

Research Journal for Preston Maness during Senior Design I: A Hardware Random Number Generator

Preston Maness

Abstract—Just a dummy abstract here. Probably won't actually use an abstract for the journal.

CONTENTS

I Initial Research - What I've Found

References

I. INITIAL RESEARCH - WHAT I'VE FOUND

BLAH blah blah... List of sources below. Going to keep adding text in here so that the itemize list doesn't get shoved up into the fancy 'B' character of "Blah."

- [1] Evaluating a TRNG in hardware.
- [2] Noise resistant TRNG. Stochastic model for parameter choicing.
- [3] Importance of RNG choice in GIS applications.
- [4] Ring-based RNG. Huh? What's that?
- [5] Investigating LFSR, LCG, and Blum Blum Shub on Xilinx FPGA
- [6] Non-Uniform RNG, Statistics of.
- [7] "Data-oriented" RNG? Not sure what this is about, but it mentions making distributions of random numbers with different characteristics (uniform, chi-squared, etc)
- [8] GPU Accelerated Scalable Parallel RNG.

REFERENCES

- [1] M. Soucarros, J. Clediere, C. Dumas, and P. Elbaz-Vincent, "Fault analysis and evaluation of a true random number generator embedded in a processor." *JOURNAL OF ELECTRONIC TESTING-THEORY AND APPLICATIONS*, vol. 29, no. 3, pp. 367 – 381, n.d. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000321520700011&site=eds-live&scope=site>
- [2] T. Amaki, M. Hashimoto, Y. Mitsuyama, and T. Onoye, "A worst-case-aware design methodology for noise-tolerant oscillator-based true random number generator with stochastic behavior modeling." *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 8, no. 8, pp. 1331 – 1342, n.d. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000322026900007&site=eds-live&scope=site>
- [3] s. Barry, Simon C.I., "How much impact does the choice of a random number generator really have?." *International Journal of Geographical Information Science*, vol. 25, no. 4, pp. 523 – 530, 2011. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=60827948&site=eds-live&scope=site>
- [4] M. Ayat, Mehdi1, m. Atani, Reza Ebrahimi2, and r. Mirzakuchaki, Sattar1, "On design of puf-based random number generators." *International Journal of Multimedia & Its Applications*, vol. 3, no. 3, pp. 30 – 40, 2011. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=61025496&site=eds-live&scope=site>
- [5] j. Kumar, Jay1, s. Shukla, Sudhanshu1, e. Prakash, Dhiraj1, p. Mishra, Pratyush1, and s. Kumar, Sudhir1, "Random number generator using various techniques through vhdl." *International Journal of Computer Applications in Engineering Sciences*, vol. 1, no. 2, pp. 127 – 129, 2011. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=82881326&site=eds-live&scope=site>
- [6] s.-k. de Schryver, Christian1, D. Schmidt, N. Wehn, E. Korn, H. Marxen, A. Kostiuk, and R. Korn, "A hardware efficient random number generator for nonuniform distributions with arbitrary precision." *International Journal of Reconfigurable Computing*, pp. 1 – 11, 2012. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=87045573&site=eds-live&scope=site>
- [7] r. Farjami Nezhad, Rasoul1, e. Effatparvar, Mehdi2, and m. Rahimzadeh, Mohammad3, "Designing a universal data-oriented random number generator." *International Journal of Modern Education & Computer Science*, vol. 5, no. 2, pp. 19 – 24, 2013. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=87626745&site=eds-live&scope=site>
- [8] S. Gao and G. Peterson, "Gasprng: Gpu accelerated scalable parallel random number generator library." *COMPUTER PHYSICS COMMUNICATIONS*, vol. 184, no. 4, pp. 1241 – 1249, n.d. [Online]. Available: <http://libproxy.txstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000315974100018&site=eds-live&scope=site>