A 0.72pJ/bit 400μm2 Physical Random Number Generator Utilizing SAR Technique for Secure Implementation on Sensor Nodes

MIKI, Takuji
MIURA, Noriyuki
NAGATA, Makoto

(Citation)
IEICE Transactions on Electronics,E102.C(7):530-537

(Issue Date)
2019-07-01

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/90008117

IEICE TRANS. ELECTRON., VOL.E102–C, NO.7 JULY 2019

PAPER Special Section on Analog Circuits and Their Application Technologies

A 0.72 pJ/bit 400 μm^2 Physical Random Number Generator Utilizing SAR Technique for Secure Implementation on Sensor Nodes

Takuji MIKI[†a)], **Noriyuki MIURA**[†], ***Members, and*** **Makoto NAGATA**[†], ***Senior Member***

SUMMARY This paper presents a low-power small-area-overhead physical random number generator utilizing SAR ADC embedded in sensor SoCs. An unpredictable random bit sequence is produced by an existing comparator in typical SAR ADCs, which results in little area overhead. Unlike the other comparator-based physical random number generator, this proposed technique does not require an offset calibration scheme since SAR binary search algorithm automatically converges the two input voltages of the comparator to balance the differential circuit pair. Although the randomness slightly depends on an quantization error due to sharing AD conversion scheme, the input signal distribution enhances the quality of random number bit sequence which can use for various security countermeasures such as masking techniques. Fabricated in 180 nm CMOS, 1 Mb/s random bit generator achieves high efficiency of 0.72 pJ/bit with only 400 μm^2 area overhead, which occupies less than 0.5% of SAR ADC, while remaining 10-bit AD conversion function.

key words: *hardware security, physical random number, random masking, SAR ADC*

1. Introduction

With the rapid spread of IoT devices, an important physical information acquired at the sensor node is exposed to the risk of leakage and tampering by malicious attackers. Implementing a secure encryption circuit on sensor SoCs is the most effective solution, however, side-channel attack (SCA) reveals the cryptographic key by analyzing power supply nodes [1]. So far, various countermeasure techniques against SCA have been reported. Figure 1 shows the three major techniques to protect sensor data in IoT devices. The first technique is logic masking which randomizes the encryption process by adding random number to the input, and later subtracting it from the output [2]. The second one is secure power converter (DC-DC) technique [3], [4]. It disrupts the correlation between the power supply noise waveform and cryptographic key by switching PWM frequency of DC-DC converters. The third one is for analog information security from side-channel attack via analog components such as analog-to-digital converter (ADC). It is newly emerged security hole [5], [6], however, the random analog masking technique can protects the information leakage [5]. These all techniques require a random number bit sequence. This paper especially focuses on random bit generation used in [5].

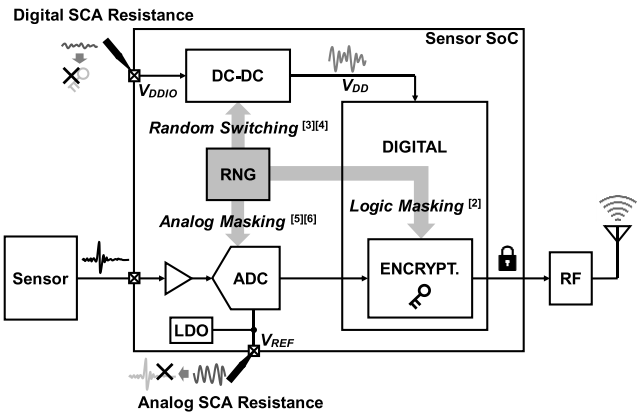

Fig. 1 Security implementation for IoT nodes.

There are various types of random number generators (RNG). Pseudo RNG using linear feedback shift register is the simplest approach, however, it can be predicted and reproduced from outside by attackers. Thus, physical random generator (P-RNG) is indispensable for strong secure implementation, since it potentially create an unpredictable random numbers by extracting entropy from physical phenomena [7]–[11]. A comparator-based P-RNG with noise amplification technique was proposed in [10]. Though it can produce a high quality random number sequence with low power, highly accurate calibration for comparator offset is needed, which causes circuit complexity and operation interruption due to the calibration period. A chaotic-map RNG based on sub-ranging ADC is reported in [11]. This approach requires post-digital processing to realize chaotic randomness, thus, the layout area for RNG becomes enlarged. These techniques can produce a true random number passing all NIST statistical random test [12], however, they sacrifice unignorable layout area. Unlike an encryption-used random number which must guarantee a true-randomness, masking techniques do not always require true random numbers. They only need un-reproducible and high-entropy random numbers for data protection from SCA. Thus, it is more important to make the RNG area as small as possible for silicon cost savings, rather than satisfying true randomness, especially in the sensor SoCs for IoT applications.

