Switched-Current 3-Bit CMOS 4.0-MHz Wideband Random Signal Generator

Chua-Chin Wang, *Senior Member, IEEE*, Jian-Ming Huang, Hon-Chen Cheng, and Ron Hu

***Abstract*—The paper presents a switched-current circuit implementation of a chaotic algorithm to generate a white noise. A 3-bit digital normalizer is utilized to adjust the coefficients in the piecewise-linear transfer function such that the probability of the generated numbers will be very close to a uniform distribution. A 1.0 –GHz linear track-and-hold circuit is applied in the random number generator (RNG) to achieve a wide output bandwidth. TSMC 0.25-μm one-poly five-metal CMOS process is adopted to carry out the proposed design to verify the wideband performance. When the operating clock is 10.0 MHz, the measured bandwidth of the generated noise is 4.0 MHz.**

***Index Terms*—Chaos, digital normalizer, long run test, random number generator, switched currents.**

I. Introduction

REAL random number generators (RNGs) have become in great demand ever since the spread-spectrum communication market started booming [2]. They also attract great research interest in the security domain of networks and wireless communications. Previous widely used pseudo-noise (PN) codes usually have a periodicity which repeats after a large number of code symbols. These codes are mathematically predictable. Researchers have turned their attentions to hardware approaches seeking the feasibility of using circuits to implement RNGs [3]–[11]. Three major trends of carrying out RNGs are direct amplification, oscillator sampling, and discrete-time chaos [6]. The discrete-time chaos (DTC) method is very welcomed due to its compatibility with digital systems. Two ways to implement the DTC are the switched-capacitor approach [4] and the switched-current approach [3]. Considering the possibility of integrating an RNG into a system-on-a-chip (SOC) IC, we adopt the switched-current scheme to carry out a 3-bit RNG with a very wide bandwidth (4 MHz) using TSMC 0.25-μm one-poly five-metal (1P5M) CMOS technology. The features of the proposed RNG include a 1.0-GHz linear track-and-hold (TH) circuit [12] to avoid charge injection and channel conductance variation problem, and a digitally controllable normalizer to dynamically adjust the coefficients to prevent any divergence. The proposed design is proven on silicon to possess the wideband performance. When the operating clock is 10.0 MHz, the measured bandwidth of the generated noise is 4.0 MHz, which is larger than all of the prior works. It also passed the long run test to verify that the proposed design can be deemed as a white noise generator.

Manuscript received April 29, 2004; revised March 3, 2005. This work was supported in part by the National Science Council under Grant NSC 91-2218-E-110-001 and 91-2622-E-110-004.

C.-C. Wang and J.-M. Huang are with the Department of Electrical Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan 80424, R.O.C. (e-mail: ccwang@ee.nsysu.edu.tw).

H.-C. Cheng is with the Taiwan Semiconductor Manufacturing Company, Hsin-Chu 300, Taiwan, R.O.C.

R. Hu is with Asuka Semiconductor Inc., Hsin-Chu, Taiwan, R.O.C.

Digital Object Identifier 10.1109/JSSC.2005.848036

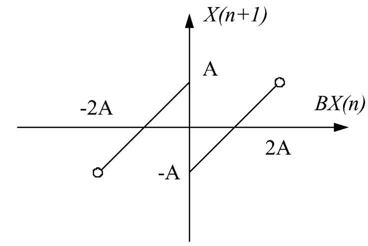

Fig. 1. Transfer function of 1-bit RNG ($B = 2$).

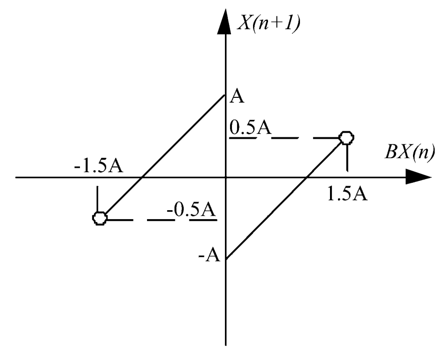

Fig. 2. Scenario given a smaller $B (B = 1.5)$.

