7-5

A Process and Temperature Tolerant Oscillator-based True Random Number Generator with Dynamic 0/1 Bias Correction

Takehiko Amaki, Masanori Hashimoto and Takao Onoye
Dept. Information Systems Engineering, Osaka University
Email: {amaki.takehiko, hasimoto}@ist.osaka-u.ac.jp

***Abstract*—This paper presents an oscillator-based true random number generator (TRNG) that dynamically unbiases 0/1 probability. The proposed TRNG automatically adjusts the duty cycle of a fast oscillator to 50 %, and generates unbiased random numbers tolerating process variation and dynamic temperature fluctuation. A prototype chip of the proposed TRNG was fabricated with a 65 nm CMOS process. Measurement results show that the developed duty cycle monitor obtained the probability of '1' 4,100 times faster than the conventional output bit observation, or estimated the probability with 70 times higher accuracy. 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 $\mu\mathrm{m}^2$ area.**

I. Introduction

Random number generation is an underlying technology to accomplish highly secure systems. For example, secret- and public-key generation and challenge-response authentication require unpredictable random number. 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 is the most significant criterion indicating the randomness of the output bit stream. The probability of '1' occurrence, p, should be 49.875 % $\leq p \leq$ 50.125 % to pass the frequency test of NIST tests [1], and the range of acceptable probability is only 0.250 %. Process variation, temperature fluctuation, and power supply noise easily make the probability exceed the acceptable range. For mitigating this, recent literatures presented methods to reduce the bias of probability of '1'. Let us show an example. Srinivasan et al. [2] proposed a TRNG employing a metastable cross-coupled inverter. The TRNG tuned the configuration every cycle according to the output bits, and then, the TRNG attained tolerance to PVT-variation.

Oscillator-based TRNG, which utilizes jitter of oscillators as a random source, is a popular method for generating true random number [3][4][5]. 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 [6].

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 above-mentioned tolerance to the deterministic noises.

II. Proposed oscillator-based TRNG

This section presents the overall structure of the proposed TRNG and explains duty cycle monitoring and correction in the proposed TRNG.

A. Overall Structure

Figure 1 shows the proposed oscillator-based TRNG with the duty cycle correction. The basic components are fast and slow oscillators and a sampler. 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. The duty cycle of the fast oscillator then 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. Temperature information, which is provided by an external thermal sensor, is also given to the corrector controller.

The duty cycle monitor receives the oscillating signal of the fast oscillator and 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. Here, let us explain why the target monitor output is selected according to the temperature. Temperature affects not only the fast oscillator but also the duty cycle monitor and the sampler, and therefore the same digitized monitor outputs do not always mean the same probability of '1' taking into account the temperature change. Accordingly, this work preliminarily measures the monitor outputs corresponding to the target probability of '1'

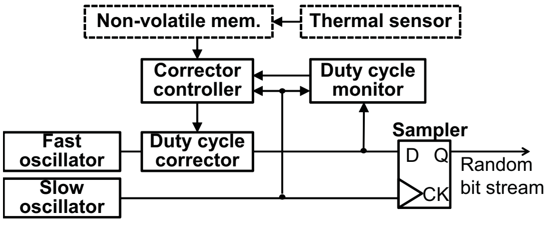

Fig. 1. Block diagram of the proposed TRNG.

978-1-4799-0280-4/13/$31.00 ©2013 IEEE

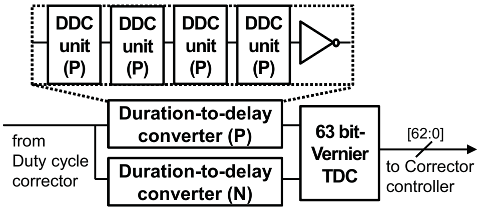

Fig. 2. Block diagram of duty cycle monitor.

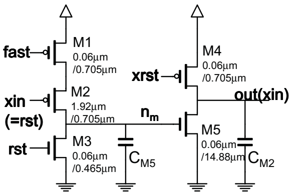

Fig. 3. DDC unit (P).

