorandom number generators (PRNGs).

2 The Generators

- "SG100-V2", version 2 of the hardware device SG100 of Protego Information AB, www.protego.se. See also notes in next section.
- "SG100-V3", version 3 of the hardware device SG100 of Protego Information AB, cryptographic shift-register based PRNG, seeded from SG100.
- "SG100-V4", version 4 of the hardware device SG100 of Protego Information AB: This one combines V2 and V3 modulo 2^{32}.

[*] e-mail: ste@random.mat.sbg.ac.at, www: http://random.mat.sbg.ac.at/team/, research supported by the Austrian Science Fund FWF, project no. P11143-MAT

3 Results

The following pages contain commented simulation results for all generators which have been introduced above. Each page contains the plot of the truncated Kolmogorov-Smirnov-values and the according uppertail-probabilities for the ‘Load Test’ (LT). The main characteristics of the LT as described in [4] are: LT is a two-level test combining an overlapping serial test at the first level which tests 4-bit words in dimensions 1 to 5 with a Kolmogorov-Smirnov test at the second level. The sample size at the first level is varied from 2^{18} to 2^{26}, the sample size at the second level is 32. The whole test uses utmost 2^{32} PRNs from the generator in order to generate a single KS-value.

3.1 Testing SG100

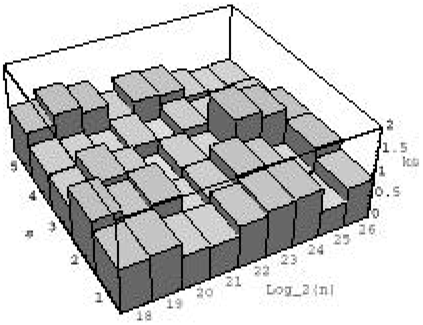
In order to test the hardware generator SG100, we have produced a large file containing noise produced by the device. This enables us to the same numbers for different dimensions in the LT. Let u_0, u_1, … denote the successive values in the noise file, $u_i \in \{0,\ldots,255\}$. 4-bit blocks as required by the LT have been constructed by cutting out firstly the upper nibble and secondly the lower nibble of each u_i. The LT thus tests every bit produced by the noise driver. This has to be taken into account if a comparison to the ordinary LT-setup in [4] is made.

Protego Information AB provided us with a set of drivers for Microsoft Windows 95 such that we had access to the raw noise of the device itself (call this Version 1), the processed noise with the cryptographic noise generator (Version2), the cryptographic noise generator itself (Version 3), and (Version 4) the driver that isusually provided with the SG100 package, see www.protego.se/hardware_prop_en.htm. Actually, Version 4 adds the output of Version 2 and Version 3 modulo 2^{32}. We used the abbreviations SG100-V1, SG100-V2, SG100-V3 and SG100-V4 for the different versions of SG100. SG100-V1 is not published here since statistical weakness of the unprocessed raw input is well-known and SG100 software prevents the user from access to this noise.

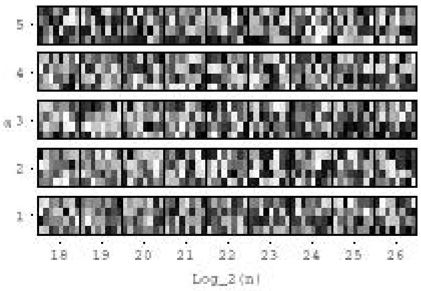
SG100-V2

SG100, cryptographic generator turned off

Load Test for SG100-V2



upper-tail probabilities

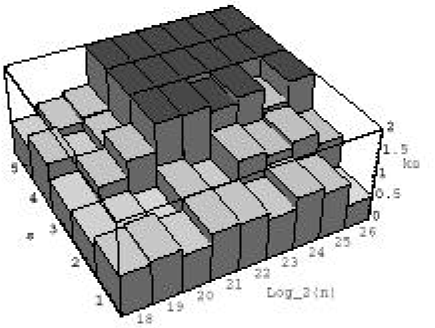


Periodlength: ∞, **Speed:** up to 9.500 bytes/sec.
Comments: No flaws detected, the SG100 passes the Load Test even when cryptographic generator is turned off.

