3-Gb/s High-Speed True Random Number Generator Using Common-Mode Operating Comparator and Sampling Uncertainty of D Flip-Flop

Sang-Geun Bae, *Student Member, IEEE*, Yongtae Kim, *Student Member, IEEE*, Yunsoo Park, *Student Member, IEEE*, and Chulwoo Kim, *Senior Member, IEEE*

***Abstract*— True random number generators (TRNGs) are important in data encryption for information security applications. In this paper, we propose a TRNG that utilizes a comparator in the common-mode operation and the sampling uncertainty of a D flip-flop (DFF). The comparator output is affected by the input common-mode noise and the noise that is simultaneously self-induced. A slicer generates an unpredictable and asynchronous pulse to the input of the DFF according to the output-referred noise of the comparator. By sampling the random pulse with a 3-GHz external clock, there is a sampling uncertainty, which helps to increase the random quality. As a result, we use the independent two random sources for TRNG. The area of the designed circuit is 1609 μm^2. In spite of the small size, the data rate of the proposed TRNG is 3 Gb/s. We verify that the output bit stream passes all of the National Institute of Standards and Technology test suites. We fabricate the TRNG in a 65-nm CMOS process with a 1.2-V supply voltage. The power consumption of the proposed TRNG is 5 mW, and the energy per bit is 1.6 pJ/b.**

***Index Terms*— Data encryption, National Institute of Standards and Technology (NIST) test, true random number generator (TRNG).**

I. Introduction

THE rapid increase in the number of devices that are connected to the Internet because of the development of Internet of things brings about a greater need for data encryption to ensure information security. Consequently, randomness has attracted a lot of attention as an essential element in the field of encryption and cryptography [1]. There are two types of random number generators—pseudorandom number generator (PRNG) and true random number generator (TRNG). The output bit sequence of the PRNG is generated with a deterministic algorithm. Despite its good statistical random characteristics, the PRNG is not suitable for encryption applications, because it is deterministic and predictable. On the other hand, the TRNG generates an unpredictable random bit sequence using specific random sources with high entropy, and is popular for data encryption in information security. The TRNG can be categorized according to the source of randomness. Typically, thermal noise [2]–[4], oscillator jitter [5]–[10], metastability [11]–[13], and time-to-oxide breakdown [14] have been utilized as random sources. The thermal noise direct-amplification method [3], [4] is often used as a source of randomness even though the noise power is very low, because it is a good source of white noise. For oscillator-based TRNGs, while the circuit implementation is relatively easy, the randomness is poor [9]. The metastability-based TRNG has good randomness, a high operating data rate [11], and no postprocessing. Unfortunately, it occupies a large area [12], [13].

Low-frequency noise, e.g., the *1/f* noise, affects the quality of randomness in the TRNG. In [5], the size of MOSFET was increased to reduce the *1/f* noise. Low-frequency noise can be prevented in our proposed TRNG by using a high-sampling operation. This will be explained later. In this paper, we propose a small-sized TRNG, as shown in Fig. 1, that is easy to design using a common-mode operating comparator and the sampling uncertainty of a D flip-flop (DFF). The proposed TRNG achieves a high data rate, good randomness with a simple structure and occupies small area, while satisfying all the National Institute of Standards and Technology (NIST) tests.

II. Circuit Implementations

Thermal-noise amplifying TRNGs [3], [4] suffer from relatively lower thermal-noise power compared with [2]. The thermal noise of CMOS devices is not sufficient to generate random bits when it is applied to the differential inputs of a comparator. In [2], a SiN layer was also fabricated in a standard CMOS process to generate a larger noise. It was able to occupy a smaller area as no additional circuits such as quality checker were required [4]. However, the manufacturing cost is increased because of the additional SiN photomask. In addition, the reference bias voltage in the comparator should be carefully applied to ensure good randomness. In [3] and [4],

Manuscript received July 7, 2016; revised August 31, 2016 and October 8, 2016; accepted November 1, 2016. Date of publication November 25, 2016; date of current version January 30, 2017. This paper was approved by Associate Editor Vivek De. This work was supported by the National Research Foundation of Korea through the Korean Government within the Ministry of Science, ICT and Future Planning under Grant 2016R1E1A1A02922127.

S.-G. Bae, Y. Park, and C. Kim are with the Department of Electrical Engineering, Korea University, Seoul, South Korea (e-mail: ckim@korea.ac.kr).