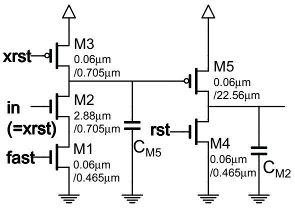

Fig. 4. DDC unit (N).

at various temperatures, and stores those outputs as a table of the target monitor outputs in the non-volatile memory.

The key components of the proposed TRNG are the duty cycle monitor and correctors, and they will be explained below.

B. Duty cycle monitor

Figure 2 shows a block diagram of the duty cycle monitor. The monitor circuit mainly consists of two (P-type and N-type) duration-to-delay converter (DDC) and a Vernier time-to-digital converter (TDC) [7]. While the P-type and N-type DDCs receive the same oscillating signal from the fast oscillator through the duty cycle corrector, 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, where the edge from the N-type DDC is earlier than the P-type. The detailed circuit-level operation of DDCs will be explained later. The important point here is that the time difference represents the duty cycle. The time difference is digitized by the Vernier TDC and then the digitized information of the duty cycle is transmitted to the controller. In this work, a 63-bit Vernier TDC is implemented.

The DDC includes serially-connected DDC units, and in this work each DDC consists of four DDC units (Fig. 2). The schematics of P-type and N-type DDC units are illustrated in Figs. 3 and 4. Here, we explain the behavior of the P-type DDC unit only, but a similar explanation is valid for N-type DDC unit. 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, the voltage of the negative input node (xin) is equal to rst, and in the other DDCs, xin is connected to the output node (out) of the previous unit. Each P-type DDC unit consists of five transistors. We specially illustrate C_{M2} and C_{M5} which represent the gate capacitances of M2 and M5, since their gate areas are larger than the other transistors.

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. Note that the fast oscillating signal is always input to fast. 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 at node n_m, which is the gate voltage of M5, 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 since even a small difference between the durations of HIGH and LOW is amplified in time by accumulating the difference across several cycles and consequently a larger temporal fluctuation of the rise transition at node n_m can be obtained. 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. This circuit operation repeats sequentially in the series-connected four DDC units. Finally, the NOT gate in Fig. 2 receives the fall edge from the last DDC unit and generates a rise signal as an output of the P-type DDC. In the N-type DDC, a buffer instead of the NOT gate is connected at the last stage.

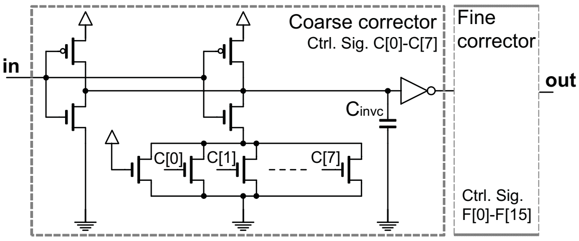

Fig. 5. Schematic of duty cycle corrector.

It should be emphasized that the proposed duty cycle monitor estimates the duty cycle for every random bit generation, i.e. the monitor outputs the estimate every cycle of the slow oscillator. On the other hand, when the duty cycle is estimated from the output bit sequence, we need to gather a number of bits to obtain statistically accurate estimation. This means that the proposed TRNG can cope with faster dynamic environmental fluctuation.

C. Duty cycle corrector

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. Figure 5 shows a schematic of the programmable delay cell, namely the duty cycle corrector. An oscillating signal from the fast oscillator is input to in, and the output signal of out is given to the duty cycle monitor and the sampler. The duty cycle corrector consists of two correctors; a coarse corrector and a fine corrector. Both the correctors have the same circuit topology, but their resolutions of duty cycle correction are differently designed via transistor sizing. The coarse corrector is configured statically, and it compensates the bias originating from process variation. On the other hand, the fine corrector is automatically controlled by the corrector controller, and it

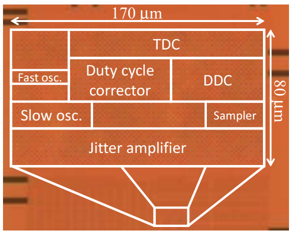

Fig. 6. Chip photo.

