IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

VOL. E97-A NO. 12
DECEMBER 2014

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER *Special Section on VLSI Design and CAD Algorithms*

A Process and Temperature Tolerant Oscillator-Based True Random Number Generator

Takehiko AMAKI[†,††], ***Nonmember***, **Masanori HASHIMOTO**[†,††a)], ***and*** **Takao ONOYE**[†,††b)], ***Members***

SUMMARY 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 μm^2 area.

key words: *true random number generator, hardware random number generator, oscillator-based random number generator*

1. 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’. Figure 1 illustrates the basic concept of bias correction. The bias monitor measures the bias of the TRNG, the information of the bias is feed to the bias corrector through the controller, and the corrector compensates the bias of the 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.

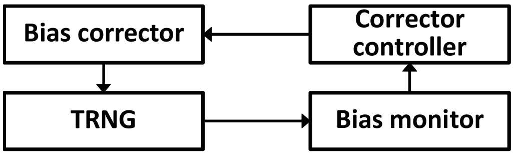


Fig. 1 Basic concept of bias corrrection.

Oscillator-based TRNG, which utilizes jitter of oscillators as a random source, is a popular method for generating true random number [3]–[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. For this purpose, we have developed a duty cycle monitor and duty cycle corrector. 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.

The rest of this paper is organized as follows. Section 2 describes the structure of the proposed TRNG and explains its operation. Section 3 presents measurement results of the proposed TRNG fabricated with a 65 nm technology. Finally, concluding remarks are given in Sect. 4.

2. Proposed Oscillator-Based TRNG

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

2.1 Overall Structure

Figure 2 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 mon-

Manuscript received March 13, 2014.
Manuscript revised June 30, 2014.

[†]The authors are with the Department of Information Systems Engineering, Osaka University, Suita-shi, 565-0871 Japan.
[††]The authors are with JST, CREST, Suita-shi, 565-0871 Japan.
a) E-mail: hasimoto@ist.osaka-u.ac.jp
b) E-mail: onoye@ist.osaka-u.ac.jp

DOI: 10.1587/transfun.E97.A.2393

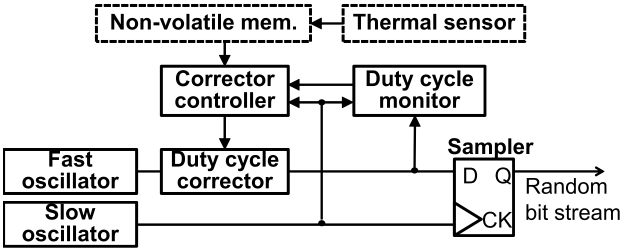


Fig. 2 Block diagram of the proposed TRNG.

itor, 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. The outputs of the monitor are digital signals, which enables easy processing in the corrector controller. 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’ at various temperatures, and stores those outputs as a table of the target monitor outputs in the non-volatile memory. The duty cycle corrector varies the duty cycle of fast oscillating signal according to the control signals. This process can also eliminate effects of manufacturing variability on the quality of TRNG output.

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

2.2 Duty Cycle Monitor

Figure 3 illustrates a concept of the proposed duty cycle monitor. Output bit sampling, which is a method of duty cycle estimation, is also shown for comparison. Output bit sampling, whose principle is similar to the random sampling method [7], gathers the output bits from the sampler and calculates the proportion of ‘1’ as the duty cycle. Note that output bit sampling uses jittery slow oscillator as the random clock while the random sampling method [7] employs the chaotic oscillator, and then output bit sampling requires several cycles of the slow oscillator. On the other hand, the proposed monitor directly measures time differences between HIGH and LOW of the fast signal and obtains the duty cycle. The monitor estimates the duty cycle within one cycle of the slow oscillator, which is much faster than output bit sampling.

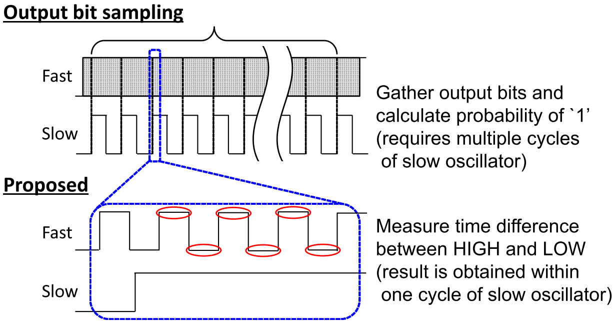

Output bit sampling
Fast
Slow
Gather output bits and calculate probability of `1' (requires multiple cycles of slow oscillator)
Proposed
Fast
Slow
Measure time difference between HIGH and LOW (result is obtained within one cycle of slow oscillator)

Fig. 3 Concept of the duty cycle monitor. Output bit sampling is also shown for comparison.