II. Three-Bit Random Number Generator

The basic theory of the 1-bit DTC algorithm is summarized as follows [3]:

$$\begin{cases} X(n+1) = B \cdot X(n) - A \cdot \mathrm{sgn}(X(n)) \\ X(0) = \frac{A}{B-1} \end{cases} \tag{1}$$

where $X(i)$ is the ith bit of the generated sequence, A and B are floating numbers. B determines the characteristics of the dynamic range of the generated signals: if $B < 1$, the $X(n)$ converges; if $B > 2, X(n)$ diverges. Hence, B must be in the range of [1, 2] to ensure the output $X(n)$ in the range of $[-A, +A]$. The transfer function of (1) is shown in Fig. 1. Notably, the slope of the transfer function is determined by B. Two scenarios with $B = 2.0$ and $B = 1.5$ are shown in Figs. 1 and 2, respectively. In the former case, the probabilities to generate "1" and "0" in the next bit are identical. However, in the latter case, when $X(n) > 0$, the probabilities to have 1 and 0 in the next bit are $1/3$ and $2/3$, respectively. Hence, we need a sophisticated mechanism to dynamically adjust A based on the given B to generate "1" and "0" with equal probability in the next bit

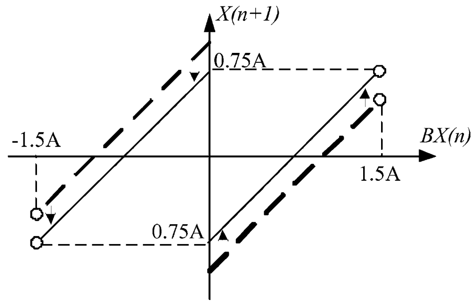

Fig. 3. Adjustment of B.

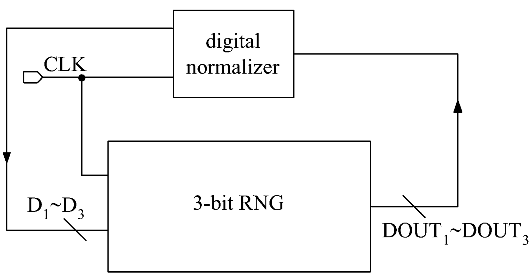

Fig. 4. Proposed 3-bit RNG.

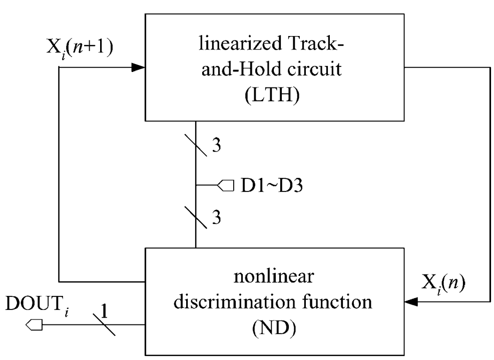

Fig. 5. Proposed 1-bit RNG.

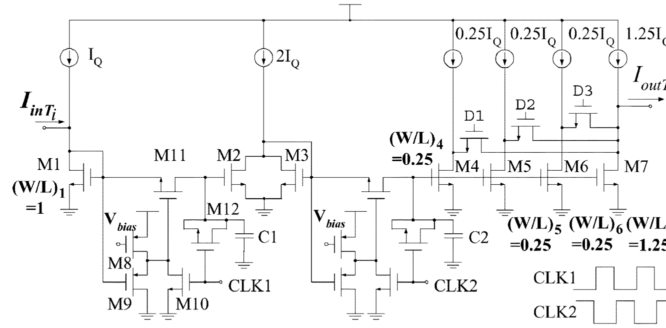

Fig. 6. Schematic of the LTH in the 1-bit RNG.

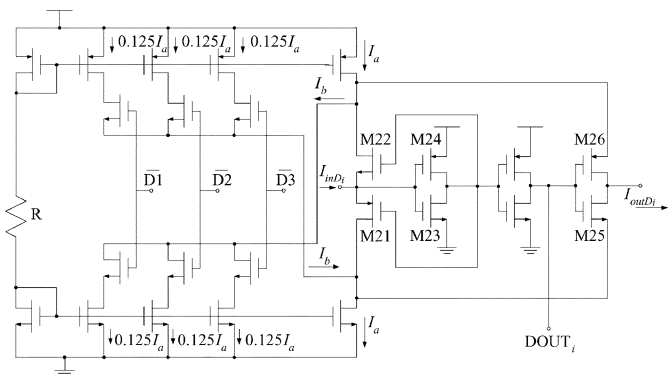

Fig. 7. Schematic of the ND in the 1-bit RNG.

