SWITCHED-CURRENT 3-BIT CMOS WIDEBAND RANDOM SIGNAL GENERATOR[§]

Chua-Chin Wang[†] , *Yih-Long Tseng, Hon-Chen Cheng*[‡] , *and Ron Hu*[¶]

Department of Electrical Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 80424
email : ccwang@ee.nsysu.edu.tw

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 sample track-and-hold circuit is applied in the random number generator (RNG) to achieve the goal of a wide 4.0 MHz bandwidth. TSMC 0.25 μm 1P5M CMOS process is used to carry out the proposed design. The operating clock is 10 MHz, while the measured bandwidth of the generated noise is 4 MHz.

Indexing terms : random number generator, digital normalizer, current switching, white noise

1. INTRODUCTION

Real random number generators (RNG) become very demanding ever since the spread-spectrum communication market started booming [2]. They also attract very much attention in the security domain of networks and wireless communications. Prior widely used PN (pseudo-noise) codes usually have a periodicity which repeats after a large number of code symbols. Researchers have turned their attentions to hardware approaches seeking the feasibility of using circuits to implement RNGs [3], [5], [6], [7]. Three major trends of carrying out RNGs are direct amplification, oscillator sampling, and discrete-time chaos [7]. The discrete-time chaos (DTC) method is very welcomed due to its compatibility with digital systems. Two ways to implement the DTC are switched-capacitor [5], and switched-current [3]. Considering the possibility of integrating an RNG in a SOC (system-on-a-chip) IC, the switched-capacitor scheme suffers several difficulties, including large area, slow speed, large power dissipation, and sensitive to process drifting. Hence, we adopt the switched-current scheme to carry out a 3-bit RNG with a very wideband (4 MHz) using TSMC 0.25 μm 1P5M CMOS technology. The features of the proposed RNG include a 1.0 GHz linear track-and-hold (TH) circuit [4] to avoid the charge injection and channel conductance variation problem, and a digitally controllable normalizer to dynamically adjust the coefficients to prevent any divergence.

2. 3-BIT RANDOM NUMBER GENERATOR

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

$$\left\{ \begin{array}{ll} X(n+1) & = B \cdot X(n) - A \cdot \mathrm{sgn}(X(n)) \\ X(0) & = \frac{A}{B-1}, \end{array} \right. \tag{1}$$

where $X(i)$ is the i 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 is the range of [1, 2] to ensure the output $X(n)$ in the range of $[-A, +A]$. The transfer function of Eqn. (1) is shown in Fig. 1.

The slope is determined by B. An ND (nonlinear discrimination) circuit is required to carries out the sgn$(X(n))$. However, such an easy implementation suffers from a serious problem, which is that the 1-bit RNG has a sensitive dependence on initial condition after a few iterations. Meanwhile, it is proved that the distribution of iterates will be close to be uniform for B near 2. It will be not the case for $B < \sqrt{2}$, e.g., Fig. 2. That is, the generated random numbers will be "colored."

[§] This research was partially supported by National Science Council under grant NSC 91-2218-E-110-001 and 91-2622-E-110-004.

[†] the contact author, who is also the Chief Technology Officer of Asuka Semiconductor Inc., Taiwan

[‡] Mr. Cheng is a M.S. student with Institute of Communication Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan.

[¶] Dr. Ron Hu is the General Manager of Asuka Semiconductor Inc., Taiwan.

2.1. 3-bit RNG design

We proposed a modified switched-current design to eliminate the mentioned "colored" problem. Referring to Fig. 3, the digital normalizer read the generated DOUT_1, DOUT_2, and DOUT_3, to determine the slope of the next iteration, which is demoted by D_1, D_2, and D_3 The 3-bit RNG comprises three 1-bit RNGs, which are shown in Fig. 4, and one digital normalizer. The single ith one-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. The digital normalizer flattens the distribution of the probability by mapping the DOUT_i into D_i, $\forall i, i = 1, 2, 3$.

2.2. 1-bit RNG

LTH circuitry : (linear track-and hold) Fig. 5 reveals the schematic to carry out the programmability of B. CLK1 and CLK2 are two non-overlapping out-of-phase clocks. The W/L ratio 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, 1.25, respectively. Thus, the overall current can be determined by D_1, D_2, and D_3. 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_{inT_i}. M8, M9, M10, M11, M12 constitute a linear track-and-hold switch. M9 stabilizes the gate drive of M11 to prevent channel conductance input-dependent variation and the charge injection effect. The output current I_{outT_i}, in fact, denotes the $X_i(n)$ to be fed into the ND as I_{inD_i} in Fig. 6. The input current I_{inT_i} is supplied by the output current I_{outD_i} in Fig. 6.

ND circuitry : (non-linear discrimination function) Fig. 6 is the ND circuit to generate the $X_i(n+1)$ and DOUT_i for the next iteration. The function is to carry out the $\pm A\cdot$ sgn$(\cdot)$ by examining the polarity of the input current I_{inD_i}, which is the I_{outT_i} of the corresponding LTH circuit. The I_a is set to 20 μA. The inverse of D1, D2, and D3, are used to select the appropriate I_b to generate $A = I_a - I_b$.