Y. Kim is with the Department of Semiconductor Systems Engineering, Korea University, Seoul, South Korea.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSSC.2016.2625341

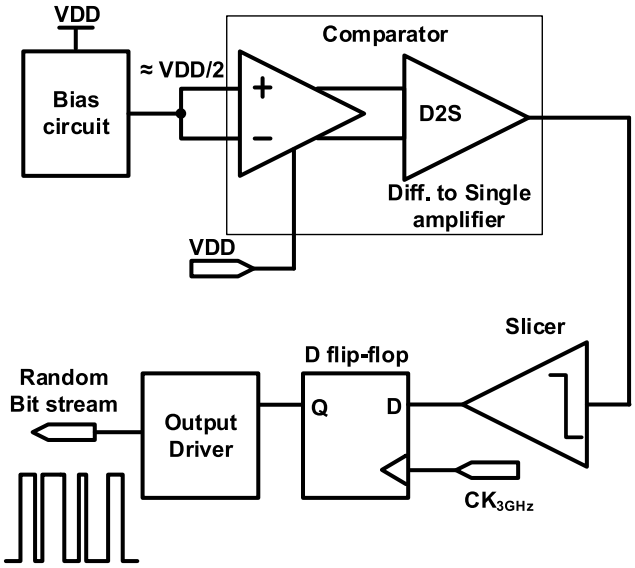


Fig. 1. Top block diagram of the proposed TRNG using a common-mode operating comparator and the sampling uncertainty of a DFF.

an external bias voltage was used. In [2], an *RC* low-pass filter was used with a small-sized nMOS that employs an additional area.

Fig. 1 shows the top block diagram of the proposed TRNG that uses a common-mode operating comparator and sampling uncertainty. It is composed of a biasing circuit (beta-multiplier voltage reference), a comparator with a differential to single amplifier (D2S), a slicer, a DFF, and an output driver. The thermal noise that is a source of randomness is induced by the biasing circuit and comparator. As shown in Fig. 1, the inputs of the comparator are connected together to the output of the bias circuit, which results in the common-mode operation. Then, the clock port is connected to V_{DD} instead of the clock signal, as shown in Fig. 1. By doing this, we resolved the above-mentioned biasing problem in the comparator. At this metastable point, the thermal noise induced by the bias circuit and comparator is added and amplified by the D2S. Then, the slicer splits the output voltage into a high or low value according to the input thermal noise. However, these unexpected pulses are not synchronized with the periodic sampling clock, which is $\mathrm{CK}_{3\ \mathrm{GHz}}$ in Fig. 1. Finally, the asynchronous sequence is sampled at 3 Gb/s by the DFF.

Fig. 2 shows the details of the proposed TRNG circuit and the simulated output random bits. The main differences between our proposed TRNG and the thermal-noise amplifying TRNG in [2]–[4] are the use of a common-mode operating comparator without clocking in our proposed TRNG. Therefore, our proposed TRNG can withstand supply fluctuations or unexpected external noise. We used the transient-noise simulation to quantify the noise in the time domain. The simulated histogram of the input of the slicer ($V_{\mathrm{SLI\_IN}}$) is shown in Fig. 3. The standard deviation (σ) of $V_{\mathrm{SLI\_IN}}$ is 8.26 mV for the case where an all circuit noise is applied. The thermal noise induced by a bias circuit is added to the comparator noise, because the common-mode gain of the comparator is approximately -4 dB at the quiescent point. To verify this, we performed simulations using only the transient noise from the bias circuit or from the comparator. The simulated standard deviation (σ) of $V_{\mathrm{SLI\_IN}}$ noise is 3.59 mV when the noise induced by only the bias circuit is applied. For the case involving only the comparator noise, the simulated value is 4.56 mV.

The mismatch inducing an offset of comparator cannot be avoided, even though the comparator is laid out using common-centroid method. We simulated the offset of the comparator using a Monte Carlo method with the mismatch under process, voltage and temperature (PVT) variation. Fig. 4 shows that the offset variation at the outputs of the comparator under PVT variation is quite small. The comparator output does not go to "1" or "0." Then, the output noise of D2S amplifier ($V_{\mathrm{SLI\_IN}}$) is also verified in 100 trials. The standard deviation of rms value for $V_{\mathrm{SLI\_IN}}$ is 1.185 mV. The lowest and highest voltages are 0.68 and 0.6859 V, respectively. Finally, the noise quality using autocorrelation and the values of Shannon entropy are simulated. The offset voltage between the comparator outputs has the largest value of 21.58 μV at 1.32 V and 100 °C. Therefore, the autocorrelation is determined at this operating point as shown in Fig. 5 and compared with the autocorrelation of the lowest offset point at 1.08 V and -40 °C. The values of Shannon entropy at minimum and maximum offsets are 0.9991 and 0.9996, respectively.

