Evaluation of Latch-based Physical Random Number Generator Implementation on 40 nm ASICs

Naoya Torii
Fujitsu Laboratories Ltd.
1-1 Kamikodanaka 4-chome
Nakahara-ku,
Kawasaki 211-8588 JAPAN
torii.naoya@jp.fujitsu.com

Dai Yamamoto
Fujitsu Laboratories Ltd.
1-1 Kamikodanaka 4-chome
Nakahara-ku,
Kawasaki 211-8588 JAPAN
yamamoto.dai@jp.fujitsu.com

Tsutomu Matsumoto
Yokohama National University
79-1 Tokiwadai, Hodogaya-ku,
Yokohama 240-8501 JAPAN
tsutomu@ynu.ac.jp

ABSTRACT

In the age of the IoT (Internet of Things), a random number generator plays an important role of generating encryption keys and authenticating a piece of an embedded equipment. The random numbers are required to be uniformly distributed statistically and unpredictable. To satisfy the requirements, a physical true random number generator (TRNG) is used. In this paper, we implement a TRNG using an SR latch on 40 nm CMOS ASIC. This TRNG generates the random number by exclusive ORing (XORing) the outputs of 256 SR latches. We evaluate the random number generated using statistical tests in accordance with BSI AIS 20/31 and using an IID (Independent and Identically Distributed) test, and the entropy estimation in accordance with NIST SP800-90B changing the supply voltage and environmental temperature within its rated values. As a result, the TRNG passed all the tests except in a few cases. From this experiment, we found that the TRNG has a robustness against environmental change. The power consumption is 18.8 μW at 2.5 MHz. This TRNG is suitable for embedded systems to improve security in IoT systems.

Keywords

Physical true random number generator; TRNG; SR latch; metastability; AIS20/30; SP800-90B

1. INTRODUCTION

The security of embedded equipment is important for the IoT system. In this paper, we implemented a physical true random number generator (TRNG) suitable for the embedded equipment.

The requirements for TRNGs in embedded equipment is considered as follows:

- Generating random numbers having high entropy,
- Small circuit size and low power consumption, and
- Resistant to environmental changes, such as changes in temperature and voltage.

Recently the basic configuration of TRNGs has been considered to be as shown in Figure 1 [14, 28]. TRNGs consist of the entropy source circuit, the health circuit, and the conditioning circuit. The entropy source circuit generates raw random numbers. The conditioning circuit reduces the bias of the raw random numbers and increases the entropy by compressing them. If the entropy source circuit generates raw random numbers with enough entropy, the conditioning circuit need not be equipped. The health circuit detects the failure of the raw random numbers and outputs an alarm signal steadily or when needed.

In this paper, we did not implement the health circuit, because the purpose was to evaluate the entropy source. We call the entropy source as the TRNG and the raw random number as the random number for simplicity.

Previous Work. Various types of TRNGs are proposed. We divide them into three types. The first type uses a noise from an analog circuit, such as a thermal noise from a resister, as an entropy source [20, 5, 4, 18]. The noise is amplified and transformed into a digital signal. A TRNG of this type is high-throughput, however, it requires a high gain amplifier and a high power consumption.

The second type uses a clock jitter. A high-speed clock jitter is sampled by a slower clock [6, 24, 7, 22, 16, 1]; for example, TRNG using ring oscillators (ROs). A RO is an oscillation circuit where an odd number of NOT gates is used to form a loop. A TRNG of this type is robust against temperature change; however, it requires many ROs to generate high entropy random numbers, hence the power consumption and circuit size increase.

The third type uses the metastability of a circuit [10, 26, 13, 12, 17]. For example, a TRNG uses SRAM data at power-on [12], inverter ring outputs using two NOT gates

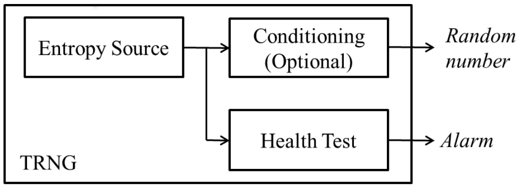

Figure 1: Block diagram of TRNG

TrustED'16, October 28 2016, Vienna, Austria
© 2016 ACM. ISBN 978-1-4503-4567-5/16/10. . . $15.00
DOI: http://dx.doi.org/10.1145/2995289.2995292

[17], and SR latches [26, 13]. This type of TRNG requires uniform characteristics of its elements and wiring. However, it is difficult to realize uniform characteristics. Therefore, a feedback circuit is required to generate high entropy random numbers. Some feedback circuits are proposed to change the characteristics of latch circuits to generate random numbers by watching the output sequence [26, 13]. With these circuits, one latch circuit generates high entropy random number; however, it requires relatively complicated feedback circuits.