In this paper, an area-efficient P-RNG sharing succes-

Manuscript received November 12, 2018.
Manuscript revised February 6, 2019.
[†]The authors are with Kobe University, Kobe-shi, 657–8501 Japan.
a) E-mail: miki@cs26.scitec.kobe-u.ac.jp
DOI: 10.1587/transele.2018CTP0012

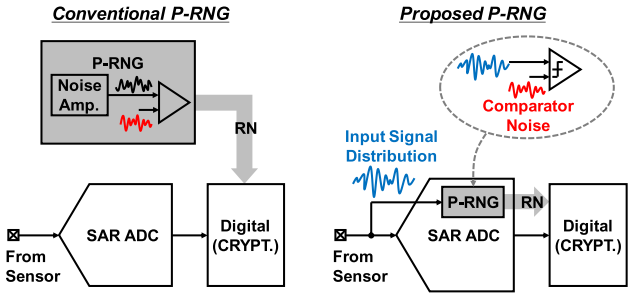

Fig. 2 Concept of the proposed P-RNG.

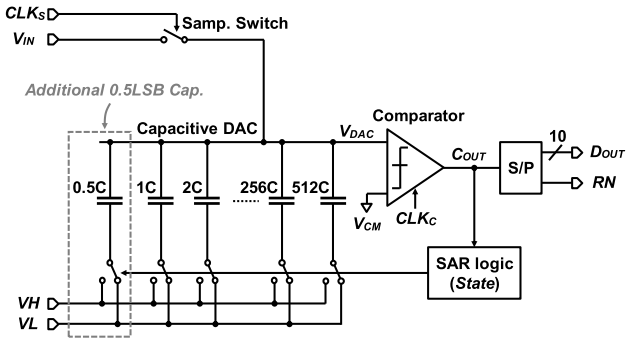

Fig. 3 Physical random number generator based on SAR ADC.

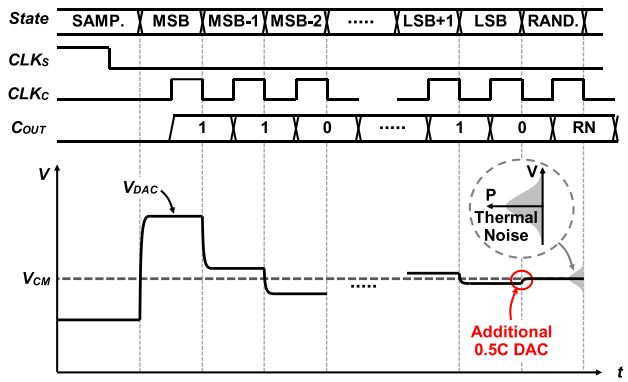

Fig. 4 Random bit generation scheme with binary search operation in SAR ADC.

sive approximation register (SAR) ADC is proposed. It generates random numbers according to the comparator thermal noise after conversion process of SAR ADC. Since SAR binary search operation converges the comparator input voltage to the mean of the noise distribution, the comparator generates random bit without offset calibration. Furthermore, the proposed P-RNG only utilizes a part of the commonly used SAR ADC which is already embedded in the sensor SoC. Thus, the area overhead for realizing P-RNG is significantly small. The proposed P-RNG prototype chip was implemented in 180 nm CMOS and successfully generates random bit sequence. The efficiency of the P-RNG achieves 0.72 pJ/bit with small area overhead of 400 μm^2 which is less than 0.5% of total SAR ADC area.

The rest of the paper is organized as follows. Section 2 will introduce an overall architecture of the proposed P-RNG based on SAR ADC. A simulation study for detailed analysis on the P-RNG behavior will be described in Sect. 3. Section 4 presents a circuit implementation including comparator design. The measurement results of the proposed P-RNG with a 180 nm CMOS prototype chip will be demonstrated in Sect. 5. Finally, Sect. 6 gives the conclusion.

2. Overall Architecture

2.1 Architectural Concept of P-RNG for IoT Sensor SoC

Figure 2 shows a system concept of the proposed P-RNG. In the conventional approach [7]–[10], the dedicated circuits for generating random number *RN* are implemented, which causes an increase in the silicon area. Moreover, the conventional P-RNGs require some noise amplifying circuits to ensure the randomness. On the other hand, the proposed P-RNG reuses some circuit parts of SAR ADC which already exists in widely used sensor SoC. This approach has two advantages. Firstly, the area overhead is extremely small. The P-RNG can output random numbers only by adding a small circuit to typical SAR ADC configuration. The ADC also operates normal digitizing process during random number generation with a slight increase of power consumption and conversion period. The other advantage is to use an input signal distribution. Since the input of the ADC is unknown sensor signal with random noise distribution, pre-processing circuit like noise amplification is not required. Thus, combining the comparator thermal noise, sampling noise and input signal distribution, the highly randomized bit sequence can be created.

2.2 P-RNG Architecture Based on SAR ADC

Figure 3 shows the overall architecture of the proposed P-RNG based on SAR ADC. It is composed by a traditional 10-bit SAR ADC architecture including binary-weighted capacitive digital-to-analog converter (C-DAC), comparator, sampling switch, SAR control logic and serial parallel converter circuit. Top-plate sampling architecture is adopted to eliminate sample and hold phase. The input voltage V_{IN} is sampled on C-DAC via the sampling switch at the edge of CLK_S controlled by the state machine in SAR logic. After sampling the input signal, the state moves to binary search phase as shown in Fig. 4. The output voltage of C-DAC, V_{DAC}, is generated by charge redistribution technique by charging or discharging the bottom plate of the C-DAC from reference voltage *VH* and *VL*, according to the decision of the comparator C_{OUT}. By comparing the V_{DAC} and common voltage V_{CM} from MSB to LSB, the input voltage is quantized to 10-bit digital data D_{OUT}. After finishing the LSB decision, the V_{DAC} is intentionally moved to be very close to V_{CM} by using 0.5 C capacitance which is added to the C-DAC. In the result, the two input voltages of the com-