TABLE I
COMBINATIONS OF THE OUTPUT CURRENT

DOUT_3 DOUT_2 DOUT_1	D3 D2 D1	B
0 0 0	0 0 0	$1.25I_Q$
0 0 1	0 1 0	$1.50I_Q$
0 1 0	0 0 0	$1.50I_Q$
0 1 1	0 1 1	$1.75I_Q$
1 0 0	1 0 0	$1.50I_Q$
1 0 1	1 1 1	$1.75I_Q$
1 1 0	1 0 1	$1.75I_Q$
1 1 1	1 1 1	$2.00I_Q$

of the sequence. A possible scenario of such an adjustment is shown in Fig. 3.

When it comes to the hardware realization of RNGs, it has been proved that the distribution of generated bits will be close to uniform for B near 2. It will be not the case for $B < \sqrt{2}$. Hence, in the process of generating random numbers, B must be dynamically adjusted to avoid drifting toward $\sqrt{2}$ or even smaller. In short, the generated random numbers will be colored if either of these two condition exists. Furthermore, in order to make generated numbers be white, the nonlinear discrimination (ND) circuit should not only carry out the $\mathrm{sgn}(X(n))$ but also be able to adjust A dynamically.

A. 3-Bit RNG Architecture

We propose a modified switched-current design to eliminate the mentioned "colored" problem. Referring to Fig. 4, a digital normalizer reads the generated bits, $\mathrm{DOUT}_1, \mathrm{DOUT}_2$, and DOUT_3, to determine the slope of the next iteration, which is denoted by $\mathrm{D}_1, \mathrm{D}_2$, and D_3. The 3-bit RNG comprises three 1-bit RNGs, which are shown in Fig. 5, and the digital normalizer. The single ith 1-bit RNG reads the generated D1, D2, and D3 and $X_i(n)$ in the last iteration to produce the $X_i(n+1)$ and DOUT_i for the next iteration. Notably, $\mathrm{D}_1, \mathrm{D}_2$, and D_3, are D1, D2, and D3, respectively. We use different symbols in different figures for the sake of clarity. In short, the digital normalizer flattens the distribution of the probability by mapping the DOUT_i into $\mathrm{D}_i,\ \forall i, i = 1, 2, 3$.

B. 1-Bit RNG Schematic Design

1) LTH Circuitry: (Linear Track-and-Hold): Fig. 6 reveals the schematic to carry out the programmability of B. CLK1 and CLK2 are two nonoverlapping clocks. The W/L ratios of M1, M2, and M3 are 1/1. By contrast, the W/L ratios of M1 to M4, M5, M6, and M7 are 1, 0.25, 0.25, 0.25, and 1.25, respectively. Thus, the overall current can be determined by D1, D2, and D3. For instance, if all of them are 1's, the overall current will be 2.0 times of I_Q. I_Q must be set to at least twice as large as the input current, $I_{\mathrm{in}T_i}$. M8, M9, M10, M11, M12 constitute a linear track-and-hold switch [12]. A cascade of two

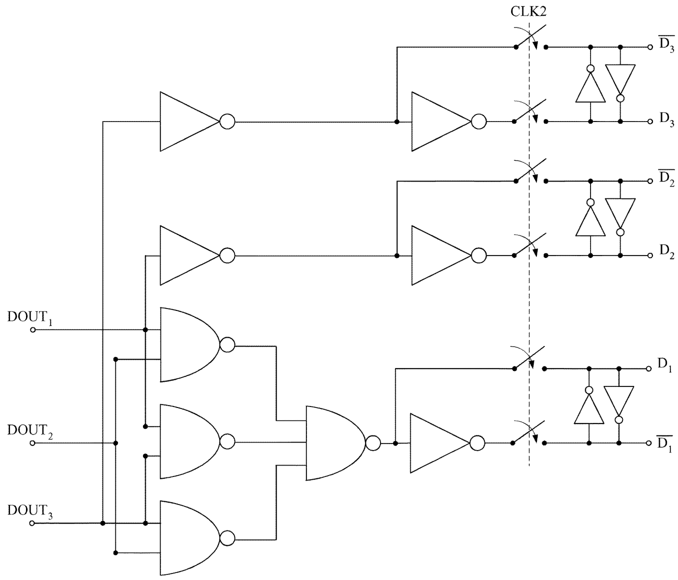

Fig. 8. Digital normalizer.