A type of TRNG not using feedback circuits is proposed [10, 29]. Hata and Ichikawa proposed a TRNG using SR latches [10]. This TRNG was implemented on a field programmable gate array (FPGA), which XORs 64 SR latches and retrieves the output using D flip-flop (D-FF). The outputs passed NIST SP800-22 statistical tests [3]. In this paper we call this TRNG as SR-TRNG. Varchola and Drutarovskya proposed a structure called TERO (Transition Effect Ring Oscillator) and implemented it on an FPGA [29]. The TERO retrieves the entropy using oscillatory metastable operation. A TRNG was implemented by the XOR of two TERO outputs on an FPGA, and the output sequences passed NIST800-22 tests. The TERO structure does not require feedback circuits and is expected to be efficiently fabricated on CMOS. Haddad et al. validated the stochastic model of TERO by 28 nm CMOS implementation [9]. However, the hardware size and the throughput were not reported.

In our previous work, we implemented an SR-TRNG on a 0.18 μm CMOS process ASIC (Application Specific Integrated Circuit) and evaluated it by statistical tests in accordance with NIST SP800-90B (first draft) [2] and BSI AIS20/31 [14]. These statistical tests are for TRNGs. In addition, we evaluated it by changing the temperature and the power voltage in the range of rated values. From this evaluation, our SR-TRNG on a 0.18 μm CMOS generated high entropy random numbers when the environments changed [15][27]. However, we did not evaluated the latch-based TRNG when the CMOS process changed.

Contribution. In this paper, we fabricated an SR-TRNG in a 40 nm CMOS process and evaluated the power consumption. In addition, we evaluated the randomness of the output sequences using AIS20/31 and SP800-90B, first and second draft (the latest draft) [28], when the temperature and voltage changed in the range of rated values. As a result, we found that this SR-TRNG generates high entropy random numbers. In addition, we discuss the difference between SR-TRNG on a 0.18 μm process and that on a 40 nm process. We found that the number of random latches (see section 2) decrease by the process miniaturization and the reason is discussed. As a result, we consider that our SR-TRNG generates high entropy random numbers and is robust against environmental fluctuation if the CMOS process changes.

Organization. This paper is organized as follows. In section 2, we describe the SR-TRNG. In section 3, we describe the implementation of an SR-TRNG on a 40 nm CMOS. In section 4, we describe the evaluation results by the statistical tests in accordance with AIS20/31 and the IID test, and the entropy estimation in accordance with SP800-90B (second draft). In section 5, we describe the evaluation of the number of latches per chip which generates random numbers and the quality of its randomness. In section 6, we discuss the difference with an SR-TRNG implemented on a 0.18 μm CMOS process. Finally, we conclude this paper.

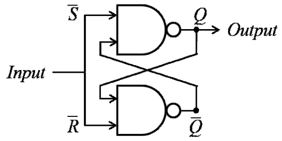

Figure 2: SR latch using NAND gates

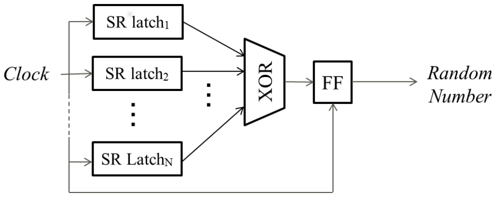

Figure 3: SR-TRNG

2. TRNG USING SR LATCHES

The SR-TRNG proposed by Hata and Ichikawa is described [10]. It uses the metastability of the SR latches as an entropy source. In general, an SR latch is uses to hold bit information. In this paper, an *Input* signal is inputted to both inputs of an SR latch as shown in Figure 2. When *Input* = 0, the SR latch is stable with *Output* = 1. When *Input* changes from 0 to 1, the SR latch temporarily enters a metastable state, and it is stable with *Output* = 0 or 1. Ideally, the probability of getting the output 0 or 1 is the same. However, the output value of the SR latch is skewed because the drive capability and the wiring length between NAND gates are not identical. Hence, if a series of rising edges (= clock signal) is inputted, the output value is one of three sequences: all 0, all 1, or a mixture of 0 or 1 (random sequence). In this paper, the SR latch to generate all 0 or all 1 is called a constant latch, and that to generate a random sequence is called a random latch.

An SR-TRNG generates a random number by XORing many SR latches and sampling with fiip-flop as shown in Figure 3. Hata and Ichikawa reported that SR-TRNG was implemented by XORing 64 latches on FPFA and passed NIST SP800-22 statistical tests [10]. This SR-TRNG is implemented by synchronous digital circuits; therefore, the design cost can be reduced. In addition, the random number generation is stopped if the clock stops inputting. Therefore, the power consumption can be reduced.

