An Oscillator-based True Random Number Generator with Process and Temperature Tolerance

Takehiko Amaki, Masanori Hashimoto and Takao Onoye
Dept. Information Systems Engineering, Osaka University

Abstract—**This paper presents an oscillator-based true random number generator (TRNG) that automatically adjusts the duty cycle of a fast oscillator to 50 %, and generates unbiased random numbers tolerating process variation and dynamic temperature fluctuation. Measurement results with 65nm test chips show that the proposed TRNG adjusted the probability of '1' to within 50 ± 0.07 % in five chips in the temperature range of 0 °C to 75 °C. Consequently, the proposed TRNG passed the NIST and DIEHARD tests at 7.5 Mbps with 6,670 μm^2 area.**

I. Introduction

Random number generation is an underlying technology to accomplish highly secure systems. For such systems, a true random number generator (TRNG), which produces random number from physical random sources, is suitable due to its inherent unpredictability of output bits.

Probability of '1' occurrence, p, is the most significant criterion indicating the randomness, and it should be 49.875 % $\leq p \leq$ 50.125 % to pass the frequency test of NIST tests [1]. Process variation, temperature fluctuation, and power supply noise easily make the probability exceed the acceptable range.

Oscillator-based TRNG, which utilizes jitter of oscillators as a randomness source, is a popular method for generating true random numbers (e.g. [2]). This is because it simply consists of digital circuits, i.e. oscillators and a sampler and hence the oscillator-based TRNG is easy to implement, process-portable, and process-scalable. In addition, the TRNG is inherently tolerant to deterministic supply noises [3].

This paper proposes an oscillator-based TRNG which dynamically adjusts the duty cycle of the oscillator for unbiasing the output random bits. Thanks to this unbiasing, the proposed TRNG attains robustness to the process and temperature variations in addition to the deterministic noises.

II. Proposed oscillator-based TRNG

Figure 1 shows the proposed oscillator-based TRNG with the duty cycle correction [4]. The fast oscillating signal is sampled with the jittery slow clock. An output being determined by a time when the clock rises, the randomly fluctuating rise edges of the slow signal result in a random bit stream. Then, the duty cycle of the fast oscillator determines the probability of '1' occurrence. In the proposed TRNG, the duty cycle correction is enabled by the duty cycle monitor, the duty cycle corrector and the corrector controller. The duty cycle monitor outputs a digitized number representing the duty cycle. The controller receives the digitized monitor output, and looks up the target monitor output from the table whose key is temperature. Then, the controller outputs a control signal to the duty cycle corrector so that the monitor output gets close to the target output.

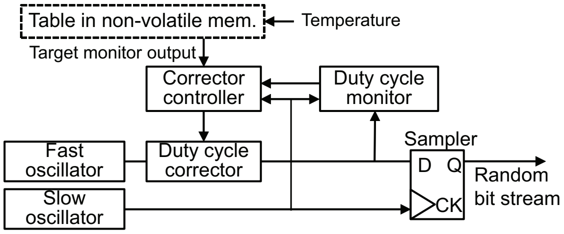

Fig. 1. Block diagram of the proposed TRNG.

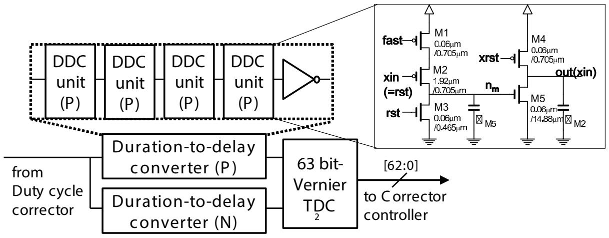

Fig. 2. Block diagram of duty cycle monitor.

The duty cycle corrector is a programmable delay cell whose propagation delay for rising input is controllable while the delay for falling input is constant. The duty cycle corrector consists of a coarse corrector and a fine corrector. Both the correctors have the same circuit topology, but their resolutions are designed differently via transistor sizing. The coarse corrector is configured statically, and it compensates the bias originating from process variation. The fine corrector is automatically controlled by the corrector controller for coping with dynamic temperature fluctuation.

Figure 2 shows a block diagram of the duty cycle monitor. While the P-type and N-type DDCs, which have complimentary structures, receive the same fast oscillating signal, the rise transition timings at the outputs are different. The time difference between the two rising edges of the P-type DDC and the N-type DDC becomes larger as the duty cycle increases. The important point here is the time difference represents the duty cycle. The time difference is digitized by the Vernier TDC and then is given to the controller.

The DDC includes serially-connected DDC units, and in this work each DDC consists of four DDC units (Fig. 2). The P-type DDC unit receives the signal from the fast oscillator (fast) and positive and negative resets (rst and xrst), where rst and xrst are generated from the signal of the slow oscillator. In the first DDC unit, xin is equal to rst, and in the other DDCs, xin is connected to out of the previous unit. In an initial state, xrst is LOW, and rst and xin of the first unit are HIGH, and thus C_{M2} is charged through M4 and C_{M5} is discharged through M3. After that, xrst changes to HIGH, and rst and xin of the first unit become LOW. In this situation, M1 and M2 charge C_{M5} while fast is LOW. The transistors of M1 and M2 cannot fully charge C_{M5} within a cycle of fast, and the voltage

978-1-4799-7792-5/15/$31.00 ©2015 IEEE

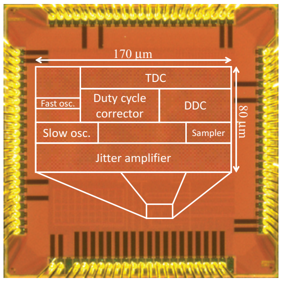

Fig. 3. Chip photo.

TABLE I
COMPARISON WITH OTHER TRNGS.