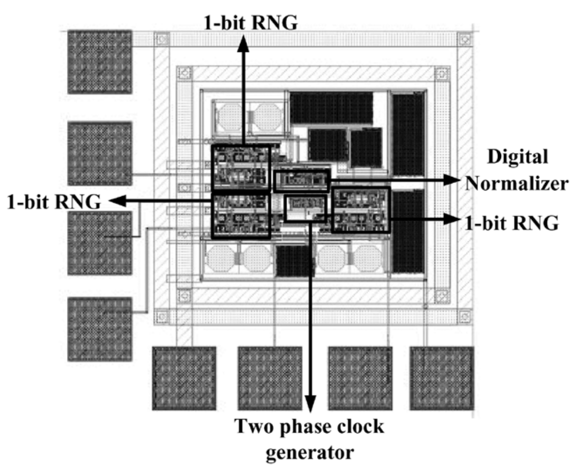

Fig. 9. Layout of the proposed 3-bit RNG.

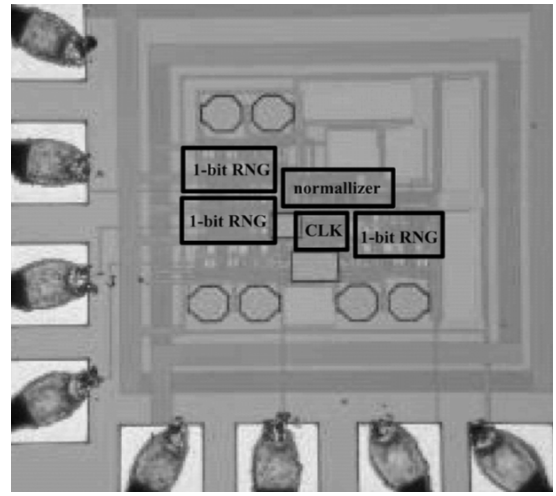

Fig. 10. Die photo of the proposed 3-bit RNG.

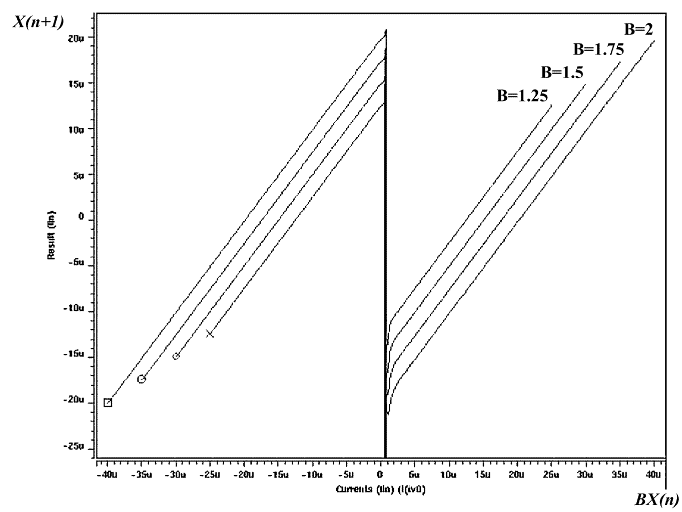

Fig. 11. Post-layout simulation of the transfer function.

track-and-hold switches perform switched current delay operation [13]. M9 stabilizes the gate drive of M11 to prevent channel conductance input-dependent variation and the charge injection effect. The output current $I_{\mathrm{out}T_i}$, in fact, denotes the $X_i(n)$ to be fed into the ND as $I_{\mathrm{in}D_i}$ in Fig. 7. The input current $I_{\mathrm{in}T_i}$ is supplied by the output current $I_{\mathrm{out}D_i}$ in Fig. 7.

2) ND Circuitry: (Nonlinear Discrimination Function): Fig. 7 is the ND circuit, which is based on [3], to generate the $X_i(n+1)$ and DOUT_i for the next iteration. The function is to carry out the $\pm A \cdot \mathrm{sgn}(\cdot)$ by examining the polarity of the input current $I_{\mathrm{in}D_i}$, which is the $I_{\mathrm{out}T_i}$ of the corresponding LTH circuit. The I_a is set to 20 μA. The inverse signals of D1, D2, and D3, are used to select the appropriate I_b to generate $A = I_a - I_b$.