We consider SR-TRNG is suitable for IoT equipment. To confirm the suitability, we fabricated an SR-TRNG on a 40 nm CMOS process and evaluated power consumption and hardware size. In addition, we also evaluated the random number by statistical tests when the temperature and supply voltage changed within the range of rated values. We compared the evaluation result with that of an SR-TRNG on a 0.18 μm CMOS process which was fabricated in our previous work.

3. ASIC IMPLEMENTATION

We fabricated an SR-TRNG chip on a 40 nm CMOS process and evaluated four chips. The rated voltage was $1.1V \pm 10\%$. The prototype chip generated a random number by XORing 256 SR latch outputs when the clock was inputted. The circuit design was the same as that in the 0.18 μm process [15, 27]. The SR latch was designed manually to be a random latch; that is, the same type of NAND gate was selected and the wiring between NAND gates were symmetrical and their length was equal. The other circuits were automatically wired.

A block diagram of the prototype chip is shown in Figure 4. The outputs of 256 SR latches were XORed and outputted random numbers. A 2 to 1 multiplexer (2-1 MUL) and a 256 to 1 multiplexer (256-1 MUL) were used for evaluation. By controlling these multiplexers, the output could be selected whether the random number was generated by XORing 256 latches or one of the 256 latches.

We measured the power consumption of the prototype chip and it was 18.8 μW at 2.5 MHz (corresponding value). We also evaluated the hardware size. This SR-TRNG consisted of 256 SR latches, XOR gates which were 256 bit inputs to 1 bit output, and one D-FF. The hardware size was evaluated as 984.3 gates.

4. RANDOMNESS EVALUATION

In this section, we evaluate whether the prototype chip generates the high entropy random number when the temperature and voltage change.

4.1 Evaluation System

Figure 4 shows an evaluation system. This system consists of the prototype chip, the evaluation board which retrieves the random number from the chip, and the interface board which connects the evaluation board to a PC for evaluation. The circuits of the interface board are implemented on FPGA board (Spartan-3E) [30]. By connecting the stabilized power source to the evaluation board, the power voltage is supplied by the unit of 0.01 V. The random number generated from the chip sends to the PC for measurement by way of the data acquisition function and the PC interface function (RS-232C) on the interface board. Using the command control function on the interface board, commands can be sent from the PC for measurement to the prototype chip. By writing a command to the command interface function, the PC for measurement can receive either the random numbers or one of the 256 latch outputs.

We acquired the random numbers and the latch outputs from four prototype chips using this evaluation system.When we measured them for performance in different temperatures, the prototype chip mounted on the evaluation board was in a constant temperature oven and the interface board operated under normal rated voltage at room temperature.

The temperatures and supply voltages for evaluation were decided from the viewpoint of upper/lower bounds of rated values. Three temperatures were selected: 85°C, 25°C, and −20°C, and three voltages were also selected: 1.21 V, 1.10 V, and 0.99 V.

4.2 Randomness Evaluation

We acquired 5.5 Mbits of random number for each pair of voltage and temperature, meaning there were 36 random number sequences (3 voltages × 3 temperature × 4 chips) for evaluation. We evaluated the randomness and entropy by statistical tests in accordance with AIS20/31 and SP800-90B.

Table 1: Pass ratio of the statistical tests

Temperature	Voltage	AIS 20/31	SP800-90B 1st draft	SP800-90B 2nd draft
−20°C	0.99V	4/4	20/20	15/20
	1.10V	4/4	20/20	19/20
	1.21V	4/4	20/20	**20/20**
25°C	0.99 V	4/4	20/20	19/20
	1.10 V	4/4	20/20	19/20
	1.21 V	4/4	20/20	20/20
85°C	0.99 V	4/4	20/20	20/20
	1.10 V	4/4	20/20	19/20
	1.21 V	4/4	20/20	19/20

4.2.1 Statistical Tests by AIS20/31

AIS20/31 includes eight statistical tests from T0 to T7. We evaluated the random numbers in accordance with test procedure A specified in AIS20/31. In test procedure A, the random numbers are evaluated by statistical tests from T0 to T5. If the random number is ideal, the probability of passing these tests is almost 0.9978, while the probability of failing more than two types of test is almost 0. If a random number fails one test, new random numbers are acquired and are tested again. If the random number fails more than one test, the statistical tests fail.

The pass ratio of tests are shown in Table 1. The random numbers acquired in nine pairs of temperatures and voltages passed all tests. We used the test library in C implemented ourselves.

