Light-weight FPGA Implementation of FIPS140-2 Online Statistical Tests

Ihsan Cicek, Mustafa Parlak, and Çetin Kaya Koç
Department of Computer Science
University of California, Santa Barbara

May 4, 2016

Abstract

True random number generators (TRNGs) are one of the most crucial primitives of cryptographic systems. TRNGs produce independent, identically distributed, and unpredictable numbers for use in session keys, protocols, and countermeasures [1]. It is well-known that the statistical properties of the TRNG output can be influenced by ambient conditions, hardware failures or side-channel attacks. A failure in the TRNG can easily result in a catastrophe that invalidates the security proofs of cryptographic algorithms, or disables countermeasures, and breaks system security. As a result of their critical role, there is an ever increasing interest on TRNG side-channel attacks in the literature, which utilize methods such as power rail frequency injection [2], electromagnetic field injection [3, 4, 5], ionizing radiation injection [5, 6], and fault injection [7]. These progressive developments in side-channel research impose the continuous run-time monitoring of the TRNG. International, and federal standards such as ISO/IEC 18031, and FIPS 140-2 mandate the use of run-time test modules for monitoring the statistical quality of the generated random bits [8, 9]. However, continuous operation of the monitoring module becomes a burden from a power consumption point of view, especially when emerging light-weight embedded systems such as internet of things, or portable applications are considered.

In this work, we present a light-weight, energy efficient, and vendor agnostic FPGA implementation of a FIPS140-2 recommended TRNG health monitor for use in light-weight cryptographic applications. We followed a puritanical hardware approach to implement the statistical tests, since green cryptographic systems have limited or no resources available for software implementation. In the hardware design, we have partitioned the design with respect to power consumption, and managed the operation through a simple, yet effective finite state machine. We have developed a new design approach for implementing the poker test in order to avoid the power and area-hungry multiplier employed in traditional designs. In addition, we utilized a multi-bit bus for reporting status to the host system, instead of a conventional mono-bit status signal which creates a single point of attack advantage for an adversary. We introduced a technology agnostic energy efficiency metric for making fair comparisons with similar designs in the literature. To the best of our knowledge, this is the first vendor agnostic design of the FIPS140-2 online tests that can be mapped to any implementation technology without requiring special hardware IP blocks.

References

[1] I. Cicek, A. Pusane, and G. Dundar, "A new dual entropy core true random number generator," *Analog Integrated Circuits and Signal Processing*, vol. 81, no. 1, pp. 61–70, 2014.

[2] S. Buchovecka and J. Hlavac, "Frequency injection attack on a random number generator," in *Design and Diagnostics of Electronic Circuits Systems (DDECS), 2013 IEEE 16th International Symposium on*, April 2013, pp. 128–130.

[3] F. Poucheret, K. Tobich, M. Lisarty, L. Chusseau, B. Robisson, and P. Maurine, "Local and direct em injection of power into cmos integrated circuits," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, Sept 2011, pp. 100–104.

[4] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, "Electromagnetic analysis on ring oscillator-based true random number generators," in *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on*, May 2013, pp. 1954–1957.

[5] M. Raitza, M. Vogt, C. Hochberger, and T. Pionteck, "Influence of magnetic fields and x-radiation on ring oscillators in fpgas," in *Parallel Distributed Processing Symposium Workshops (IPDPSW), 2014 IEEE International*, May 2014, pp. 199–204.

[6] H. Martin, A. Vaskova, C. Lopez-Ongil, E. San Millan, and M. Portela-Garcia, "Effect of ionizing radiation on trngs for safe telecommunications: Robustness and randomness," in *On-Line Testing Symposium (IOLTS), 2014 IEEE 20th International*, July 2014, pp. 202–205.

[7] H. Martin, T. Korak, E. San Millan, and M. Hutter, "Fault attacks on strngs: Impact of glitches, temperature, and underpowering on randomness," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 2, pp. 266–277, Feb 2015.

[8] International Organization for Standardization, "Information technology – security techniques – random bit generation," *ISO 18031:2011(E).*, Mar. 2011.

[9] NIST, "FIPS PUB 140-2, security requirements for cryptographic modules," U.S. DoC/National Institute of Standards and Technology, FIPS-140-2, 2002.