3) $I_{\mathrm{in}D_i} = I_{\mathrm{out}T_i} > 0$: M21 and M23 are on, M22 is off, DOUT_i is high. Then, M25 is also turned on. The output current is $I_{\mathrm{out}D_i} = I_{\mathrm{in}D_i} - (I_a - I_b)$.

4) $I_{\mathrm{in}D_i} = I_{\mathrm{out}T_i} < 0$: M22 and M24 are on, while M21 is off to make DOUT_i low. Thus, M26 is on. $I_{\mathrm{out}D_i} = I_{\mathrm{in}D_i} + (I_a - I_b)$.

C. Digital Normalizer

Referring to the 1-bit RNG, a total of 4 values of B can be synthesized by $\mathrm{D}_1, \mathrm{D}_2, \mathrm{D}_3$: 1.25, 1.5, 1.75, and 2.0 times of I_Q, as shown in Table I. However, there are a total of 8 combinations of 3 binary bits. It is easy to find out that the probability of 1.25, 1.5, 1.75, and 2.0 times of I_Q is $1/8, 3/8, 3/8$, and $1/8$. A digital normalizer, shown in Fig. 8, resolves the problem by mapping the DOUT_i into D_i, $\forall i, i = 1, 2, 3$, to normalize the probability to be $1/4$.

$$
\begin{aligned}
\mathrm{D}_3 &= \mathrm{DOUT}_3 \\
\mathrm{D}_2 &= \mathrm{DOUT}_1 \\
\mathrm{D}_1 &= \mathrm{DOUT}_1\mathrm{DOUT}_2 + \mathrm{DOUT}_2\mathrm{DOUT}_3 + \mathrm{DOUT}_3\mathrm{DOUT}_1.
\end{aligned} \tag{2}
$$

In short, the function of the digital normalizer is to equalize the probability of $B = 1.25, 1.5, 1.75, 2.0$ for the next iteration. Thus, the entire 3-bit RNG is immune to any process, voltage, and temperature (PVT) variations.

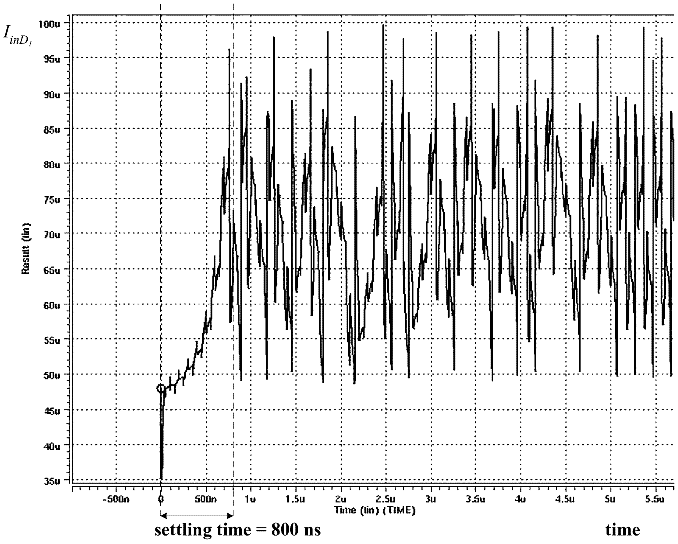

Fig. 12. Time domain analysis of the output.