4.2.2 IID Test by SP800-90B

IID is an abbreviation for Independent and Identically Distributed, which is defined as "a sequence of random variables for which each element of the sequence has the same probability distribution as the other values, and all values are mutually independent" in SP800-90B [28]. If a random number generated by an entropy source passes the IID validation tests, the entropy source can be thought to generate a high-entropy random number. IID validation tests contain shuffling tests on independence and stability (six tests) and specific statistical tests (two tests). We used the test library for second draft [19]. In addition, we also used the test library in C implemented ourselves in accordance with SP800-90B (first draft) for reference.

Table 1 shows the pass rates of the IID validation test. SP800-90B requires at least 1 Mbits for IID validation. To increase the number of the IID evaluation, we divided the measured data (5.5 Mbits) into five data sets. Each data set included 1 Mbits and the last 0.5 Mbits were not used for the evaluation. Concerning the tests in accordance with SP800-90 (first draft), all data sets by four chips evaluated as IID in all pairs of temperatures and voltages. Concerning SP800-90 (second draft), some data sets were not evaluated as the IID at −20°C and 0.99 V. However, in the other pairs of temperatures and voltages, most of the data sets were evaluated as the IID. From these results, we consider our SR-TRNG generates random numbers evaluated as IID. In addition, the evaluations in SP 800-90B (second draft) con-

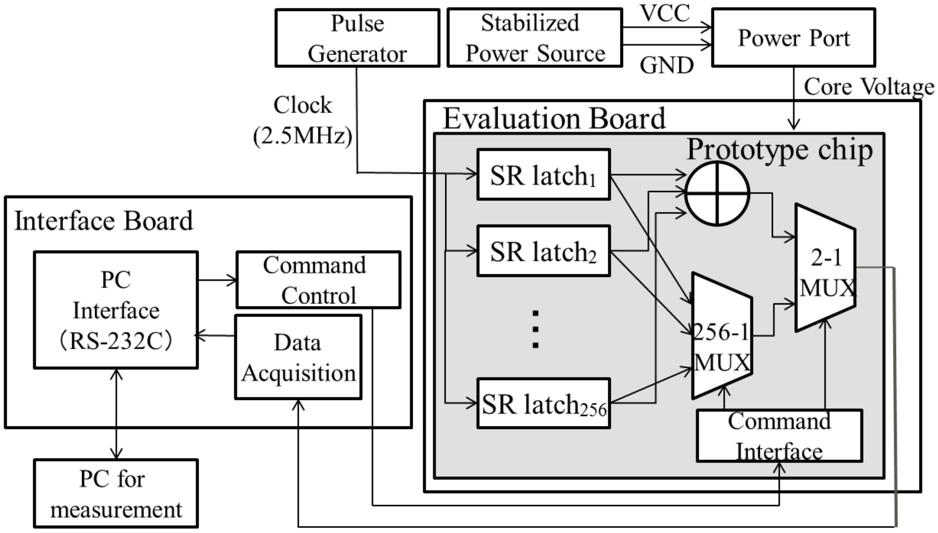

Figure 4: Evaluation System

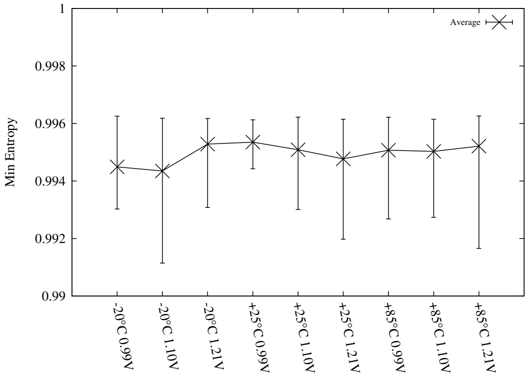

Figure 5: Min-entropy Evaluation (SP800-90B second draft)

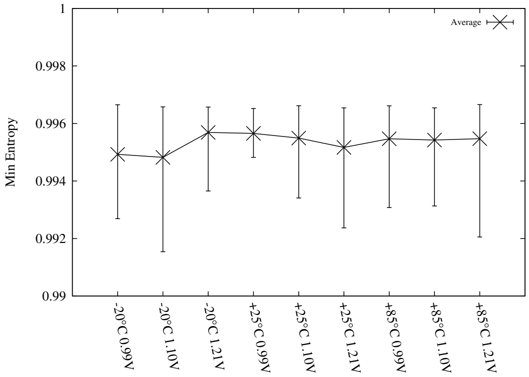

Figure 6: Min-entropy Evaluation (SP800-90B first draft)

sidered to have detected the statistical characteristics better than that in first draft.

SP800-90B (second draft) requires the restart test to evaluate the random number as IID. Instead of acquiring the restart data, we used another data set which was not used in the IID evaluation. Therefore, the results did not comply with the second draft perfectly. We remain hopeful expect that the result will be the same when we use the restart data.