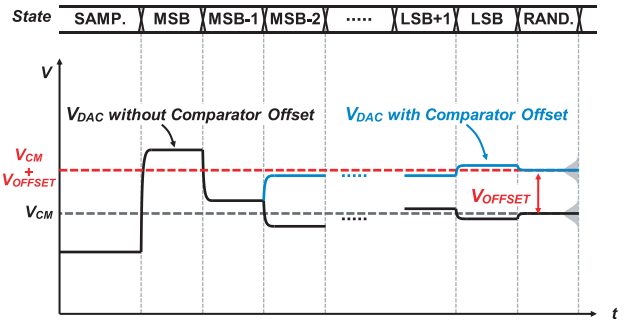

Fig. 5 Convergence procedure with comparator offset.

parator are almost the same voltage after LSB judgement as shown in Fig. 4. Thus, one more comparison at the additional phase leads to metastable output from the comparator. This metastable output *RN* follows the comparator noise distribution derived from the resistive thermal noise, which results in physically random number generation.

The proposed P-RNG scheme can effectively generate random numbers even with comparator offset error. The comparator offset is caused by mismatches of differential pairs in pre-amplifier and latch circuits. The conventional comparator-based P-RNG technique requires offset calibration by adjusting output load of the comparator [10]. Since high resolution alignment is needed for the calibration, additional adjustment components cause circuit complexity and an increase in parasitic elements. The increase of output load induces not only transient response degradation but also noise reduction, thus another noise amplification block has to be added. However, the binary search algorithm in the proposed P-RNG scheme automatically converges the V_{DAC} to the mean of the comparator noise, $V_{CM} + V_{OFFSET}$, as shown in Fig. 5. Thus, the comparator outputs physical random numbers after LSB decision and 0.5 LSB shift of V_{DAC} without any offset calibration.

3. Simulation Study

Figure 6 shows the simulation model of the proposed P-RNG. Single-ended model is considered for simplicity, however, it can be also applied to differential structure as the same approach. The random numbers are generated by utilizing metastability of comparator due to the thermal noise. In this model, the comparator noise V_{N_CMP} is injected to the comparison target node as an input referred noise. SAR ADC operation is represented as AD and DA conversion, and the C-DAC output voltage V_{DAC} after final comparison for LSB decision is expressed by subtracting quantized value from the input value. This indicates the quantization error of SAR ADC, and causes the comparator input voltage shift from the mean value of the V_{N_CMP} distribution. Thus, the quality of randomness are degraded by the quantization error. Sampling noise V_{N_SMP}, which is injected at the sampling phase and its value is calculated as kT/C where C is total sampling capacitance, can randomize the quantization error. However the mean of the input voltage distribution V_{CM_IN} averagely remains as the quantization error since the sampling noise is normally distributed. To suppress the quantization error, increasing a resolution of ADC is one solution. Thus, the 0.5 C capacitor is added to the C-DAC in the proposed P-RNG. Figure 7 shows the simulation results of averaging of random number *RN* whose values are "1" or "0". When the V_{CM_IN} is 0, which means no quantization error, the occurrence probability of "1" is approximately 50%, resulting in high quality randomness. However, a large quantization error caused by the coarse SAR ADC without 0.5 C capacitance induces a large difference from ideal occurrence of 50% as shown in dot line of the figures. By increasing the ADC resolution with 0.5 C capacitance and reducing the quantization error, the mean value errors of random numbers can be suppressed as shown in the solid line of the figure. This simulation results also show the effect of a randomness improvement depending on the amount of comparator noise. Too small comparator noise of $\sigma = 0.2$ LSB is slightly worse than typically used noise value of $\sigma = 0.3$ LSB in terms of randomness as shown by the gray line in Fig. 7. This is because the wide range of noise distribution can cover the shift of comparator input voltage. However, too large comparator noise more than 0.3 LSB reduces a signal to noise ratio (SNR) and degrades the performance of ADC. In this work, the SNR

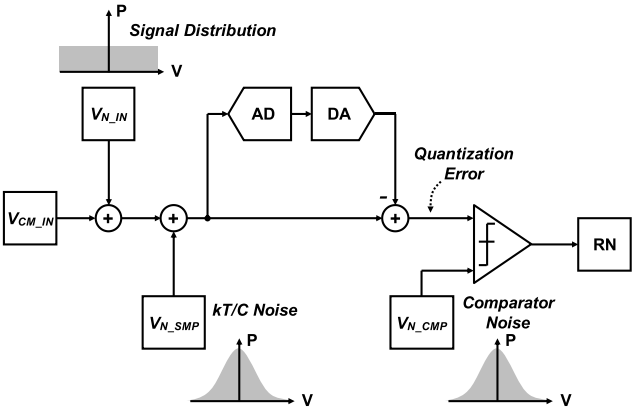

Fig. 6 Simulation model of the proposed P-RNG.