This is different from a conventional meta-stability-based TRNG [11], because the cross-coupled inverter pair in meta-stability state was used. They controlled the number of pMOS and nMOS in cross-coupled inverter to cancel out the common-mode noise such as supply perturbation. The clocked comparator in meta-stability [12], [13] determines the output, directly. However, it has a limitation to increase the data rate due to slower slope of output. In this paper, the combination of continuous comparator and slicer can have 3-Gbps data rate. The beta-multiplier voltage-reference circuit is designed such that it enables the bias circuit to generate a bias point of the half V_{DD}. Then, a slicer determines the output to be "1" or "0," according to the ambiguousness of the input. The slicer is designed such that it generates a random sequence asynchronously. Therefore, depending on the arrival time of data ($V_{\mathrm{DFF\_IN}}$) in the DFF, there is some ambiguousness when it is sampled by a 3-GHz clock. This is a random mechanism that is similar to an oscillator-based TRNG [5]–[10]. This helps to increase the random quality. The conceptual illustration for the proposed TRNG is shown in Fig. 6. It is composed of parts having thermal-noise amplification and sampling uncertainty. This allows good quality of randomness in the output binary sequence. In addition, as shown in Fig. 7, the width of the asynchronous pulse is unpredictable. According to the simulation result, the minimum and maximum pulsewidth are approximately 98 ps and 2.09 ns, respectively, under PVT variations. We chose a sampling clock frequency of 3 GHz by considering a min/max pulsewidth of $V_{\mathrm{DFF\_IN}}$. If the minimum pulsewidth is larger than a twice of clock period. The output data keeps its value at least over two times. We also consider about the maximum pulsewidth. It brings a large run length of output data, if the maximum pulsewidth is too long in terms of sampling frequency. However, the longest

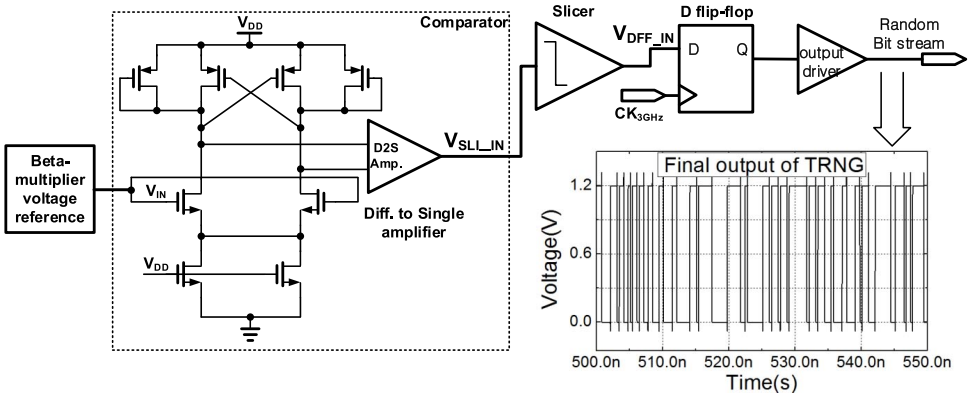


Fig. 2. Schematic of proposed TRNG circuit and simulation result of random bit stream.

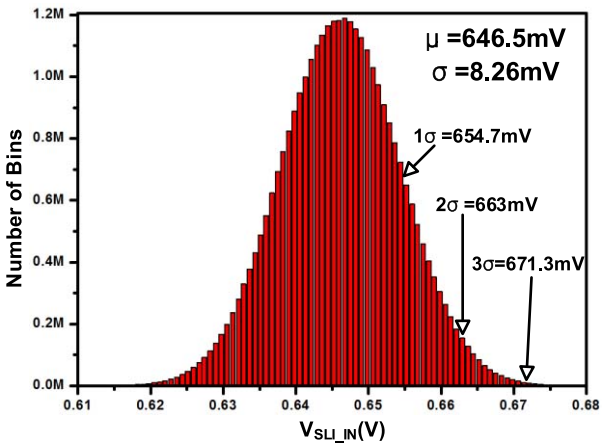


Fig. 3. Simulated histogram result of $V_{\mathrm{SLI\_IN}}$.