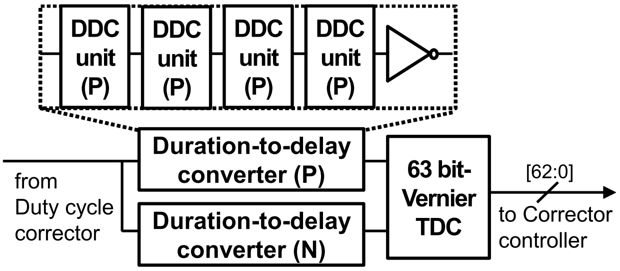


Fig. 4 Block diagram of duty cycle monitor.

Figure 4 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) [8]. 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. An 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. 4). The schematics of P-type and N-type DDC units are illustrated in Figs. 5 and 6. 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

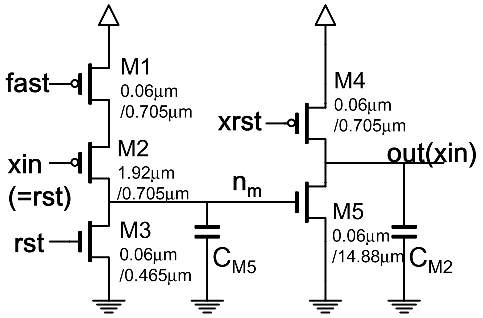


Fig. 5 DDC unit (P).

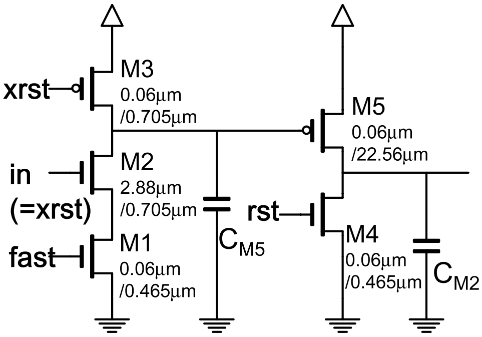


Fig. 6 DDC unit (N).

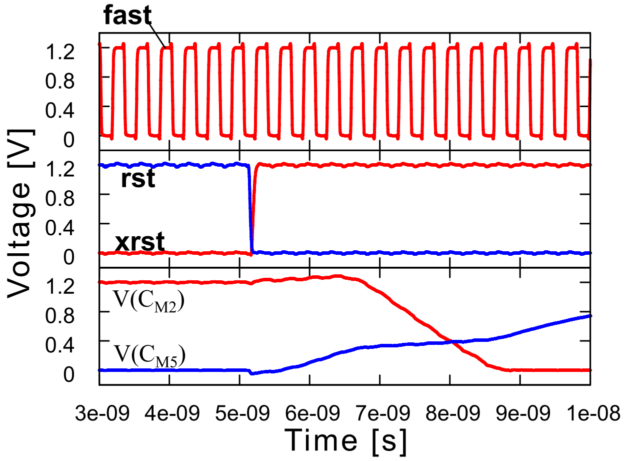


Fig. 7 Waveforms inside a P-type DDC unit.

areas are larger than other transistors.

Figure 7 exemplifies waveforms at the nodes in the P-type DDC unit. V(C_{M5}) and V(C_{M2}) mean the input gate voltages to M5 and M2. 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. 4 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.

To sum up, the propagation delay of the P-type DDC unit depends on the time necessary to charge C_{M5} up, and therefore, the delay gets larger as the duty cycle of fast increases. In contrast, the delay of the N-type DDC gets smaller as the duty cycle increases. Therefore, the time difference between the rise transitions of P-type and N-type DDCs increases as the duty cycle becomes higher. This time difference is digitized by the TDC and its information is given to the corrector controller. Please remind that the corrector controller selects the target monitor output from the table stored in the non-volatile memory according to the temperature, and this target monitor output in the table was determined based on the preliminary measurement for calibration as mentioned in Sect. 2.1. This calibration eliminates effects of manufacturing variability on DDC and TDC and impacts of through-current and gate-leakage current on DDC performance, and makes accuracies of, for example, C_{M5}, less important.

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.