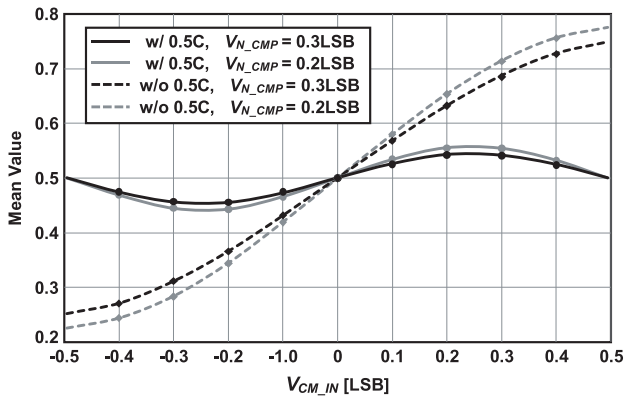

Fig. 7 Simulated mean value of RN versus quantization error of ADC.

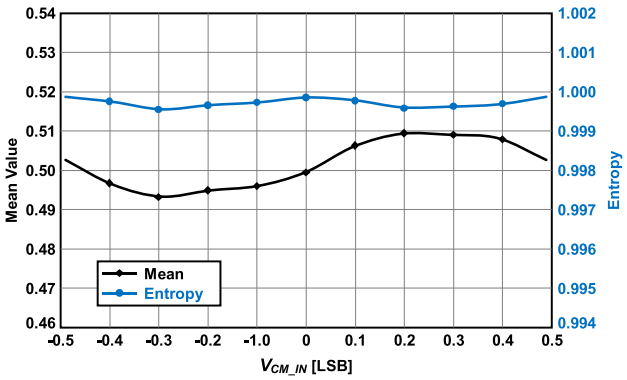

Fig. 8 Simulated mean value and entropy with input signal distribution.

of SAR ADC decreases by about 1.5 dB as the comparator noise rises from 0.2 LSB to 0.3 LSB.

To enhance the quality of randomness, input signal distribution can be used in the proposed SAR ADC-shared P-RNG architecture. Since the ADC digitizes an application specific signal, the input voltage is randomly varies. In the simulation model, the noise with normal or uniform distribution V_{N_IN} is injected to the input signal as shown in Fig. 6. The noise randomizes the mean value of input signal V_{CM_IN}, thus, the randomness dependency on the quantization error is drastically reduced. In the result, the occurrence probability of random bit "1" and "0" is almost 50% over the entire range of quantization noise as shown in the simulation results of Fig. 8. This simulation results is a case of P-RNG model with 0.5 C capacitance, 0.3 LSB comparator noise and normally distributed input noise. The randomness is evaluated using entropy value defined as follows,

$$H(X) = -\sum_{i=1}^{N} P_i \log P_i \tag{1}$$

where P_1 and P_2 are the probabilities of occurrence of "1" and "0", respectively, in random number sequence X. The P-RNG model achieves high entropy with nearly equal to 1 as shown in Fig. 8, which indicates a high-quality randomness passing some sub-tests of NIST true random test.

4. Circuit Implementation

The proposed P-RNG is assumed to be embedded in SAR ADC for sensor front-end. Thus, the target specifications are 10-bit 1 MS/s, which are not so high performance and can be applied to various sensor applications. Since the P-RNG works on IoT nodes with limited power source and space, silicon area and power consumption of P-RNG should be suppressed. To save ADC power consumption, split-type capacitor technique is employed to save switching energy of C-DAC [13]. SAR control logic is composed of synchronized architecture for slow speed and low power operation. Clock signal with a frequency of 12 MHz is externally input to SAR control logic and generates 1 MHz sampling timing clock CLK_S and comparison clock CLK_C for 10-bit quantization and random number generation.

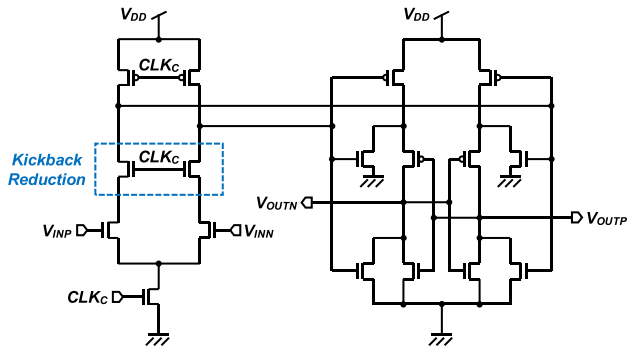

Fig. 9 Circuit schematic of comparator.

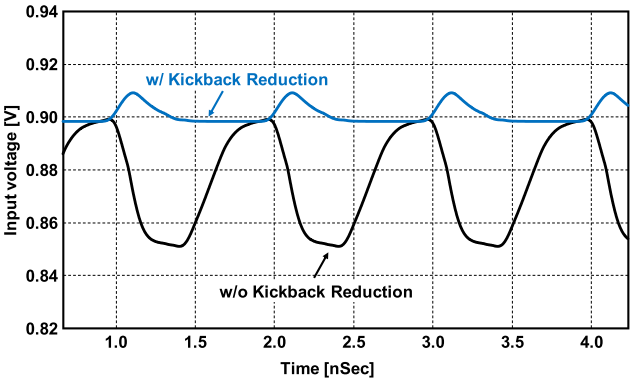

Fig. 10 Simulated waveform of comparator input voltage.