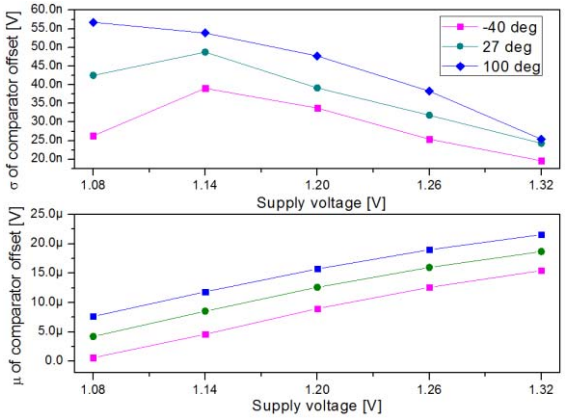


Fig. 4. Monte Carlo mismatch simulation results for standard deviation and mean value of comparator offset under PVT variation.

pulsewidth (2.09 ns) makes 6∼7 run length at 3-GHz sampling, and this is acceptable. In addition, we employed a slicer using the inverter chain, which can be adjusted externally to the logic threshold voltage ($V_{\mathrm{TH\_SLI}}$). Then, $V_{\mathrm{TH\_SLI}}$ is manually controlled according to the PVT variations. The advantages of this TRNG are as follows. First, the quality of randomness is increased by simultaneously using the thermal noise at the comparator in common mode and the sampling uncertainty of the DFF as the sources of randomness. Second, the area can be reduced significantly, because it does not require any additional circuits such as a filtering circuit due to

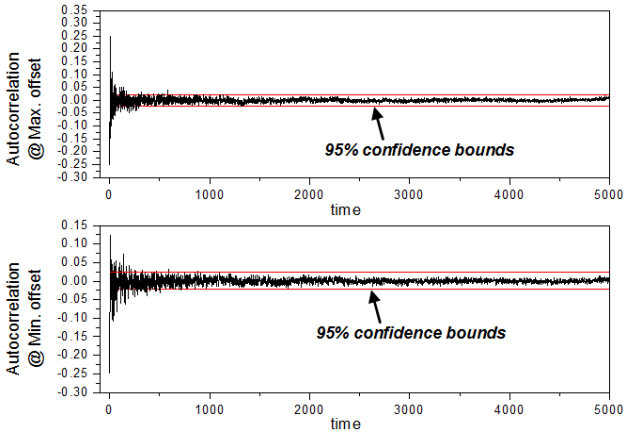


Fig. 5. Autocorrelation results at the maximum and minimum comparator offset.

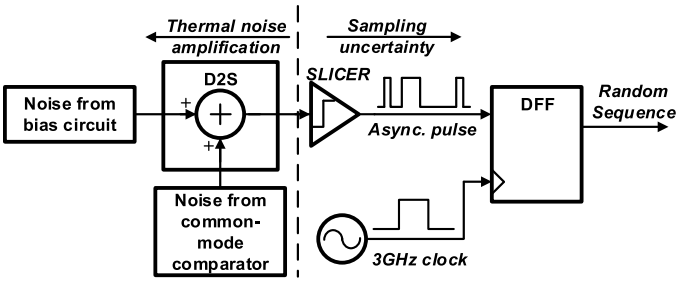


Fig. 6. Conceptual illustration for the proposed TRNG.

common-mode comparator. Finally, the data rate is very high, i.e., up to 3 Gb/s.

III. Measurement and Analysis

The chip microphotograph of the proposed TRNG is shown in Fig. 8. Without the output buffer, the TRNG core cell occupies an area of 1609 μm^2 (20.5 μm × 78.5 μm). Fig. 9 shows a small section of the measured output bit stream and a sampling clock signal waveforms. The 3-GHz clock is externally injected by a signal generator equipment. The oscilloscope captures and stores 100k b of output bit stream for an analysis at an interval of 3 GHz. Fast Fourier transform (FFT) of 2^{17} (# of 131 072 data) with the Hanning window using MATLAB is obtained first, to determine whether it has a periodic component, as shown in Fig. 10. It is shown to be fairly flat in the frequency domain, indicating that the measured output is a random bit stream. In addition,