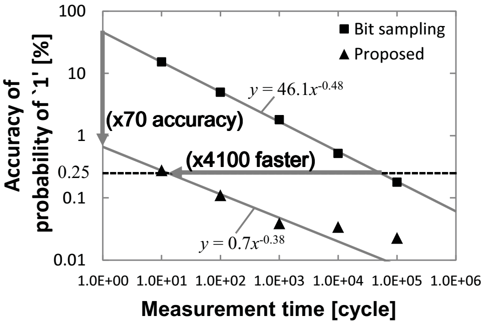

Fig. 7. Accuracy of probability of ‘1’.

corrects the bias due to dynamic temperature fluctuation.

The coarse corrector consists of a programmable inverter [2] and a normal inverter whose input capacitance is $\mathrm{C_{invc}}$ (Fig. 5). Here, we only explain the behavior of the coarse corrector since the fine corrector operates in the same manner. The programmable inverter consists of two inverters connected in parallel, one of which includes gating transistors to control NMOS drive strength. A rising signal of in propagates through the programmable inverter by discharging $\mathrm{C_{invc}}$ with the NMOSs, and the discharging current depends on the number of enabled transistors. The control signal, C, thus changes the delay for a rise input signal. On the other hand, the PMOS drive strength is constant. Consequently, the duty cycle corrector adjusts the duty cycle by changing the rise propagation delay.

III. Measurement Results

This section shows measurement results of the proposed TRNG and gives comparisons with TRNGs in literatures.

A. Prototype chip

The proposed TRNG was fabricated with a 65 nm CMOS process. Figure 6 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 $\mu\mathrm{m}^2$. The corrector controller and the table of the target monitor outputs were implemented with FPGA (Cyclone II), and a discrete thermal sensor (MAXIM DS1621) was employed.

B. Duty cycle monitor

This subsection evaluates the quickness of the duty cycle estimation. For comparison, a random bit sampling method is considered here, which gathers a bit sequence from the TRNG output and calculates the proportion of ‘1’ occurrence.

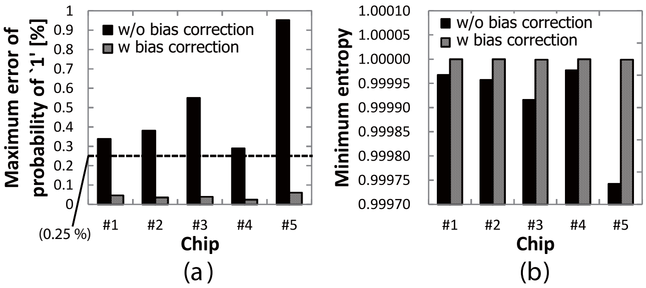

Fig. 8. (a) Maximum error of probability of ‘1’ (b) Minimum entropy. Temperature is changed from 0 °C to 75 °C.

TABLE I
Results of NIST randomness test. Temperature is 25 °C.

Test name	P-value	Pass rate
Frequency	0.0003	0.99
BlockFrequency	0.0083	0.98
CumulativeSums	0.0019	0.99
Runs	0.4190	0.98
LongestRun	0.1296	0.99
Rank	0.1296	0.98
FFT	0.7399	1.00
NonOverlappingTemplate	0.1626	0.96
OverlappingTemplate	0.0401	0.98
Universal	0.4012	0.99
ApproximateEntropy	0.4012	0.99
RandomExcursions	0.0007	0.98
RandomExcursionsVariant	0.0027	0.98
Serial	0.2757	1.00
LinearComplexity	0.9241	1.00
Summary	ALL PASS	

Figure 7 shows the accuracies of probability estimation with the duty cycle monitor and with the random sampling. The y-axis represents the standard deviation of the measured 100 duty cycles, which corresponds to the statistical accuracy of the duty cycle estimation. The x-axis is the time spent to measure a duty cycle. The time unit is the number of cycles of the slow oscillator. As the measurement time becomes longer, the random sampling method has more 0/1 samples and the proposed monitor can output more estimates of duty cycle. In this case, the statistical uncertainty decreases. From another viewpoint, the x-axis can be regarded as the time required to attain the corresponding accuracy. VDD for the DDC was 0.9 V and VDD for the others were 1.2 V.