4.2.3 Estimate Min-entropy by SP800-90B

“The min-entropy of a random variable is a lower bound on its entropy." [28] An ideal binary random number generates 1 and 0 at the same probability. Hence, min-entropy per bit is ideally 1. Evaluation of min-entropy is specified depending on whether the random number is IID or not in SP800-90B. From the IID evaluation above, we consider the random numbers generated by our SR-TRNG as the IID random number.

Figure 5 shows the min-entropy per bit in accordance with the min-entropy estimation in SP800-90B (second draft). The × mark and the upper and lower lines show the average, maximum, and minimum of the min-entropy. For reference, that in SP-800-90B (first draft) is also shown in Figure 6. The results were almost the same between the SP800-90B first and second drafts. In both estimations, the min-entropies of our SR-TRNGs were from 0.994 to 0.996 on average, which was near the ideal value of 1 when the voltages and the temperatures were changed.

5. RANDOM LATCH EVALUATION

In this section, we evaluate the number and quality of random latches in our SR-TRNG when the voltages and the temperatures are changed.

When the number of random latches increases in the SR-TRNG, the higher entropy random number is considered to be generated. In addition, a random latch is considered to be higher quality when the probability of 0 or 1 in the output is near 1/2.

For four SR-TRNG chips, we acquired 20 Kbits each from 256 SR latches per chip at nine pairs of voltages and temperatures. We evaluated the random latches with these data.

5.1 Number of Random latches

Figure 7 shows the number of random latches when the pairs of voltage and temperature change. The bars and the upper and lower lines show the average, maximum, and minimum of the number of random latches in the test cases.

The number of random latches changed depending on voltage and temperature. Changing the voltage and/or temperature transformed some constant latches into random latches and vice versa. There were about 27 random latches and 299 constant latches on average in the SR-TRNG chip. The minimum number of random latches was 15 when the temperature and the voltage was $-20°\mathrm{C}$ and 0.99 V, respectively. From these observations, it can be said that our SR-TRNG is robust against a disturbance of voltage and temperature.

5.2 Quality of Random latches

In this section, we evaluate the quality of random latches. Theoretically, one high-quality random latch is enough to generate high-entropy random numbers. In this paper we define the quality of each latch as the frequency ratio of 0 or 1 in the output sequence. The highest quality is 50%. The quality 40% and 60% can be considered to be the same as the aspect of the random number. Therefore, the range of the quality is defined from 0% (constant output 0 or 1) to 50%. The quality of random latches in an SR-TRNG is considered to affect that of the random number output. Therefore, the quality of random latch is one of the important elements to evaluate in the SR-TRNG.

Figure 8 shows the number of random latches and their quality when the environment changed. The horizontal axis represents the temperature and voltage, and the vertical axis represents the number of random latches. We divided the quality of random latches $(0-50\%)$ into units of 10% and counted the number of random latches in each interval.

In any combination of voltage and temperature, there were a few high-quality random latches of which the quality was between 40% and 50%. The number of high quality random latches in Hata and Ichikawa prototype SR-TRNG was low [10]; however, the output passed the NIST SP800-22 statistical test. Therefore, we expected that our SR-TRNG implemented on 40 nm technology would also generate high-entropy random numbers. On the other hand, the number of low-quality random latches of which the quality was between 0% and 10%, was larger. The low-quality random latches contributed to increase the entropy of the SR-TRNG random number by XOR operation. From this consideration, it can be said that the prototype chip of our SR-TRNG on 40 nm technology has high robustness against environmental fluctuation.

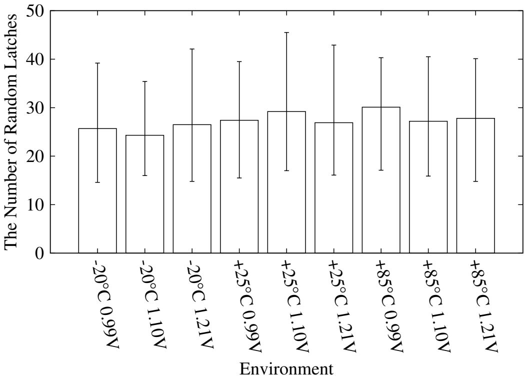

Figure 7: The number of random latches

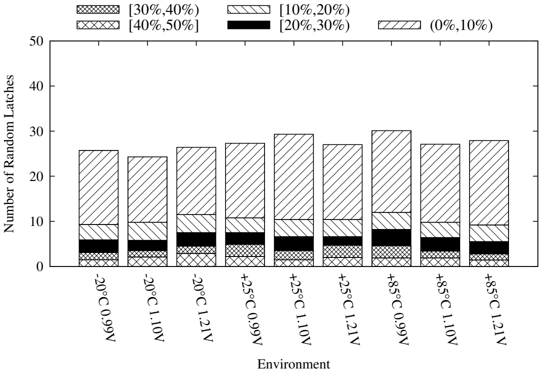

Figure 8: Quality of random latch (40nm technology)