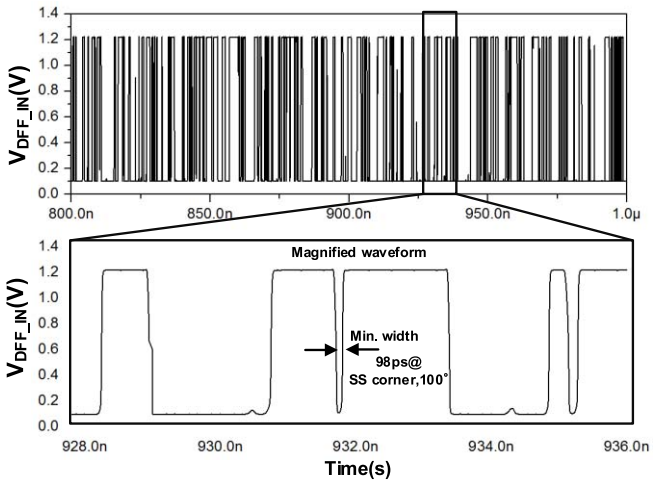


Fig. 7. Simulated waveform for V_{SLI_IN} and magnified waveform, which is near the smallest pulsewidth.

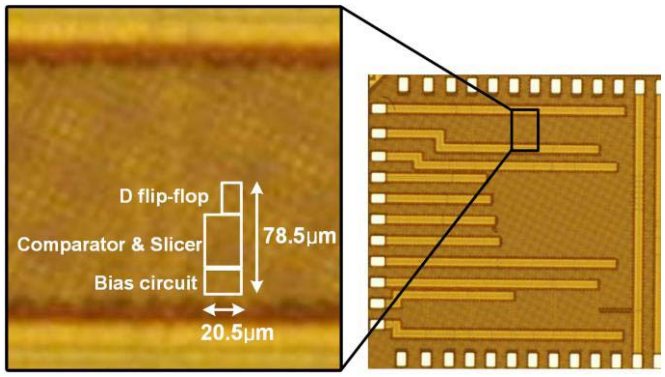


Fig. 8. Chip microphotograph of the proposed TRNG in 65-nm CMOS technology.

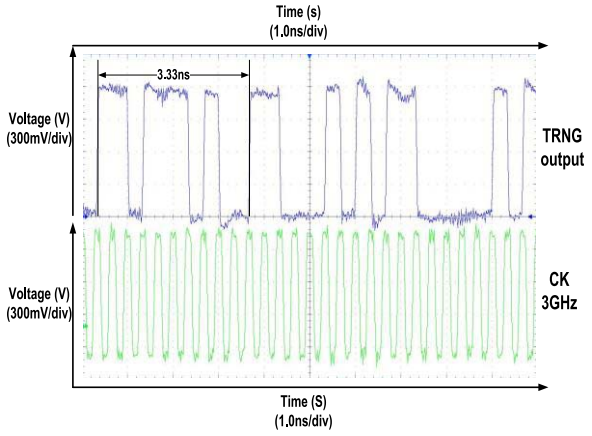


Fig. 9. Portion of measured waveforms for TRNG output and 3-GHz clock signal.

we determined that it does not have a *1/f* noise property. The flicker or *1/f* noise level increases significantly as the frequency decreases. As shown in Fig. 11, because of the flicker noise, the simulated noise power is gradually increased at 10 kHz. However, random source should have a flat frequency response to realize good randomness. To reduce the flicker noise, the size was increased [5] and extra filter was used [13] in previous works. The proposed TRNG can overcome flicker noise via high-speed sampling, i.e., 3 GHz. According to the FFT theory, the lowest component in the

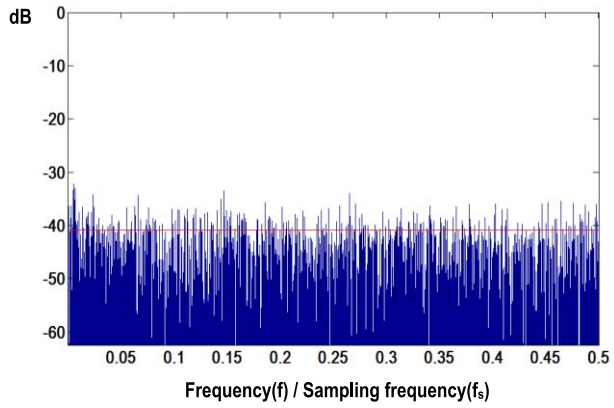


Fig. 10. FFT result obtained using Hanning window with 100k measured samples.