	Bucci2003[7]	Bucci2008[2]	Pareschi2010[8]	Srinivasan2010[6]	This work
Principal	Direct amp.	Oscillator-based	Chaos-based	Metastable-based	Oscillator-based
Technology	180 nm	90 nm	180 nm	45 nm	65 nm
Area normalized to 45nm	1,563 μm^2	3,250 μm^2	7,875 μm^2	4,004 μm^2	3,335 μm^2
Throughput	40 Mbps	1.74 Mbps	80 Mbps	2.4 Gbps	7.5 Mbps
Randomness Assessment	FIPS140-1 Knuth	AIS31 Entropy eval.	NIST SP800-22	NIST SP800-22 Entropy eval. Autocorrelation eval. Run length eval.	NIST SP800-22 DIEHARD
Post processing	XOR	LSFR	-	-	-

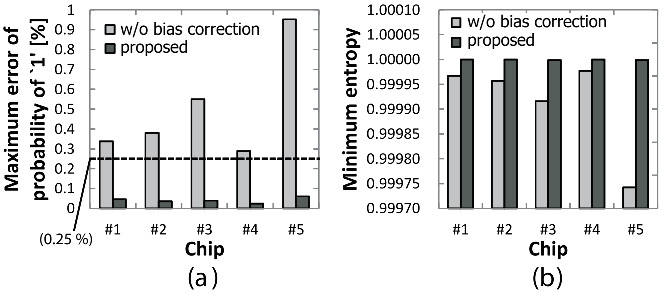

Fig. 4. (a) Maximum error of probability of '1' (b) Minimum entropy. Temperature is changed from 0 °C to 75 °C.

at node n_m increases gradually rather than stepwise, because the frequency of fast is high and the RC product of C_{M5} and the series on-resistances of M1 and M2 is much larger than the cycle time of the fast oscillator. This gradual charging enhances the time resolution of the proposed monitor. In the meantime, the voltage at n_m exceeds the threshold voltage of M5, and M5 turns on. C_{M2} is discharged through M5, and then, LOW signal is output to the next DDC unit.

It should be emphasized that the proposed monitor estimates the duty cycle for every random bit generation, and hence the proposed TRNG can cope with faster dynamic environmental fluctuation compared to conventional output bit sampling.

III. MEASUREMENT RESULTS

The proposed TRNG was fabricated with a 65 nm CMOS process. Figure 3 shows a chip photo of the implemented TRNG. The oscillators, the duty cycle monitor, the duty cycle corrector and the sampler were implemented on the chip, and the total macro cell area is 6,500 μm^2. The corrector controller and the table of the target monitor outputs were implemented with FPGA and a discrete thermal sensor was employed. The throughput was determined to make the slow oscillator have enough jitter [5].

Figure 4 (a) shows the maximum errors from 50% with and without the bias correction. Five TRNGs on different chips were measured. Temperature was changed from 0 °C to 75 °C. The proposed TRNG effectively reduces the error to 0.07 %. Figure 4 (b) shows the minimum entropy with and without the correction. The proposed TRNG attained more than 0.999999 of entropy in the five chips even under temperature variation, while the entropy without bias correction degraded significantly. Thus, the proposed TRNG attained process and temperature tolerance.

In addition, we confirmed that the measurement time of the proposed monitor was 4,100 times as short as that of the random sampling. From another point of view, the proposed monitor attained 70 times higher accuracy when the measurement time is one cycle of the slow oscillator.

The implemented TRNG with the proposed 0/1 bias corrrelation successfully passed all the NIST and DIEHARD tests.

Table I shows the performance comparison to other recent TRNGs. The proposed TRNG passed NIST test with a small area without using post processing. In addition, this work has a significant advantage that the TRNG is tolerant to process variation and temperature fluctuation in addition to the robustness to deterministic noises [3], whereas these tolerance and robustness are not clearly demonstrated in the previous publications except [6].

ACKNOWLEDGMENT

This work is supported by SCOPE program of Ministry of Internal Affairs and Communications. The VLSI chip has been fabricated in the chip fabrication program of VDEC, the University of Tokyo in collaboration with STARC, e-Shuttle, Inc., and Fujitsu Ltd.

REFERENCES

[1] A. Rukhin, et al., "A statistical test suite for the validation of random number generators and pseudorandom number generators for cryptographic applications," NIST, pub.800-22rev1a, 2010.

[2] M. Bucci and R. Luzzi, "Fully digital random bit generators for cryptographic applications," *IEEE TCAS-I*, vol. 55, no. 3, pp. 861–875, 2008.

[3] C. S. Petrie and J. A. Connelly, "Modeling and simulation of oscillator-based random number generators," *ISCAS*, vol. 4, pp. 324–327, 1996.

[4] T. Amaki, et al., "A Process and Temperature Tolerant Oscillator-Based True Random Number Generator with Dynamic 0/1 Bias Correction," *A-SSCC*, pp. 133–136, 2013.

[5] T. Amaki, et al., "A Worst-Case-Aware Design Methodology for Noise-Tolerant Oscillator-Based True Random Number Generator with Stochastic Behavior Modeling," *IEEE TIFS*, vol. 8, no. 8, pp. 1331–1342, 2013.

[6] S. Srinivasan, et al., "2.4 GHz 7mW all-digital PVT-variation tolerant true random number generator in 45nm CMOS," *Symposium on VLSI Circuits*, pp. 203–204, 2010.

[7] M. Bucci, et al., "A high-speed IC random-number source for smartcard microcontrollers," *IEEE TCAS-I*, vol. 50, no. 11, pp. 1373–1380, 2003.

[8] F. Pareschi, et al., "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE TCAS-I*, vol. 57, no. 12, pp. 3124–3137, 2010.