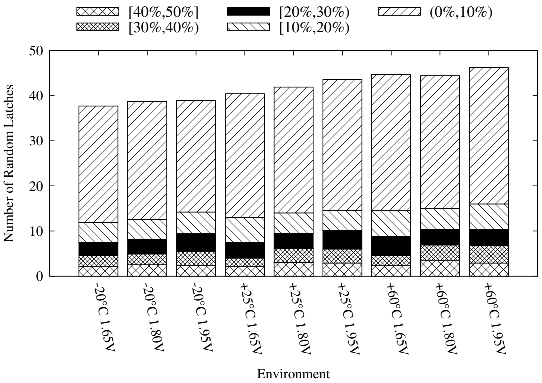

Figure 9: The quality of random latches (0.18μm technology [15, 27])

6. DISCUSSION

6.1 Effect of CMOS process

In this section, we consider the effect of process miniaturization in our SR-TRNG implementation. We compare the number of random latches in the SR-TRNG by a 40 nm process with those in SR-TRNG by 0.18 μm [15, 27]. The same logic design was used to implement the SR-TRNG; therefore, the chip area and the power consumption was reduced by process technology miniaturization. Both SR-TRNGs generated random numbers with high entropies to pass AIS20/31 statistical tests, were evaluated as IID by

SP800-90B, and have tolerance against environmental fluctuation.

However, the number of random latches decreased by the technology miniaturization in our implementation. Figure 9 shows the evaluation of the number of random latches in the 0.18 μm process [15, 27]. Comparing with that in 40 nm, the number of random latches decreases in every combination of temperatures and voltages in 40 nm technology.

Here, we consider the reason why the number of random latches decreases by technology miniaturization. To generate a high quality random number by a random latch, the components of the random latch are considered to have identical characteristics. That is, the two NAND gates and its wiring characteristics are required to be identical. Therefore, we consider that the characteristics fluctuation increases by the process technology miniaturization.

The effect of process miniaturization has been reported [11, 21, 25]. Both the threshold voltage fluctuation in each MOSFET in the NAND gate and the standard deviation of 1/f noise are inversely proportional to $\sqrt{LW}$ (L: channel length, W: channel width). In addition, by decreasing the supply voltage, the effect of them increases to a relatively large degree. The cross-section areas of the wiring are also miniaturized, hence the resistance and the inductance increase.

The output of the random latch is decided by the difference between the two NAND gates characteristics. The random latch consists of two NAND gates, and they are allocated adjacently. Therefore, the difference of their characteristics is considered to be relatively small. However, the threshold voltage of NMOS in the CMOS is known to be difficult to control. We expect that the fluctuation of the threshold voltage of the NMOS causes the decrease of the random latches.

From these considerations, the number of latches in SR-TRNG is required to increase when the process technology is miniaturized.

6.2 Performance

In this section, we consider a factor to decide the throughput of our SR-TRNG. The clock, that is the throughput of our SR-TRNG, is 2.5 MHz. We did not evaluate the highest clock to generate the random number, because we expected that 2.5 MHz was fast enough to generate random numbers for IoT equipment.

The throughput of the SR-TRNG depends on the duration time of the metastability state. The duration time is expressed as follows [8, 12]:

$$t_d = \tau_r \cdot \ln(\frac{\Delta V_f}{\Delta V_i}) \tag{1}$$

where τ_r is a constant depending on the devices and the circuit, ΔV_f is the final difference between the initial voltage and the metastable voltage, and ΔV_i is the initial difference between the initial voltage and the metastable voltage. The metastable voltage is decided mainly by the mismatch of the devices and output loads at noiseless state. In practice there are noises; therefore, the initial voltage ΔV_i varies. The noises have two elements:

- The noise decided by the circuit elements ΔV_d
- The thermal noise ΔV_n

It is reported that a latch will be the random latch which consists of well-balanced elements when ΔV_d is relatively small and the thermal noise is dominant. That is, when ΔV_d is large, the duration time of metastability of a latch will be shorter and the latch will be the constant latch. When ΔV_d is less than or equal to the thermal noises, the duration time of metastability of a latch will be longer and the latch will be the random latch [26].

To increase the throughput, it is preferable for the constant τ_r to be small. It is decided by the wiring capacity and resistance, and the transconductance of the MOSFET. To design the SR-TRNG, it is a point to consider that the value of τ_r and the circuit noise ΔV_d is small.