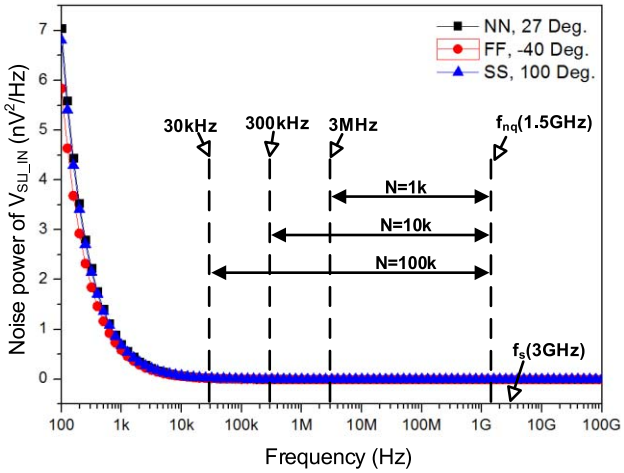
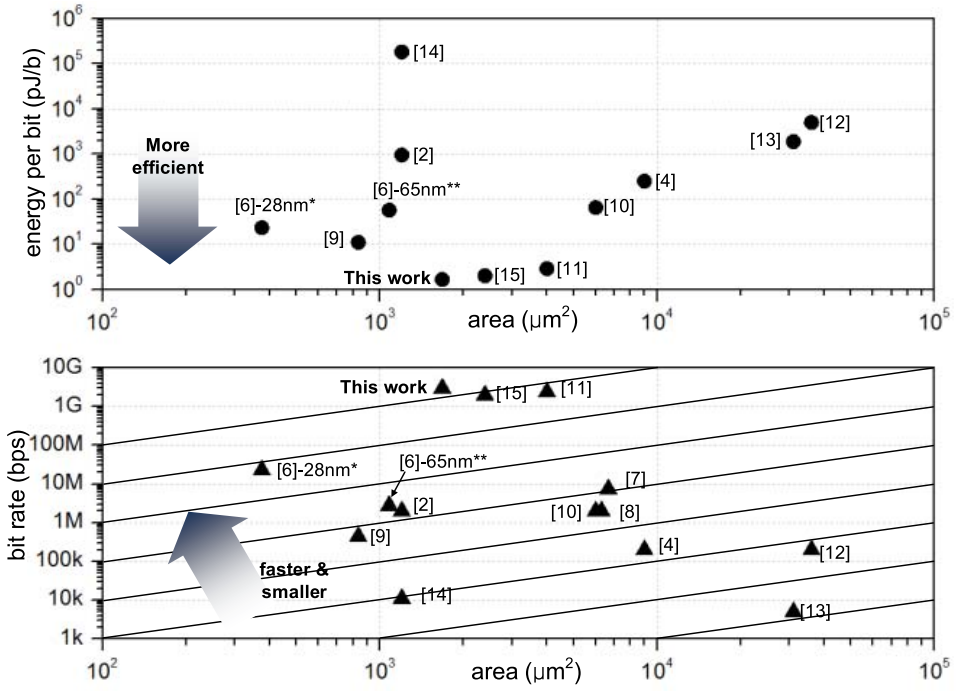


Fig. 11. Simulated noise for V_{SLI_IN} at different corners and frequency range according to the number of samples (N).

frequency domain is equal to f_s/N, where f_s and N are the sampling frequency and the number of samples, respectively. As shown in Fig. 11, the bandwidth of the FFT linearly increases according to N. If N is 100k, the lowest component is 30 kHz, which is less influenced by the *1/f* noise. This is another advantage of reducing the area. The FFT of the measured 100-kb data results shown in Fig. 10 has the same results as those that were explained previously.

We used a well-known statistical method, i.e., the NIST test suite [15], [16], to analyze the extent to which the sampled data is randomized quantitatively. This is the most popular statistical test suite for analyzing a random sequence. Table I shows the NIST test results of the measured output random bit stream of the proposed TRNG. The P-values for all of the NIST tests are higher than the pass criteria. Therefore, the proposed TRNG passes all of the NIST tests.

Table II shows a comparison of the proposed TRNG results with previous works. The bit rate of the proposed TRNG is the highest, whereas the energy per bit is the lowest. Moreover, the TRNG core area is small, even though 65-nm CMOS is not the most advanced process node among [2], [6], and [11]. Therefore, this area can be further reduced. The circuit has a simple architecture and occupies a small area, i.e., 1609 μm^2. In spite of the small size, the proposed TRNG achieves a high data rate of up to 3 Gb/s. The output



* [6]-28nm means 28nm CMOS used TRNG in Ref. [6].
** [6]-65nm means 65nm CMOS used TRNG in Ref. [6].

Fig. 12. Comparisons of energy per bit (top) and for the bit rate versus area (bottom).