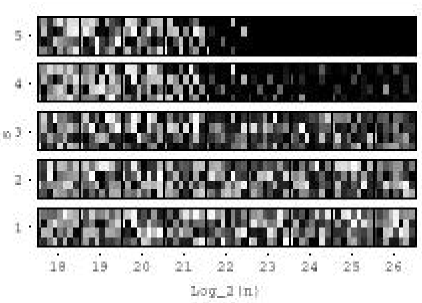
SG100-V3

SG100, cryptographic shift-register based PRNG,
seeded from SG100

Load Test for SG100-V3



upper-tail probabilities

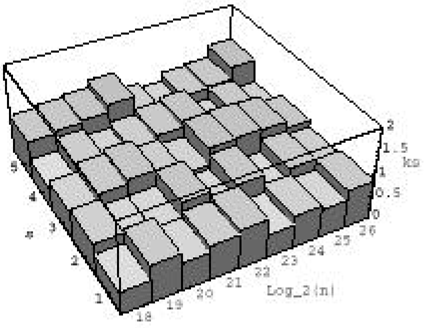


Periodlength: ∞, **Speed:** not measured.
Comments: The cryptographic generator of SG100 has about the same quality as the top-performing LCG with modulus 2^{32}. Note, that this comparison does not take into account that the LT for SG100 uses all eight bits from every pseudorandom number, whereas the usual LT cuts out the most significant 4 bits only.

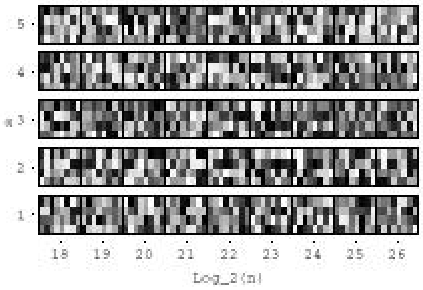
SG100-V4

SG100, as delivered by Protego Information AB.

Load Test for SG100-V4



upper-tail probabilities



Periodlength: ∞, **Speed:** up to 9.500 bytes/sec.
Comments: No flaws detected, the SG100 passes the Load Test with flying colors. The overlapping serial test is not able to distinguish the noise of SG100 from real random noise.

Acknowledgements: The computations in this study heavely rest upon PRNG library [3] and the testing environment pLAB, see [1, 2]. The author would like to thank the people of the pLAB research group for there support.

References

[1] H.Leeb. pLAB – a system for generating and testing random numbers. Report no. 3, pLAB – reports, University of Salzburg, 1997. Available on the internet at http://random.mat.sbg.ac.at/team/.

[2] H. Leeb pLAB – library reference, version 1.0. Report no. 4, pLAB – reports, University of Salzburg, 1997. Available on the internet at http://random.mat.sbg.ac.at/team/

[3] O. Lendl. Design and implementation of a generic pseudorandom number generator library. Report no. 5, pLAB – reports, University of Salzburg, Austria, 1997. Available on the internet at http://random.mat.sbg.ac.at/team/

[4] S. Wegenkittl. The pLAB Picturebook: Load tests and ultimate load tests, part I. Report no. 1, pLAB – reports, University of Salzburg, 1997. Available on the internet at http://random.mat.sbg.ac.at/team/

THE

PLab

RESEARCH
GROUP

Institut für Mathematik
Universität Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg

Research goals

- Analysis of random number generators (RNGs)
- Design of figures of merit for RNGs
- Software tools for generating and testing random numbers

Staff

- Ass. Prof. Dr. Peter Hellekalek, group leader
- Mag. Dr. Karl Entacher
- Mag. Otmar Lendl
- Mag. Stefan Wegenkittl
- Mag. Hannes Leeb
- Mag. Karin Schaber

Address

Dept. Of Mathematics, University of Salzburg,
Hellbrunnerstr. 34, A-5020 Salzburg, Austria.
e-mail: Peter.Hellekaleg@sbg.ac.at
www: http://random.mat.sbg.ac.at

Editor of report series: Peter Hellekalek

The aim of this report series is the fast distribution of recent results of the pLAB research group. Documents are also available via World Wide Web at http://random.mat.sbg.ac.at