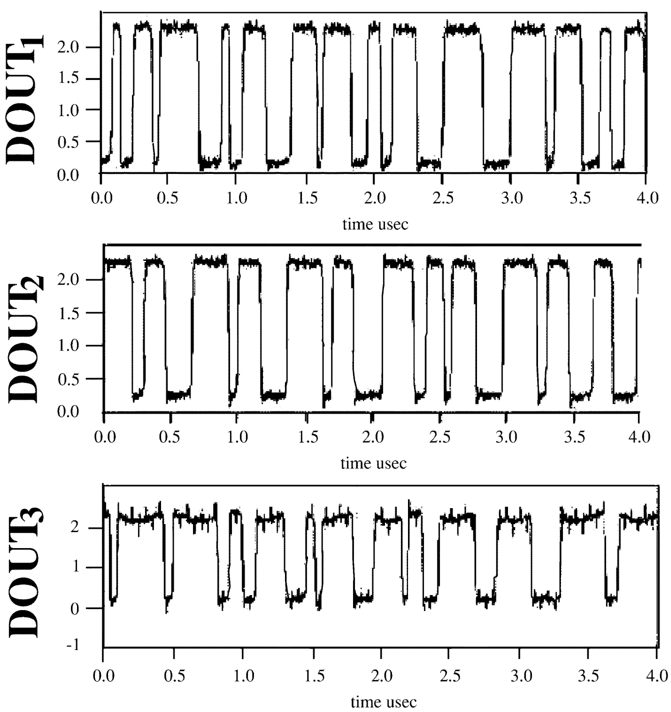

Fig. 13. All of the generated sequecnces.

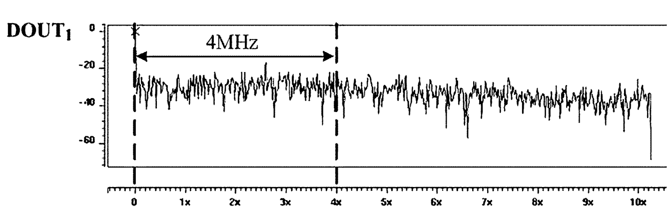

Fig. 14. Spectrum of the generated signals.

III. Measurement and Testing

A. Implementation and Measurement

The overall design is implemented by Taiwan Semiconductor Manufacturing Company (TSMC) 0.25-μm 1P5M

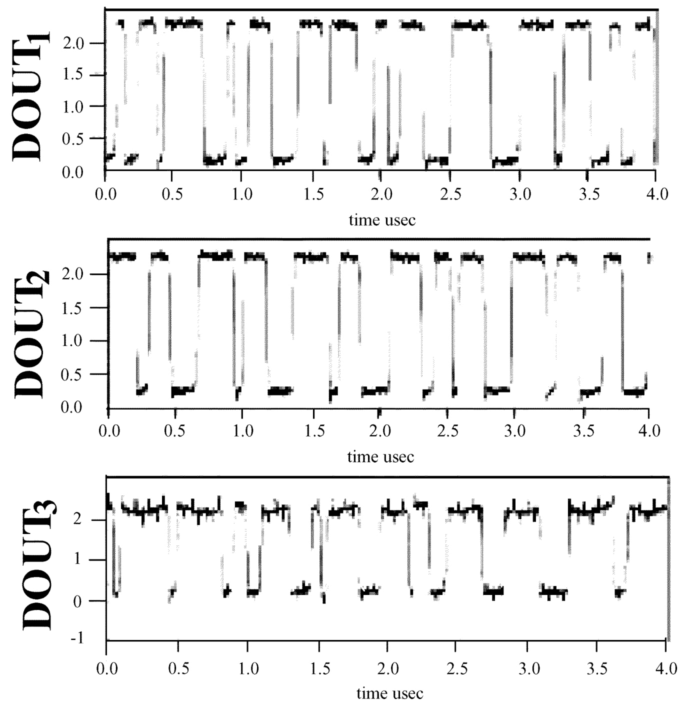

Fig. 15. Bit sequence of the generated signals.

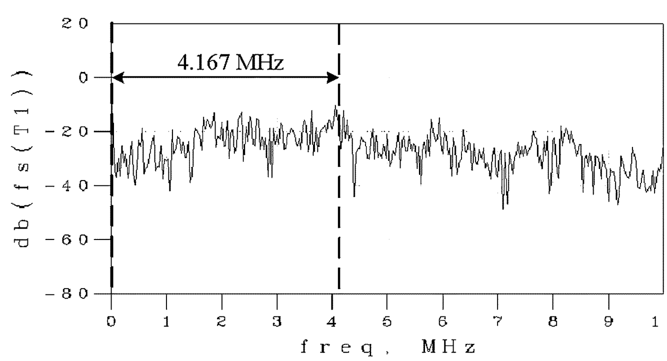

Fig. 16. Measured spectrum of the generated signals.