Figure 7 shows that the measurement time of the proposed monitor is 4,100 times as short as that of the random sampling when the pass mark of accuracy is set to 0.25 % as an example. From another point of view, the proposed monitor attains 70 times higher accuracy when the measurement time is one cycle of the slow oscillator. That is, in this case, the error of the probability of ‘1’ from 50 % is estimated to be 0.7 % with the proposed duty monitor while the error is 46.1 % with the random sampling method. For reference, the TRNG in [2] adjusts the bias every cycle according to the output bit, which corresponds to the probability estimation by the random sampling method with one cycle.

C. Duty cycle correction

This subsection shows the utility of the dynamic duty cycle correction. 2-Mbit streams were measured with a logic ana-

TABLE II

COMPARISON WITH OTHER TRNGS.

	Bucci2003[11]	Bucci2008[3]	Pareschi2010[12]	Srinivasan2010[2]	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	25,000 $\mu\mathrm{m}^2$	13,000 $\mu\mathrm{m}^2$	126,000 $\mu\mathrm{m}^2$	4,004 $\mu\mathrm{m}^2$	6,670 $\mu\mathrm{m}^2$
Area normalized to 45nm	1,563 $\mu\mathrm{m}^2$	3,250 $\mu\mathrm{m}^2$	7,875 $\mu\mathrm{m}^2$	4,004 $\mu\mathrm{m}^2$	3,335 $\mu\mathrm{m}^2$
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	-	-	-

lyzer, and the probability of '1' and entropy were calculated. Five TRNGs on different chips were measured. Temperature was changed from 0 °C to 75 °C.

Figure 8 (a) shows the maximum errors from 50% with and without the bias correction. The proposed TRNG effectively reduces the error to 0.07 %. Figure 8 (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.

D. Randomness test

The proposed TRNG was evaluated with NIST [1] and DIEHARD [8] tests. NIST and DIEHARD tests evaluated 100 M and 80 M random bits obtained from the TRNG, respectively. Temperature was set to 25 °C. A bitrate controller which was attached to the TRNG output discarded a half of the sampled bits. The frequency of the slow oscillator was 15.1 MHz, and then, the TRNG throughput was 7.5 MHz, where the throughput was determined to make the slow oscillator have enough jitter [9].

Table I lists the results of NIST randomness test. The implemented TRNG with the proposed 0/1 bias correlation successfully passed all the tests.

DIEHARD test returned 221 p-values, and the smallest and largest values were 0.0046 and 0.9995. According to [10], a TRNG passes the entire test suite with a 95 % confidence interval when the p-values are between 0.0001 and 0.9999. We thus conclude the proposed TRNG passed DIEHARD test.

E. Comparison

We finally compare the proposed TRNG to others. The area of our TRNG is estimated as follows. The area for the oscillators, the sampler, and the duty cycle monitor and corrector is estimated to be 6,500 μm^2 from the test chip layout. The corrector controller, which was implemented on an FPGA in the measurement, was synthesized for the same 65nm process by a logic synthesis tool and the estimated area is 170 $\mu\mathrm{m}^2$. A temperature sensor was assumed to already exist for other purposes. The total area is therefore 6,670 $\mu\mathrm{m}^2$.

Table II 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 [6], whereas these tolerance and robustness are not clearly stated in the previous publications.

IV. CONCLUSION

This paper presented an oscillator-based TRNG with dynamic 0/1 bias correction. The proposed duty cycle monitor and corrector make the TRNG tolerant to process and temperature variations, and their contribution to the randomness improvement was clarified with 65nm test chips.

ACKNOWLEDGMENT

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

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] 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.

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

[4] G. K. Balachandran and R. E. Barnett, "A 440-nA true random number generator for passive RFID tags," *IEEE TCAS-I*, vol. 55, no. 11, 2008.

[5] B. Sunar, et al., "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Computers*, vol. 56, no. 1, pp. 109–119, 2007.

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

[7] P. Dudek, et al., "A high-resolution CMOS time-to-digital converter utilizing a Vernier delay line," *IEEE JSSC*, vol. 35, no. 2, pp. 240–247, 2000.

[8] G. Marsaglia, Diehard battery of tests of randomness, 1995.

[9] 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.

[10] Intel platform security division, "The Intel random number generator," Intel technical brief, 1999.

[11] 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.

[12] 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.