2.3 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 8 shows the behavior of the delay cell. An oscillating signal is input to in and is output to out being delayed through the cell. The time of HIGH and LOW of in are T_{HIGH} and T_{LOW}, and those of out are T'_{HIGH} and T'_{LOW}, respectively. The propagation delay for fall edge is D_{fall} and that for rise edge is D_{rise}, which is controlled with ctrl. Here, $T'_{HIGH} = T_{HIGH} - D_{rise} + D_{fall}$ and $T'_{LOW} = T_{LOW} + D_{rise} - D_{fall}$ as illustrated in Fig. 8. Then, the duty cycle of in, d_{in}, and that of out, d_{out}, are expressed as follows:

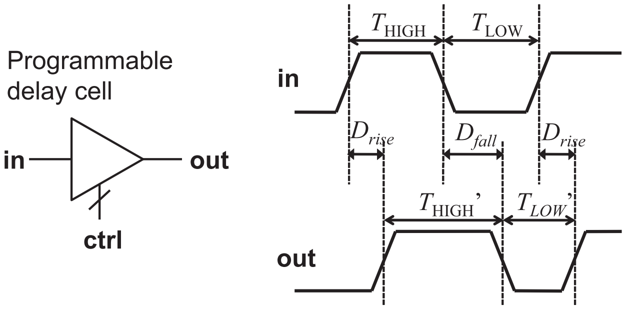


Fig. 8 Behavior of programmable delay cell for duty cycle correction.

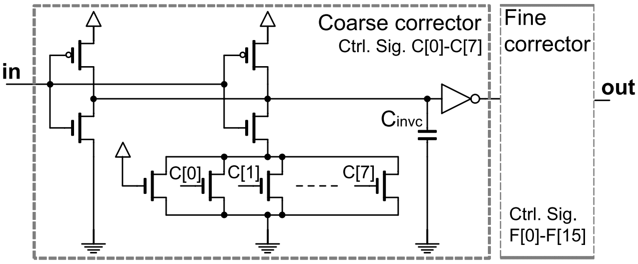


Fig. 9 Schematic of duty cycle corrector.

$$d_{in} = \frac{T_{HIGH}}{T_{HIGH} + T_{LOW}}, \tag{1}$$

$$\begin{aligned} d_{out} &= \frac{T'_{HIGH}}{T'_{HIGH} + T'_{LOW}} \\ &= \left(d_{in} + \frac{D_{fall}}{T_{HIGH}+T_{LOW}}\right) + \frac{D_{rise}}{T_{HIGH}+T_{LOW}}. \end{aligned} \tag{2}$$

The programmable delay cell tunes d_{out} by changing D_{rise}.

Figure 9 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 corrects the bias due to dynamic temperature fluctuation.

We next explain the behavior of the corrector. Here, only the coarse corrector is explained 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 (Eq. (2)).

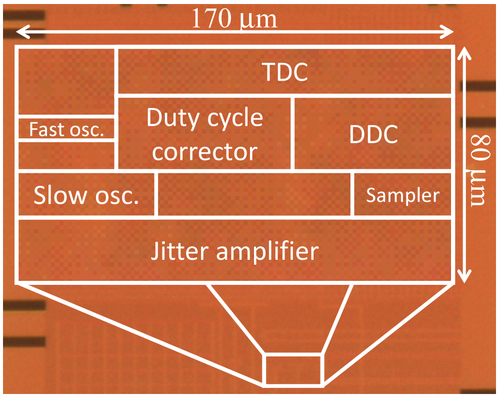


Fig. 10 Chip photo.

3. Measurement Results

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

3.1 Prototype Chip

The proposed TRNG was fabricated with a 65 nm CMOS process. Figure 10 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.

3.2 Duty Cycle Monitor

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

Figure 11 shows the accuracies of probability estimation with the duty cycle monitor and with the output bit 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 output bit 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.

Note that the measured output value of the monitor x was digital data whose bit length was 6 bits, and the value was converted into the duty cycle. The first order

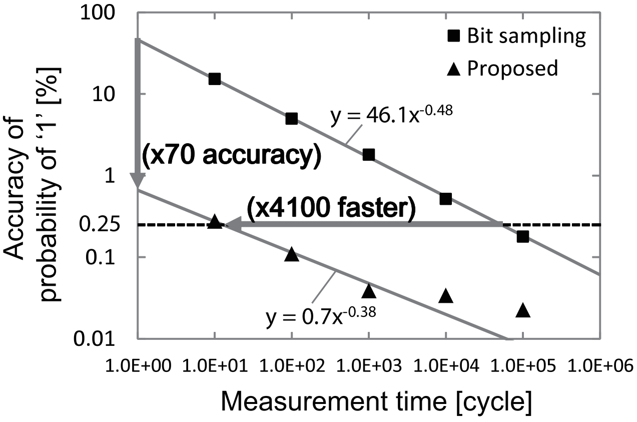


Fig. 11 Accuracy of probability of '1'.

approximation of the probability of '1' at 25°C was $y = 0.16x + 44.22$, and then, the measured output value x was multiplied by 0.16. For example, when a standard deviation of measured output values is 3.0, the converted accuracy of duty cycle is $3.0 \times 0.16 = 0.48\%$.