TABLE II
MEASUREMENT RESULTS OF THE PROTOTYPE

transistor count	242
power	350.0 mW* @ 10 MHz
die size	0.528×0.495 mm^2
VDD range	2.50 V ± 10%
temperature	-25°C to +75°C
max. clock	10.0 MHz
output BW	4.167 MHz

(* Note : Power consumption of pads is concluded.)

CMOS process. The layout of the proposed design is given in Fig. 9, while the die photo of the proposed design is shown in Fig. 10. Fig. 11 is the post-layout simulation result of the RNG transfer function. The time domain analysis for the settling time is given in Fig. 12. Figs. 13 and 14 are the results of the post-layout simulations. Fig. 13 demonstrates the waveforms of generated sequences of DOUT_1 to DOUT_3. Fig. 14 shows the spectrum of DOUT_1. The power drop-off occurs at 4.0 MHz.

TABLE III
COMPARISON TO PRIOR DESIGNS

	[3]	[4]	[7]	[11]	ours
process	1.6 μm	3.0 μm	0.6 μm	0.8 μm	0.25 μm
system clock (MHz)	0.5	0.2	12	1	10
output BW (MHz)	0.15	0.08	N/A	N/A	4.0
output channels	1	1	1	1	3
normalized power consumption (mW)	N/A	N/A	N/A	3.2 *	117
normalized core size (μm^2)	2340	N/A	N/A	410	22234

(* Note : Power consmption of pads is cncluded.)

TABLE IV
LONG RUN TEST RESULT

no. of consecutive bits	DOUT_1		DOUT_2		DOUT_3	
	0s'	1s'	0s'	1s'	0's	1s'
1	1083	634	1037	770	1168	994
2	1452	1288	1115	490	1108	617
3	1248	1359	454	673	601	629
4	304	688	272	386	245	400
5	21	91	204	276	211	282
6	7	19	65	222	65	210
7	1	14	60	103	50	131
8	0	15	29	110	31	90
9	0	7	9	65	6	43
10	0	1	3	46	5	36
11	0	0	0	31	3	17
12	0	0	1	19	0	17
13	0	0	1	21	1	14
14	0	0	1	11	0	3
15	0	0	0	8	0	3
16	0	0	0	5	1	1
17	0	0	0	3	0	1
18	0	0	0	5	0	2
19	0	0	0	2	0	1
20	0	0	0	1	0	3
21	0	0	0	1	0	1
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0
25	0	0	0	0	0	0
26	0	0	0	0	0	1
27	0	0	0	0	0	0

By contrast, Fig. 15 shows the measured waveforms of the generated sequences of DOUT_1 to DOUT_3. Fig. 16 is the measured spectrum of DOUT_1. The measurements of the prototype were carried out by Agilent 33250A (clock generator), Tektronix TDS680B (OSC) and Agilent 66319B (power supply). The power drop-off occurs at 4.167 MHz. The overall measurements of the chip are summarized in Table II.

A comparison of our proposed RNG and several prior RNG designs is summarized in Table III. Our design possesses the edge of the output bandwidth as well as the output bit length.

B. Testing—Long Run Test

One of the basic test for a white-noise RNG is the long run test: the maximum number of consecutive "1"s or "0"s must be less than 34 in any 20,000 consecutively generated bits. Hence, we have activated the proposed RNG and collected the generated bits to get the statistical results in Table IV.

Based on Table IV, the maximal length of consecutive "1" or "0" is 26 which is smaller than the upper bound of 34. Hence, the proposed RNG is deemed as the true white-noise RNG.

IV. CONCLUSION

A 3-bit RNG design is present in this paper, which utilizes a digital normalizer to flatten the distribution of the probability in the entire range of B parameter. The "colored" random number problem in prior designs is resolved. The coefficients of the proposed design are dynamically adjustable. The physical measurement of the proposed design verifies the superiority of the output bandwidth. Meanwhile, the proposed RNG design also passes the long run test to prove that it is qualified as a white noise generator.