6.3 Temperature characteristics

In this section, we consider the effect of temperature change. In this implementation, the NAND gate consists of MOSFETs. When the temperature increases, the threshold voltage V_{th} and the mobility μ is expressed as follows [12, 23]:

$$V_{th} = V_{th0} - \kappa T, \tag{2}$$

$$\mu = \mu_0 \left(\frac{T_0}{T}\right)^m \tag{3}$$

where V_{th0} is the threshold voltage at absolute zero temperature, κ is the temperature coefficient of the threshold voltage, μ_0 is mobility at T_0, and m is the temperature coefficient of the mobility.

From these equations, when the temperature increases, the absolute value of the threshold voltage V_{th} decreases and subthreshold current increases. On the other hand, the mobility μ decreases and subthreshold current decreases. Therefore, an input clock of the latch changes from 0 to 1, meaning the threshold voltage and the mobility affect the subthreshold current in opposite directions. The effect depends on the process and elements. In this implementation, the change of the threshold voltage is common to two NAND gates which consist of a latch circuit. Therefore, the common changes are canceled out and the temperature change has little effect on the output of the latch. It can be presumed that this is one of the reasons that the temperature fluctuations have little effect on the quality of random numbers.

6.4 Comparison

Table 2 shows the comparison with previous works implemented by CMOS ASIC. Bucci and Luzzi [7] includes a health test circuit and the other does not. The statistical test is not the same. Hence, the comparison is for reference only. Our previous implementation of SR-TRNG on 0.18 μm technology is shown in line 8 [15, 27]. Compared with our previous implementation, the power consumption is about 1/14.

Our SR-TRNG is considered to be well-balanced between the power consumption and the throughput.

7. CONCLUSION

In this paper, we fabricated a true random number generator using an SR latch in 40 nm CMOS and evaluated the robustness against temperature and voltage changes in the rated values. That is, the supply voltages were from 0.99 V to 1.21 V, and the temperatures were from −20°C to 85°C. We evaluated the random numbers in accordance with

Table 2: Comparison with previous works

Entropy source	Reference	Technology	Power	Throughput	Post-proc.	Evaluation
Noise of analog curcuit	[20]	2 μm	3.9 mW	1.4 Mbps	-	FIPS140-1, DIEHARD
	[5]	0.18 μm	2.3 mW	5 Mbps	XOR decorrelating	FIPS140-1, Knuth 2nd ed.
	[4]	0.12 μm	50 μW	200 Kbps	v.Neumann	Entropy dist
	[18]	0.25 μm	1.9 mW	2 Mbps	-	FIPS140-2
Oscillator	[6]	0.18 μm	2.3 mW	10 Mbps	-	FIPS140-1, Knuth 2nd ed
	[7]	90 nm	240 μW	1.74 Mbps	LSFR	AIS31,Entropy dist.
	[22]	130 nm	650 nW	25 bps	6bit LSFR	SP800-22 Basic
	[16]	65 nm	2 mW	11 Kbps	-	SP800-22
	[1]	65 nm	-	7.5 Mbps	-	SP800-22Basic, DIEHARD
Metastable	[26]	0.13μm	1 mW	40 Kbps	5:1decimation	SP800-22 Basic
	[13]	0.35 μm	9.4 μW	5 Kbps	NSFR	SP800-22 Basic
	[17]	45 nm	7 mW	2.4 Gbps	-	SP800-22
	[15, 27]	0.18 μm	0.27 mW	2.5 Mbps	-	SP800-90B & -22, AIS20/31
	This work	40 nm	18.8 μW	2.5 Mbps	-	SP800-90B, AIS20/31

AIS20/31 [14] and SP800-90B [2, 28] and our SR-TRNG passed all the statistical tests except in a few cases. The min-entropy was near 1, which was a value of an ideal random number. It is evident from this evaluation that our SR-TRNG generates high-entropy random numbers in the environments tested. The power consumption was 18.8 μW at 2.5 MHz clock.

In addition, we discussed the difference between SR-TRNG on a 0.18 μm process and that on a 40 nm process. We found that the number of random latches decreased by process miniaturization. Therefore, the number of latches in an SR-TRNG is required to increase when the process technology is miniaturized.

The fact that our SR-TRNG generates high-entropy random number reveals that it can be applied to various applications, such as a seed source of a pseudo random number generator or a key generation. Hence, our SR-TRNG is suitable for IoT equipment.

8. REFERENCES

[1] T. Amaki, M. Hashimoto, and T. Onoye. A process and temperature tolerant oscillator-based true random number generator. *IEICE Trans. Fundamentals*, E97-A(12):2393–2399, 2014.

[2] E. Barker. SP800-90B: DRAFT recommendation for the entropy sources used for random bit generation (1st draft). Technical report, National Institute of Standards & Technology (NIST), 2012.

[3] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo. SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, National Institute of Standards & Technology (NIST), April 2010.