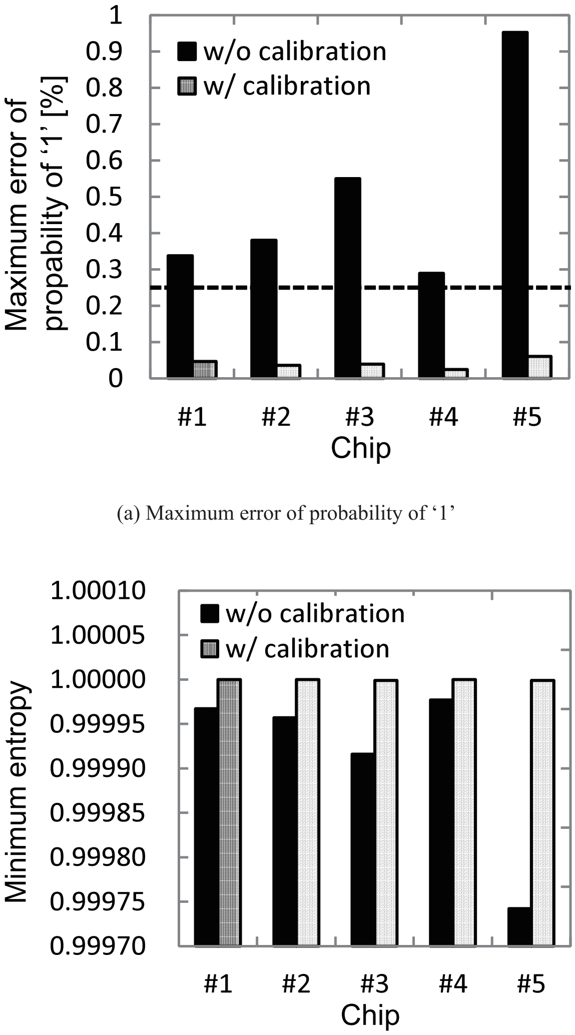
Figure 11 shows that the measurement time of the proposed monitor is 4,100 times as short as that of the output bit sampling when the pass mark of accuracy is set to 0.25% as an example. From another point of view, the proposed monitor attains 70 times higher accuracy when the measurement time is one 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 output bit 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 output bit sampling method with one cycle.

3.3 Duty Cycle Correction

This subsection shows the utility of the dynamic duty cycle correction. 2-Mbit streams were measured with a logic analyzer, 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 12 (a) shows the maximum errors from 50% with and without the bias correction. The proposed TRNG effectively reduces the error to 0.07%. Figure 12 (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.

For ensuring high randomness even under process variation and temperature fluctuation, the proposed TRNG introduced a feedback loop to control the probability of '1' occurrence mainly consisting of duty cycle monitor, duty cycle corrector and corrector controller, since the duty cycle of the fast oscillator mainly determine the probability of '1' occurrence. The experiment confirmed that the proposed TRNG attained process and temperature tolerance.



(a) Maximum error of probability of '1'

(b) Minimum entropy

Fig. 12 (a) Maximum error of probability of '1' (b) Minimum entropy. Temperature is changed from 0°C to 75°C.

3.4 Randomness Test

The proposed TRNG was evaluated with NIST [1] and DIEHARD [9] tests. NIST and DIEHARD tests evaluated 100 M and 80 M random bits obtained from the TRNG, respectively. Temperature was set to 25°C.

The oscillator-based TRNG exploits the jitter of oscillators as randomness source. As the oscillating frequency of the slow oscillator, which is related to the TRNG throughput, becomes higher, the cycle time of the oscillator becomes shorter and consequently the absolute value of the jitter decreases. To generate good random numbers, the absolute value of the jitter should be several times larger than the cycle time of the fast oscillator [10]. Therefore, there is the maximum throughput for the oscillator-based TRNG to have enough randomness and pass the randomness tests. In this experiment, 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. Above this throughput, the TRNG cannot pass NIST tests.

Table 1 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 as listed in Table 2. According to [11], 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.