REFERENCES

[1] R. J. Baker, H. W. Li, and D. E. Boyce, *CMOS—Circuit Design, Layout, and Simulation*. New York, NY: IEEE Press, 1998.
[2] C. Chien, *Digital Radio Systems on a Chip*. Reading, MA: Kluwer, 2001.
[3] M. Degaldo-Restituto, F. Medeiro, and A. Rodriguez-Vazquez, "Nonlinear switched-current CMOS IC for random signal generation," *Electron. Lett.*, vol. 29, no. 25, pp. 2190–2191, Dec. 1993.
[4] A. Rodriguez-Vazquez, M. Delgado, S. Espejo, and J. L. Huertas, "Switched-capacitor broad-band noise generator for CMOS VLSI," *Electron. Lett.*, vol. 27, no. 21, pp. 1913–1914, Oct. 1991.
[5] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generation—Part II: Practical realization," *IEEE Trans. Circuits Syst. I: Fund. Theory Applicat.*, vol. 48, no. 3, pp. 382–385, Mar. 2001.
[6] M. Degaldo-Restituto and A. Rodriguez-Vazquez, "Integrated chaos generators," *Proc. IEEE*, vol. 90, no. 5, pp. 747–767, May 2002.
[7] F. Cortigiani, C. Petri, S. Rocchi, and V. Vignoli, "Very high-speed true random noise generator," in *Proc. Int. Conf. Electronics Circuits and Systems (ICECS2000)*, vol. 1, Dec. 2000, pp. 120–123.
[8] A. Gerosa, R. Bernardini, and S. Pietri, "A fully integrated 8-bit, 20 MHz, truly random numbers generator, based on a chaotic system," in *Proc. Southwest Symp. Mixed-Signal Design (SSMSD2001)*, Feb. 2001, pp. 87–92.
[9] P. Dudek and V. D. Juncu, "Compact discrete-time chaos generator circuit," *Electron. Lett.*, vol. 39, no. 20, pp. 1431–1432, Oct. 2003.
[10] J. Yu, H. Shen, and X.-L. Yan, "Implementation of a chaos-based, high-speed truly random number generator," in *Proc. Int. Conf. ASIC*, vol. 1, Oct. 2003, pp. 526–529.
[11] Z. Huang, G. Bai, and H. Chen, "A chaotic circuit for truly random number generation," in *Proc. Int. Conf. ASIC*, vol. 1, Oct. 2003, pp. 548–551.
[12] D. Jakonis and C. Svensson, "A 1 GHz linearized CMOS track-and-hold circuit," in *Proc. IEEE Symp. Circuits and Systesms (ISCAS'2002)*, vol. V, May 2002, pp. 577–580.
[13] J. B. Hughes, I. C. Macbeth, and D. M. Pattullo, "Switched current filters," *Proc. Inst. Electr. Eng.*, vol. 137, no. 2, pp. 156–162, Apr. 1990.

Chua-Chin Wang (M'97–SM'04) was born in Taiwan in 1962. He received the B.S. degree in electrical engineering from National Taiwan University in 1984, and the M.S. and Ph.D. degree in electrical engineering from State University of New York in Stony Brook in 1988 and 1992, respectively.

In 1992, he joined the Department of Electrical Engineering, National Sun Yat-Sen University, Taiwan, R.O.C. He is currently a Professor. His recent research interests include VLSI design, low-power, and high-speed logic circuit design, neural networks, and wireless communication.

Jian-Ming Huang was born in Taiwan in 1980. He received the B.S. and M.S. degrees from the Department of Electrical Engineering, National Sun Yat-Sen University, in 2002 and 2004, respectively. He is currently working toward the Ph.D. degree in the Department of Electrical Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan, R.O.C.

His recent research interests include VLSI design, interfacing I/O circuits, and digital TV broadcasting.

Hon-Chen Cheng was born in Tainan, Taiwan, in 1979. He received the B.S. and the M.S. degrees in engineering from National Sun Yat-Sen University, Kaohsuing, Taiwan, R.O.C., in 2001 and 2003, respectively.

In 2003, he joined the Design Service Division, Taiwan Semiconductor Manufacturing Company, Ltd., Hsin-Chu, Taiwan. He has been engaged in the development of device and process technologies for submicron CMOS static memories.

Ron Hu was born in Tainan, Taiwan, in 1962. He received the B.S. degree from National Taiwan Institute of Technology, Taiwan, R.O.C., in 1987, the M.S. degree from Utah State University, Logan, in 1990, and the Ph.D. degree from State University of New York, Stony Brook, in 1994, all in electrical engineering.

He joined Holtek Semiconductor Inc., Taiwan, in 1994. He has been General Manager of Asuka Semiconductor Inc., Taiwan, since 2001. His research interests include consumer product circuit design and wireless communication.