The circuit schematic of comparator is depicted in Fig. 9. To realize low power operation with no continuous current, double-tail latch type comparator is employed [14], [15]. Since the randomness of the proposed P-RNG is not influenced by comparator offset, additional adjustment circuits to align the balance of differential pair and offset calibration sequence are not needed. If the ADC offset error affects some system errors, it can be calibrated after conversion in digital domain. In general SAR ADC, comparator kickback does not cause much problem since the voltage variation of comparator input node is limited owing to a large input capacitance and sufficient settling time. However, considering that the comparator is shared for random number generation, the signal-dependent kickback error should be suppressed to avoid quality degradation of randomness. Thus, two cascade switch transistors are inserted between input transistors and latch enabling pass for kickback reduction [16]. It suppresses the voltage variation at drain node of the input transistors, which results in the reduction of the voltage shift on the comparator input node as shown in Fig. 10. This technique unfortunately increases thermal noise of comparator due to additional switches. However, as described in Sect. 3, comparator thermal noise contributes to enhance the quality of randomness, and 0.3 LSB of noise sigma is an optimal value. In a low speed and medium resolution sensor frontend SAR ADC, comparator circuit can be easily designed with low noise because of slow speed operation as shown in black line

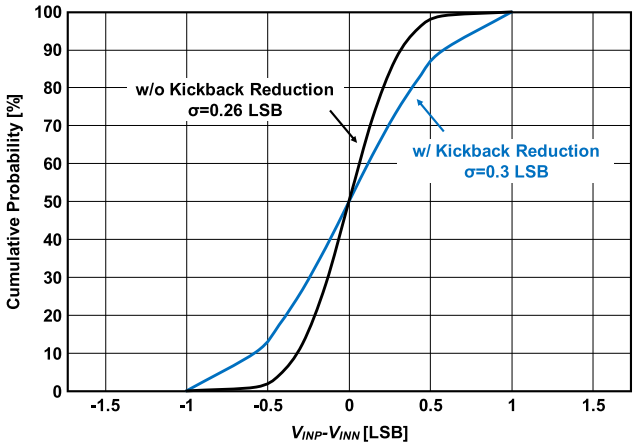

Fig. 11 Simulated noise value of the comparator.

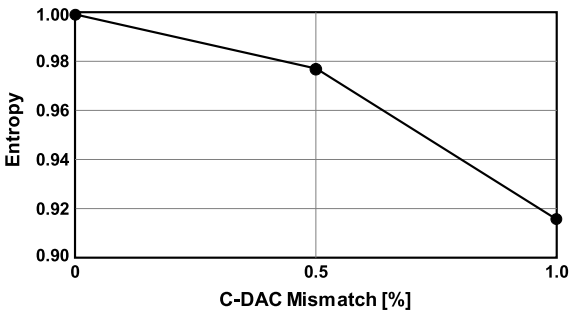

Fig. 12 Simulated entropy with non-linear error of SAR ADC.

of Fig. 11. Then, the cascade switch transistors for kickback reduction can be applied to such comparators and the noise distribution is increased from 0.26 LSB to 0.3 LSB as shown in blue line of Fig. 11.

Non-linear error of SAR ADC due to C-DAC mismatch as well as comparator kickback should be suppressed to generate high quality random numbers. Figure 12 shows the simulated entropy values with non-linear error of SAR ADC. C-DAC mismatch causes SAR binary search error, resulting in degradation of INL/DNL. It also induces the convergent voltage V_{DAC} after LSB decision to be outside of the comparator noise distribution range, which is equivalent to an increase of quantization error. Thus, the randomness of the P-RNG output is degraded by non-linearity of SAR ADC as shown in the simulation result of Fig. 12.

5. Measurement Results

The test chip of the P-RNG based on SAR ADC was fabricated in 180 nm digital CMOS process. Figure 13 shows the chip microphotograph. The C-DAC is formed by MIM capacitance. To enhance the quality of randomness of the P-RNG, only 0.5 C capacitors and associate digital circuits are added to the 10-bit 1 MS/s SAR ADC. The total area overhead is only 400 μm^2 which is approximately 0.5% of total SAR ADC area.

Figure 14 shows the measured waveforms of random

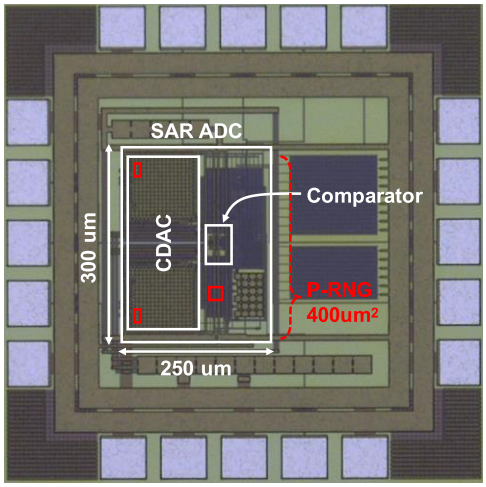

Fig. 13 Die photo.