3.5 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 65 nm process by a logic synthesis tool and the estimated area is 170 μm^2. A temperature sensor was assumed to already exist for other purposes. The total area is therefore 6,670 μm^2.

Table 3 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 demonstrated in most previous publications. For example, TRNGs in [3], [12] have a feedback loop based on output bit sampling, but its effectiveness for the tolerance improvement is not discussed in experiments. In addition, these TRNGs use post processing, and hence the unbiasing performance of the feedback loop, such as accuracy and response time, could be moderate. In [13], variation tolerance is not discussed. On the other hand, a bias correction method for metastable-based TRNG and its effectiveness are presented in [2]. This work adjusts metastable condition of cross-coupled inverters to make the occurrence probability of ‘1’ 50% according to the result of output bit sampling.

Table 1 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	

Table 2 DIEHARD randomness test results. Temperature is 25°C.

Minimum p-value	0.0046
Maximum p-value	0.9995
Result	PASS

4. 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 65 nm test chips.

Acknowledgment

The VLSI chip in this study has been fabricated in the chip fabrication program of VLSI Design and Education Center (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, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, “A statistical test suite for the validation of random number generators and pseudorandom number genera-

Table 3 Comparison with other TRNGs.

	Bucci2003 [12]	Bucci2008 [3]	Pareschi2010 [13]	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 μm^2	13,000 μm^2	126,000 μm^2	4,004 μm^2	6,670 μm^2
Area normalized to 45 nm	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	-	-	-

tors for cryptographic applications," NIST, pub.800-22rev1a, 2010.

[2] S. Srinivasan, S. Mathew, R. Ramanarayanan, F. Sheikh, M. Anders, H. Kaul, V. Erraguntla, R. Krishnamurthy, and G. Taylor, "2.4 GHz 7 mW all-digital PVT-variation tolerant true random number generator in 45 nm CMOS," Symposium on VLSI Circuits, pp.203–204, 2010.

[3] M. Bucci and R. Luzzi, "Fully digital random bit generators for cryptographic applications," IEEE Trans. Circuits Syst. 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 Trans. Circuits Syst. I, vol.55, no.11, pp.3723–3732, 2008.

[5] B. Sunar, B. Sunar, W.J. Martin, and D.R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," IEEE Trans. Comput., 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," Proc. ISCAS, vol.4, pp.324–327, 1996.

[7] R.Z. Bhatti, M. Denneau, and J. Draper, "Duty cycle measurement and correction using a random sampling technique," Proc. MWSCAS, pp.1043–1046, 2005.

[8] P. Dudek, S. Szczepanski, and J.V. Hatfield, "A high-resolution CMOS time-to-digital converter utilizing a Vernier delay line," IEEE J. Solid-State Circuits, vol.35, no.2, pp.240–247, 2000.

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

[10] 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 Trans. Information Forensics and Security, vol.8, no.8, pp.1331–1342, 2013.

[11] Intel platform security division, "The Intel random number generator," Intel Technical Brief, 1999.

[12] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, "A high-speed IC random-number source for smartcard microcontrollers," IEEE Trans. Circuits Syst. I, vol.50, no.11, pp.1373–1380, 2003.

[13] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," IEEE Trans. Circuits Syst. I, vol.57, no.12, pp.3124–3137, 2010.

Takehiko Amaki received the B.E., M.E., and Ph.D. degrees in information systems engineering from Osaka University, Osaka, Japan, in 2008, 2010, and 2013, respectively. He is currently with TOSHIBA Corporation. His research interest includes hardware random number generator.

Masanori Hashimoto received the B.E., M.E. and Ph.D. degrees in Communications and Computer Engineering from Kyoto University, Kyoto, Japan, in 1997, 1999, and 2001, respectively. Since 2004, he has been an Associate Professor in Department of Information Systems Engineering, Graduate School of Information Science and Technology, Osaka University. His research interest includes computer-aided-design for digital integrated circuits, and high-speed circuit design. Dr. Hashimoto served on the technical program committees for international conferences including DAC, ICCAD, ITC, Symposium on VLSI Circuits, ASP-DAC, DATE, ISPD and ICCD. He is a member of IEEE, ACM and IPSJ.

Takao Onoye received the B.E. and M.E. degrees in Electronic Engineering, and Dr.Eng. degree in Information Systems Engineering all from Osaka University, Japan, in 1991, 1993, and 1997, respectively. He is currently a professor in the Department of Information Systems Engineering, Osaka University. His research interests include media-centric low-power architecture and its SoC implementation. He is a member of IEEE, IPSJ, and ITE-J.