TABLE I
MEASURED NIST TEST SUITE RESULTS WITH 100 kb (ALPHA = 0.01)

Test	P-value	Pass/Fail
The Approximate Entropy Test	0.826335	pass
The Linear Complexity Test	0.976849	pass
The Random Excursions Variant Test	0.858946	Pass
Frequency Test within a Block	0.211072	Pass
Tests for the Longest-Run-of-Ones in a Block	0.718945	Pass
The Binary Matrix Rank Test	0.306156	Pass
The Cumulative Sums (Cusums) Test	0.669886	Pass
The Non-overlapping Template Matching Test	0.07879	Pass
The Runs Test	0.561917	Pass
The Discrete Fourier Transform (Spectral) Test	0.847187	Pass
The Overlapping Template Matching Test	0.110434	Pass
The Serial Test	0.766182	Pass
The Frequency (Monobit) Test	0.953749	Pass
The Random Excursions Test	0.573306	Pass
Maurer's "Universal Statistical" Test	0.282568	Pass

TABLE II
COMPARISON AND SUMMARY OF PROPOSED TRNG CIRCUIT MEASUREMENT RESULTS

	This work	JSSC'12 [11]	ISSCC'08 [2]	ISSCC'07 [12]	ISSCC'14 [6]-28nm*
Entropy Source	**Metastability and Jitter**	Metastability	SiN MOSFET	Metastability	Osc. Jitter
Process	**65 nm**	45 nm	0.25 μm	130 nm	28 nm
TRNG Core Area (um^2)	**1609**	4004	1200	36300	375
NIST Pass	**All**	All	-	5	All
bit rate (Mb/s)	**3000**	2400	2	0.2	23.16
Power Consumption (mW)	**5**	7	1.9	1	0.54
Efficiency (pJ/bit)	**1.6**	2.92	950	5000	0.23

* [6]-28nm means 28nm CMOS used TRNG in Ref. [6].

random bit stream is verified by passing all of the NIST test suites. The supply voltage is 1.2 V and power consumption is 5 mW. As a result, the energy per bit is 0.0016 pJ/b. Matsumoto *et al.* [2] showed that there is a reasonable relationship between bit rate and occupied area. For example, to increase the bit rate up to 3 Gbps using the TRNG that was implemented in [2], a 1500× TRNG is required, because its bit rate is 2 Mbps. By using this relationship [2], we can easily compare the TRNGs with the diagonal auxiliary line even when the bit rate is different. We plotted the bit-energy efficiency (pJ/b) against the area and the bit rate (bits per second) against the area, as shown in the top and bottom of Fig. 12, respectively. As shown in the bottom of Fig. 12, the proposed TRNG achieved a superior performance compared with those in other studies. Moreover, the bit efficiency (pJ/b) is also the lowest, as shown in Fig. 12 (top).

IV. CONCLUSION

We proposed a TRNG that uses a common-mode operating comparator and the sampling uncertainty of a DFF with a standard CMOS process. The main features of the proposed TRNG are as follows. First, we utilized both of the randomness sources simultaneously, which resulted in a

better-quality random sequence. Second, we achieved higher thermal noise using standard CMOS technology without the need for a complex noise-control circuit or feedback topology. The thermal noise from the voltage reference was added to the comparator output nodes owing to the common-mode operation. Third, the comparator-biasing problem associated with the common-mode operation was avoided by connecting the comparator inputs together. Finally, by sampling a 100-kb data stream at 3 GHz, we realized *1/f* noise filtering for white noise without the need for filtering components. We fabricated the proposed TRNG using a 65-nm CMOS process, and the output bit stream of the TRNG was measured using a 1.2-V supply voltage. The proposed TRNG dissipates a power of 5 mW including the output driver at 3 Gbps, and the bit energy efficiency is 1.67 pJ/b. Our measurement results showed that all of the NIST test suites were satisfied.

ACKNOWLEDGMENT

The authors would like to acknowledge the multi-project wafer of IC design education center for fabrication.

REFERENCES

[1] M. Drutarovsky and P. Galajda, "A robust chaos-based true random number generator embedded in reconfigurable switched-capacitor hardware," in *Proc. 17th Int. Conf. Radioelektronika*, 2007, pp. 1–6.

[2] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, "1200 μm^2 physical random-number generators based on SiN MOSFET for secure smart-card application," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers*, Feb. 2008, pp. 414–415.

[3] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, May 2000.

[4] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2006, pp. 536–537.

[5] S. Robson, B. Leung, and G. Gong, "Truly random number generator based on a ring oscillator utilizing last passage time," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 12, pp. 937–941, Dec. 2014.

[6] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "A 23 Mb/s 23 pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 280–281.