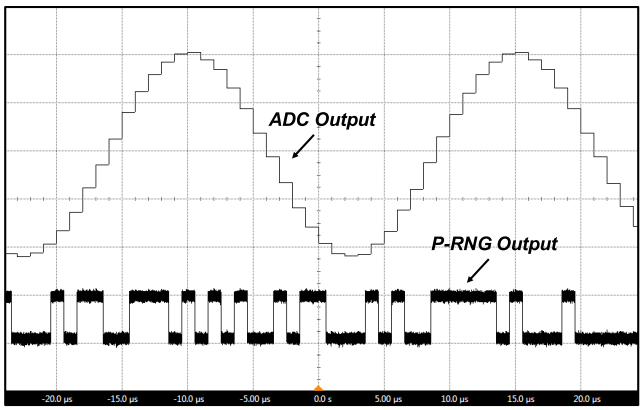

Fig. 14 Measured waveforms of P-RNG and ADC output.

Table 1 NIST test result.

NIST TEST	P-value	Result
Frequency	0.162606	Pass
Block Frequency	0.213309	Pass
Cumulative Sums	0.122325	Pass
Runs	0.048716	Pass
Longest Runs of 1's	0.000089	Fail
Rank	0.739918	Pass
FFT	0.637119	Pass
Non-overlapping Template	0.000439	Fail
Overlapping Template	0.000001	Fail
Universal	0.809199	Pass
Approximate Entropy	0.000413	Fail
Random Excursions	0.000000	Fail
Random Excursions Variant	0.000000	Fail
Serial	0.739918	Pass
Linear Complexity	0.350485	Pass

number of the P-RNG output when SAR ADC normally digitizes sine wave analog input signal. The proposed P-RNG can generate 1/0 random numbers of almost equal occurrence probability with no calibration for comparator offset.

The randomness of the P-RNG output was evaluated by using NIST 800-22 test [12]. Table 1 shows all subtest results with 1M samples of the P-RNG output. In general, a subtest is passed when the P-value is more than 0.01, and

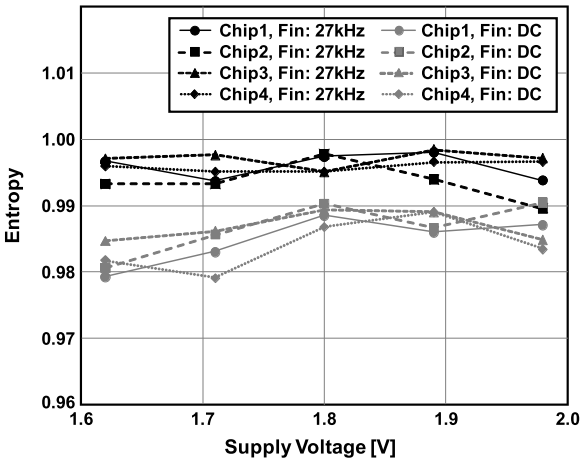

Fig. 15 Measured entropy versus supply voltage variation with input signal.

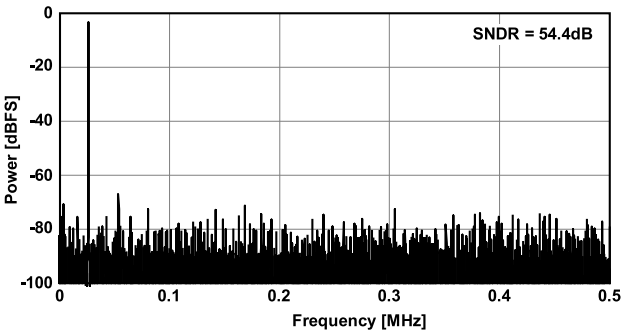

Fig. 16 Measured FFT spectrum of SAR ADC.

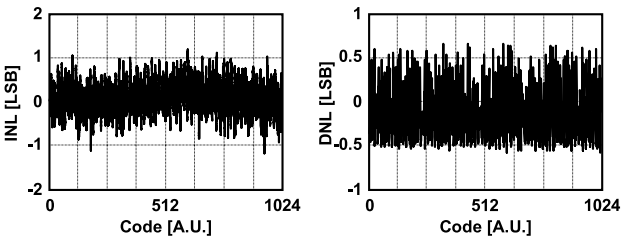

Fig. 17 Measured INL and DNL.

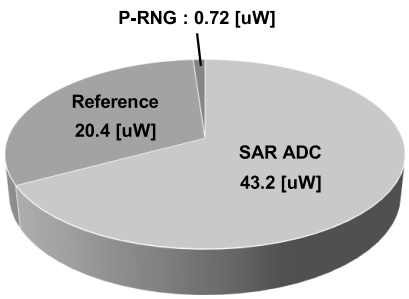

Fig. 18 Power consumption.

if all subtest are passed, the random numbers is certified as a true random number which can be used for encryption. However, the proposed P-RNG failed some subtests. This is because the random distribution is partially distracted by non-linear quantization error due to C-DAC mismatch and the other external non-ideality factors such as power supply noise. Thus, this P-RNG does not generate "true" random numbers, but high quality random numbers passing 9/15 of NIST tests, which is enough for secure random masking.