$I_{inD_i} = I_{outT_i} > 0$: M21 and M23 are on, M22 off, to cause DOUT_i to be high. Then, M25 is also turned on. The output current is $I_{outD_i} = I_{inD_i} - (I_a - I_b)$.

$I_{inD_i} = I_{outT_i} < 0$: M22 and M24 are on, while M21 is off to make DOUT_i low. M26, thus, is on. $I_{outD_i} = I_{inD_i} + (I_a - I_b)$.

2.3. Digital normalizer

Referring to the 1-bit RNG, a total of 4 values of B can be synthesized by D_1, D_2, D_3 : 1.25, 1.5, 1.75, and 2.0 times of I_0, as shown in Table 1. 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, 1/8. A digital normalizer shown in Fig. 7 to resolve the problem by mapping the DOUT_i into D_i, $\forall i, i = 1, 2, 3$, to normalize the probability to be 1/4.

$$\begin{aligned} \mathrm{D}_3 &= \mathrm{DOUT}_3, \quad \mathrm{D}_2 = \mathrm{DOUT}_1 \qquad (2) \\ \mathrm{D}_1 &= \mathrm{DOUT}_1\mathrm{DOUT}_2 + \mathrm{DOUT}_2\mathrm{DOUT}_3 \\ &\quad + \mathrm{DOUT}_3\mathrm{DOUT}_1 \end{aligned}$$

D3 D2 D1	$\times\, I_0$
0 0 0	1.25
0 0 1	1.50
0 1 0	1.50
0 1 1	1.75
1 0 0	1.50
1 0 1	1.75
1 1 0	1.75
1 1 1	2.00

Table 1: combinations of the output current

3. SIMULATION AND IMPLEMENTATION

The overall design is implemented by TSMC 0.25 μm 1P5M CMOS process. The layout is given Fig. 8. Fig. 9 is the post-layout simulation result of the RNG transfer function. The time domain analysis for the settling time is given in Fig. 10. Fig. 11 and 12, respectively, demonstrate the generated sequence and spectrum of DOUT_1. The power drop-off occurs at 4.0 MHz. The overall characteristics of the chip is summarized in the following table.

power	30.0 mW @ 10 MHz
die size	0.259 mm^2
VDD range	2.50 V ± 10%
temperature	-25°C to +75°C
max. clock	10 MHz
output BW	4.0 MHz

Table 2: characteristics of the proposed design

4. CONCLUSION

A modified 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 numbers problem in prior designs is resolved. The coefficients of the proposed design are dynamically adjustable.

5. REFERENCES

[1] R. J. Baker, H. W. Li, and D. E. Boyce, "CMOS - circuit design, layout, and simulation," Reading: IEEE Press, 1998.

[2] C. Chien, "Digital radio systems on a chip," Reading: Kluwer Academic Publishers, 2001.

[3] M. Degaldo-Restituto, F. Medeiro, and A. Rodriguez-Vazquez, "Nonlinear switched-current CMOS IC for random signal generation," *Electronics Letters,* vol. 29, no. 25, pp. 2190-2191, Dec. 1993.

[4] D. Kakonis, and C. Svensson, "A 1 GHz linearized CMOS track-and-hold circuit," *2002 IEEE Symp. on Circuits and Systesms (ISCAS'2002),* vol. V, pp. 577-580, May 2002.

[5] A. Rodriguez-Vazquez, M. Delgado, S. Espejo, and J. L. Huertas, "Switched-capacitor broadband noise generator for CMOS VLSI," *Electronics Letters,* vol. 27, no. 21, pp. 1913-1914, Oct. 1991.

[6] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generation - part II: practical realization," *IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Applications,* vol. 48, no. 3, pp. 382-385, Mar. 2001.

[7] M. Degaldo-Restituto, and A. Rodriguez-Vazquez,, "Integrated chaos generators," *Proc. of the IEEE,* vol. 90, no. 5, pp. 747-767, May 2002.

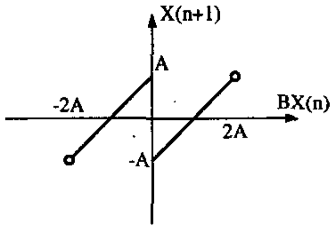

Figure 1: transfer function of 1-bit RNG

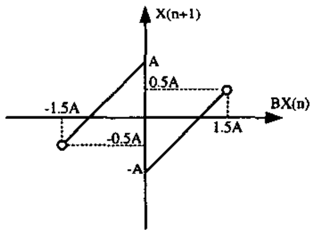

Figure 2: scenario given a smaller B

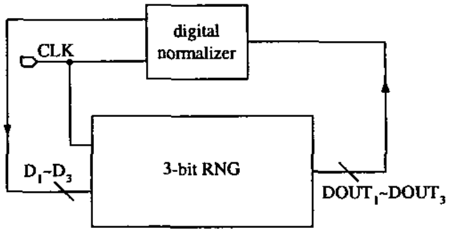

Figure 3: proposed 3-bit RNG

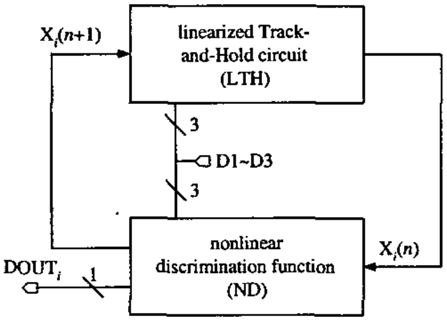
Xi(n+1)
linearized Track-and-Hold circuit (LTH)
3
D1~D3
3
DOUTi
1
nonlinear discrimination function (ND)
Xi(n)