[7] T. Amaki, M. Hashimoto, and T. Onoye, "A process and temperature tolerant oscillator-based true random number generator with dynamic 0/1 bias correction," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2013, pp. 133–136.

[8] T. Amaki, M. Hashimoto, and T. Onoye, "An oscillator-based true random number generator with jitter amplifier," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 725–728.

[9] K. Yang, D. Blaauw, and D. Sylvester, "A robust −40 to 120 °C all-digital true random number generator in 40 nm CMOS," in *Symp. VLSI Circuits Dig. Papers*, Jun. 2015, pp. C248–C249.

[10] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, and C. H. Kim, "True random number generator circuits based on single- and multi-phase beat frequency detection," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Sep. 2014, pp. 1–4.

[11] S. K. Mathew *et al.*, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[12] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2007, pp. 404–405.

[13] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio, "A 3 μW CMOS true random number generator with adaptive floating-gate offset cancellation," *IEEE J. Solid-State Circuits*, vol. 43, no. 5, pp. 1324–1336, May 2008.

[14] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown," in *Symp. VLSI Circuits Dig. Papers*, Jun. 2011, pp. C216–C217.

[15] V. B. Suresh, D. Antonioli, and W. P. Burleson, "On-chip lightweight implementation of reduced NIST randomness test suite," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2013, pp. 93–98.

[16] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Revision 1a*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Apr. 2010.

Sang-Geun Bae (S'11) was born in Chuncheon, South Korea, in 1984. He received the B.S. and M.S. degrees in electrical and electronic engineering from Kangwon National University, Chuncheon, in 2009 and 2011, respectively. He is currently pursuing the Ph.D. degree with Korea University, Seoul, South Korea.

He was a Visiting Scholar with the University of California at Los Angeles, Los Angeles, CA, USA, in 2012. He has been working on phase-locked loop for frequency synthesizer and spread spectrum clock generator. His current research interests include CMOS-integrated circuits and systems for wired communications.

Yongtae Kim (S'15) was born in Seoul, South Korea, in 1987. He received the B.S. degree in electrical and electronic engineering from Kwangwoon University, Seoul, in 2013, and the M.S. degree in electrical and electronic engineering from Korea University, Seoul, in 2015.

He is currently with the Division of Flash Memory Design, SK-hynix, Icheon, South Korea.

Yunsoo Park (S'14) received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2014, where he is currently pursuing the integrated M.S. and Ph.D. degrees in the area of integrated circuits and systems.

His current research interests include time-interleaved ADC calibration techniques and high-speed ADC designs.

Chulwoo Kim (S'98–M'02–SM'06) received the B.S. and M.S. degrees in electronics engineering from Korea University, Seoul, South Korea, in 1994 and 1996, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Illinois at Urbana–Champaign, IL, USA in 2001.

In 1999, he was an Intern with Design Technology, Intel Corporation, Santa Clara, CA, USA. In 2001, he joined the IBM Microelectronics Division, Austin, TX, USA, where he was involved in cell processor design. Since 2002, he has been with the School of Electrical Engineering, Korea University, where he is currently a Professor. He was a Visiting Professor with the University of California at Los Angeles, CA, USA, in 2008 and with the University of California at Santa Cruz, CA, USA, in 2012. He has co-authored two books, namely, *CMOS Digital Integrated Circuits: Analysis and Design* (McGraw Hill, 4th edition, 2014) and *High-Bandwidth Memory Interface* (Springer, 2013). His current research interests include wireline transceiver, memory, power management, and data converters.

Dr. Kim was a recipient of the Samsung HumanTech Thesis Contest Bronze Award in 1996, the ISLPED Low-Power Design Contest Award in 2001 and 2014, the DAC Student Design Contest Award in 2002, the SRC Inventor Recognition Awards in 2002, the Young Scientist Award from the Ministry of Science and Technology of Korea in 2003, the Seoktop Award for excellence in teaching in 2006 and 2011, the ASP-DAC Best Design Award in 2008, the Special Feature Award in 2014, and the Korea Semiconductor Design Contest: Ministry of Trade, Industry and Energy Award in 2013. He has served on the Technical Program Committee of the IEEE International Solid-State Circuits Conference. He has been a Guest Editor of the IEEE JOURNAL OF SOLID-STATE CIRCUITS. He is currently on the Editorial Board of IEEE TRANSACTIONS ON VLSI SYSTEMS. He was elected as the Distinguished Lecturer of the IEEE Solid-State Circuits Society for 2015–2016.