Figure 15 shows the measured entropy versus supply voltage variation. The supply voltage is 1.8 V in typical condition and assumed to +/− 10% voltage variation. Four chips are measured to evaluate whether the randomness is maintained against chip variation. The entropy values were measured with 1M samples while giving 1 Vpp 27 kHz sinusoid signal and DC voltage to the input of SAR ADC. When applying DC voltage, the randomness is determined by comparator noise and kT/C noise. These values are defined at the circuit design strategy. In this work, comparator noise and sampling capacitor values are 0.3 LSB and 2 pF, respectively. The entropy values at DC input are slightly lower than the case of sinusoid input but still high enough. Thus, the random number can be used for masking even when the slow signal is input to the IoT sensor node such as temperature and humidity. By giving the sinusoid signal to the ADC, input distribution enhances the randomness, which leads to achieve high entropy values with nearly equal to 1 during the supply voltage range and across the multiple-chip.

Figure 16 shows the FFT spectrum of the SAR ADC at the sampling frequency of 1 MHz. The ADC successfully achieves 54.4 dB SNDR at 30 kHz input signal. The measured INL and DNL are within +/− 1.2 LSB and +/− 0.6 LSB, respectively, as shown in Fig. 17. These results indicate the proposed P-RNG architecture shared with SAR ADC can achieve both high quality random number generation and AD conversion function. Figure 18 shows power consumption breakdown of the SAR ADC and the P-RNG. Total power consumption of SAR ADC including comparator and digital control logic is 43.2 μW. The reference voltage for SAR ADC is isolated from analog power supply voltage and consumes 20.4 μW. The power consumption of the P-RNG is only 0.72 μW including one more comparison, C-DAC operation after LSB decision and associated digital circuit operation.

Table 2 shows the performance summary and comparison. The chaotic-map random generator [11] and this work generate both random numbers and AD conversion data simultaneously, then, most circuit components can be shared among RNG and ADC. Thus, in the area section of these technique, only area overhead for RNG is displayed in Table 2. The other techniques [8]–[10] require the dedicated area for generating random numbers. From the comparison table, the proposed P-RNG shows the smallest area of 400 μm^2. Moreover it requires no calibration scheme for comparator offset which might cause complex control. Although the proposed P-RNG is a little bit insufficient to the true randomness, it can generate high entropy random numbers which is valid for secure masking technique.

Table 2 Performance comparison.

	ISSCC'08 [8]	ASSCC'09 [9]	ASSCC'14 [10]	ESSCIRC'16 [11]	This Work
Process [um]	0.25	0.18	0.04	0.18	0.18
Entropy Source	Meta-stability	Oscillator Jitter	Meta-stability	Chaotic-Map	Meta-stability
Bit Rate [Mb/s]	2	0.04	0.5	0.27	1
Power [uW]	1900	1.04	0.214	0.082	0.72
FoM [pJ/bit]	950	26	0.43	0.3	0.72
Area [um^2]	1200	50000	1400	4500	400
Random Test	FIPS140-2 PASS	FIPS140-2 80% PASS	NIST PASS	NIST PASS	NIST 9/15 PASS
Purpose	Secure Smart Card	RFID	Crypto-graphy	Crypto-graphy	Masking

6. Conclusion

In this paper, an area-efficient P-RNG is proposed. As an entropy source, comparator metastability is used to realize unrepeatable randomness. The comparator is shared with SAR ADC which already exists in analog frontend circuit of sensor SoCs. Thus the required circuits for P-RNG is only to enhance the quality of randomness, resulting in quite small area overhead. Owing to the binary search scheme of SAR ADC, offset calibration-free comparator-based P-RNG is realized. Simulation study reveals optimal noise source in SAR ADC and random number generation mechanism utilizing signal distribution. The comparator is designed for both signal-dependent kickback error reduction and appropriate noise distribution. The prototype P-RNG implemented in 180 nm CMOS demonstrates random number generation while operating 1 MS/s 10 bit ADC function. The power consumption of the P-RNG is 0.72 μW which is good energy efficiency of 0.72 pJ/bit. Though the proposed P-RNG is less than true random number quality, high entropy randomness is achieved across 10% supply voltage variation with ultra small layout area overhead of 400 μm^2.

Acknowledgments

This paper is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

References

[1] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," CRYPTO 1996: Advances in Cryptology — CRYPTO '96, Lecture Notes in Computer Science, vol.1109, pp.104–113, Springer, Berlin, Heidelberg, Aug. 1996.

[2] S. Chari, C.S. Jutla, J.R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," CRYPTO 1999: Advances in Cryptology — CRYPTO '99, Lecture Notes in Computer Science, vol.1666, pp.398–412, Springer, Berlin, Heidelberg, 1999.

[3] M. Kar, A. Singh, S.K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," IEEE J. Solid-State Circuits, vol.53, no.8, pp.2399–2414, Aug. 2018.

[4] W.-H. Yang, L.-C. Chu, S.-H. Yang, Y.-J. Lai, S.-Q. Chen, K.-H. Chen, Y.-H. Lin, S.-R. Lin, and T.-Y. Tsai, "An enhanced-security buck DC-DC converter with true-random-number-based pseudo hysteresis controller for Internet-of-Everything (IoE) devices," IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, pp.126–127, Feb. 2018.

[5] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, "A random interrupt dithering SAR technique for secure ADC against reference-charge side-channel attack," submitted to IEEE Trans. Circuits Syst. II, Exp. Briefs.