[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 *2006 IEEE International Solid State Circuits Conference - Digest of Technical Papers*, pages 1666–1675, Feb 2006.

[5] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo. A high-speed IC random-number source for smartcard microcontrollers. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 50(11):1373–1380, Nov 2003.

[6] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC. *IEEE Trans. Comput.*, 52(4):403–409, Apr. 2003.

[7] M. Bucci and R. Luzzi. Fully digital random bit generators for cryptographic applications. *IEEE Trans. Circuits Syst. I, Reg. Papers*, 55(3):861–875, 2008.

[8] C. Dike and E. Burton. Miller and noise effects in a synchronizing flip-flop. *IEEE Journal of Solid-State Circuits*, 34(6):849–855, jun 1999.

[9] P. Haddad, V. Fischer, F. Bernard, and J. Nicolai. A physical approach for stochastic modeling of tero-based TRNG. In *Cryptographic Hardware and Embedded Systems - CHES 2015*, volume 9293 of *Lecture Notes in Computer Science*, pages 357–372, 2015.

[10] H. Hata and S. Ichikawa. FPGA implementation of metastability-based true random number generator. *IEICE Transactions*, 95-D(2):426–436, 2012.

[11] T. Hiramoto, K. Takeuchi, and A. Nishida. 1. variability of characteristics in scaled MOSFETs (<special section>LSI design techniques under increase of device variations in CMOS scaling)(in Japanese). *IEICE*, 92(6):416–426, jun 2009.

[12] D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Computers*, 58(9):1198–1210, 2009.

[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 Journal of Solid-State Circuits*, 43(5):1324–1336, 2008.

[14] W. Killmann and W. Schindler. *A proposal for: Functionality classes for random number generators Version 2.0.* Bundesamt für Sicherheit in der Informationstechnik (BSI), September 2011.

[15] H. Kokubo, D. Yamamoto, M. Takenaka, K. Itoh, and

N. Torii. Evaluation of ASIC implementation of physical random number generators using RS latches. In *Smart Card Research and Advanced Applications - CARDIS 2013*, volume 8419 of *Lecture Notes in Computer Science*, pages 3–15, 2013.

[16] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw. A true random number generator using time-dependent dielectric breakdown. In *VLSI Circuits (VLSIC), 2011 Symposium on*, pages 216–217, June 2011.

[17] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, 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 Journal of Solid-State Circuits*, 47(11):2807–2821, 2012.

[18] 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 *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 414–624, Feb 2008.

[19] K. McKay and J. Kelsey. SP800-90B Entropy Assessment. https://github.com/usnistgov/SP800-90B_EntropyAssessment, 2016. National Institute of Standards & Technology (NIST).

[20] C. S. Petrie and J. A. Connelly. A noise-based ic random number generator for applications in cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 47(5):615–621, May 2000.

[21] A. T. Putra, A. Nishida, S. Kamohara, and T. Hiramoto. Random threshold voltage variability induced by gate-edge fluctuations in nanoscale metaloxide semiconductor field-effect transistors. *Applied Physics Express*, 2(2):024501, 2009.

[22] C. D. Roover and M. Steyaert. A 500 mV 650 pW random number generator in 130 nm cmos for a uwb localization system. In *ESSCIRC, 2010 Proceedings of the*, pages 278–281, Sept 2010.

[23] S. Selberherr. MOS device modeling at 77 K. *IEEE Trans Elec. Dev.*, 36(8):1464–1474, 1989.

[24] 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.Computers*, 56(1):109–119, Jan 2007.

[25] K. Takeuchi, T. Tatsumi, and A. Furukawa. Channel engineering for the reduction of random-dopant-placement-induced threshold voltage fluctuation. In *Electron Devices Meeting, 1997. IEDM '97. Technical Digest., International*, pages 841–844, Dec 1997.

[26] C. Tokunaga, D. Blaauw, and T. Mudge. True random number generator with a metastability-based quality control. *IEEE Journal of Solid-State Circuits*, 43(1):78–85, Jan 2008.

[27] N. Torii, H. Kokubo, D. Yamamoto, K. Itoh, M. Takenaka, and T. Matsumoto. ASIC implementation of random number generators using SR latches and its evaluation. *EURASIP J. Information Security*, 2016(1):1–12, 2016.

[28] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle. SP800-90B:DRAFT recommendation for the entropy sources used for random bit generation (second draft). Technical report, National Institute of Standards & Technology (NIST), 2016.

[29] M. Varchola and M. Drutarovský. New high entropy element for FPGA based true random number generators. In *Cryptographic Hardware and Embedded Systems, CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 351–365, 2010.

[30] Xilinx Inc. Spartan-3E Starter Kit. http://www.xilinx.com/products/boards-and-kits/hw-spar3e-sk-us-g.html.