Figure 4: proposed 1-bit RNG

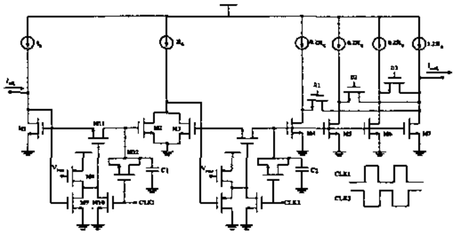

Figure 5: schematic of the LTH in the 1-bit RNG

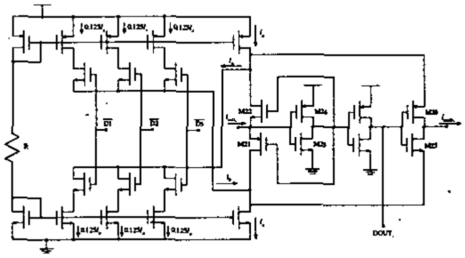

Figure 6: schematic of the ND in the 1-bit RNG

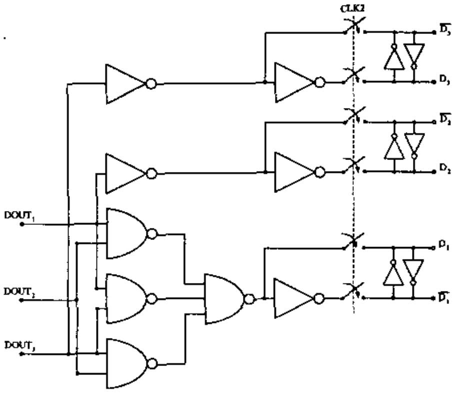

Figure 7: digital normalizer

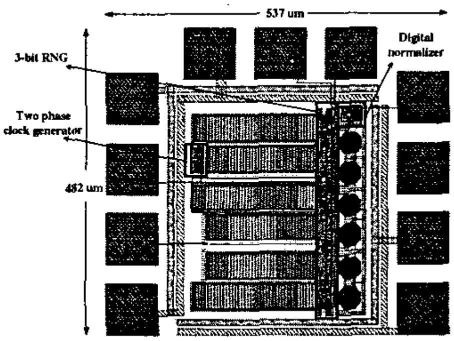

Figure 8: layout of the proposed 3-bit RNG

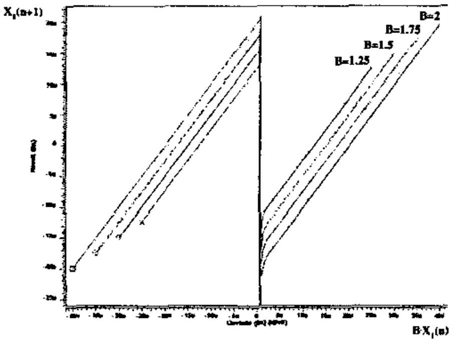

Figure 9: post-layout simulation of the transfer function

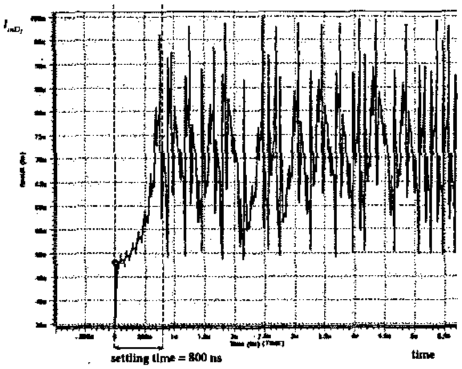

Figure 10: time domain analysis of the output

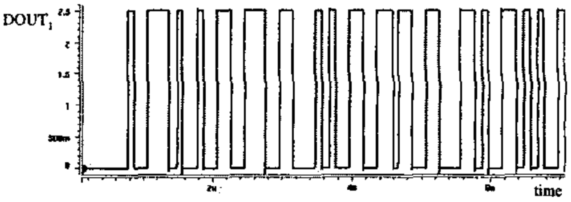

Figure 11: one of the generated sequecnces

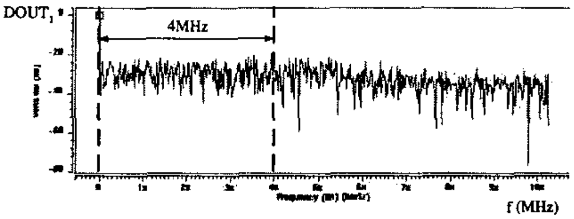

Figure 12: spectrum of the generated signals