[6] V.V. Gadde, H. Awano, and M. Ikeda, "An encryption-authentication unfiled A/D conversion scheme for IoT sensor nodes," Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), pp.123–126, Nov. 2018.

[7] S.K. Mathew, S. Srinivasan, M.A. Anders, H. Kaul, S.K. Hsu, F. Sheikh, A. Agarwal, S. Satparthy, and R.K. Krishnamurthy, "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.

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

[9] W. Chen, W. Che, Z. Bi, J. Wang, N. Yan, X. Tan, J. Wang, H. Min, and J. Tan, "A 1.04 μW truly random number generator for Gen2 RFID tag," Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), pp.117–120, Nov. 2009.

[10] T.-K. Kuan, Y.-H. Chiang, and S.-I. Liu, "A 0.43pJ/bit true random number generator," Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), pp.33–36, Nov. 2014.

[11] M. Kim, U. Ha, Y. Lee, K. Lee, and H.-J. Yoo, "A 82nW chaotic-map true random number generator based on sub-ranging SAR ADC," Proc. IEEE Eur. Solid-State Circuits Conf. (ESSCIRC), pp.157–160, Sept. 2016.

[12] "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," National Inst. Standards and Technology, Pub. 800-22, 2001.

[13] B.P. Ginsburg and A.P. Chandrakasan, "500-MS/s 5-bit ADC in 65-nm CMOS with split capacitor array DAC," IEEE J. Solid-Sate Circuits, vol.42, no.4, pp.739–747, April 2007.

[14] D. Schinkel, E. Mensink, E. Klumperink, E. van Tuijl, and B. Nauta, "A double-tail latch-type voltage sense amplifier with 18ps setup+hold time," IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, pp.314–315, Feb. 2007.

[15] M. Miyahara, Y. Asada, D. Paik, and A. Matsuzawa, "A low-noise self-calibrating dynamic comparator for high-speed ADCs," Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), pp.269–272, Nov. 2008.

[16] D. Paik, Y. Asada, M. Miyahara, and A. Matsuzawa, "An 8-bit 600-MSps flash ADC using interpolating and background self-calibrating techniques," IEICE Trans. Fundamentals, vol.E93-A, no.2, pp.402–414, Feb. 2010.

Takuji Miki received the B.S. and M.S. degrees from Ritsumeikan University, Kyoto, Japan, in 2004 and 2006, respectively, and the Ph.D. degree from Kobe University, Kobe, Japan, in 2017. From 2006 to 2016, he was with Panasonic Corporation, Osaka, Japan, where he was involved in the development of high performance analog and mixed-signal integrated circuits for consumer and industrial applications. He is currently a Project Associate Professor with the graduate school of science, technology and innovation, Kobe University. His current research interests include data converters, sensor interface and hardware security.

Noriyuki Miura received the B.S., M.S., and Ph.D. degrees in electrical engineering all from Keio University, Yokohama, Japan. From 2005 to 2008, he was a JSPS Research Fellow and since 2007 an Assistant Professor with Keio University, where he developed wireless interconnect technology for 3D integration. He is currently an Associate Professor with Kobe University, Kobe, Japan, and concurrently a JST PRESTO researcher, working on hardware security and next-generation heterogeneous computing system. Dr. Miura is currently serving as a Technical Program Committee (TPC) Member for A-SSCC and Symposium on VLSI Circuits. He served as the TPC Vice Chair of 2015 A-SSCC. He was a recipient of the Top ISSCC Paper Contributors 2004–2013, the IACR CHES Best Paper Award in 2014, the IEICE Suematsu Yasuharu Award in 2017, and the Marubun Research Encouragement Award in 2019.

Makoto Nagata received the B.S. and M.S. degrees in physics from Gakushuin University, Tokyo, in 1991 and 1993, respectively, and the Ph.D. in electronics engineering from Hiroshima University, Hiroshima, in 2001. He was a research associate at Hiroshima University from 1994 to 2002, an associate professor of Kobe University from 2002 to 2009, and then promoted to a full professor in 2009. He is currently a professor of the graduate school of science, technology and innovation, Kobe University, Kobe, Japan. He is a senior member of IEEE and IEICE. His research interests include design techniques toward high performance mixed analog, RF, and digital VLSI systems with particular emphasis on power/signal/substrate integrity and electromagnetic compatibility, testing and diagnosis, advanced packaging, as well as their applications for hardware security and safety. He was a co-recipient of the best paper awards from IEEE 3D-Test 2013, IACR CHES 2014, and IEEE APEMC 2015. Dr. Nagata has been a member of a variety of technical program committees of international conferences such as the Symposium on VLSI Circuits (2002–2009), Custom Integrated Circuits Conference (2007–2009), Asian Solid-State Circuits Conference (2005–2009), International Solid-State Circuits Conference (2014–2017), and many others. He is chairing Technology Directions subcommittee for International Solid-State Circuits Conference (2018–). He served as a technical program chair (2010–2011) and symposium chair (2012–2013) for Symposium on VLSI circuits and a chapter chair for IEEE SSCS Kansai Chapter (2017–2018). He is currently an associate editor for IEEE Transactions on VLSI Systems (2015–), and served as an associate editor of the IEICE Transactions on Electronics (2002–2005).