ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.9, No.22, 1756–1761

An ultra-low-power pseudo-random number generator based on biologically inspired chaotic silicon neuron circuit

Vinaya L. Shrestha[1a)], **Qingyun Ma**[1b)], **Mohammad R. Haider**[1c)], **and Yehia Massoud**[2d)]

[1] *Department of Electrical and Computer Engineering, The University of Alabama at Birmingham, Birmingham, AL 35294*

[2] *Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609*

a) *vinaya@uab.edu*

b) *maq@uab.edu*

c) *mrhaider@uab.edu*

d) *massoud@wpi.edu*

Abstract: This work presents an ultra-low-power, biologically inspired pseudo-random number generator based on the Hodgkin-Huxley silicon neuron circuit. The chaotic phenomenon observed in neurons is exploited to generate random numbers. The random sequence generated by the proposed system passed the statistical tests specified by Federal Information Processing Standard. The proposed random number generator circuit provides an ultra-low-power alternative for pseudo-random number generation with 180 nW power consumption.

Keywords: chaos, low-power, random number generator

Classification: Electron devices, circuits, and systems

References

[1] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, March 2008.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[3] İ. Çiçek and G. Dündar, "A hardware efficient chaotic ring oscillator based true random number generator," *IEEE Int. Conf. Electronics, Circuits and Systems*, pp. 430–433, Dec. 2011.

[4] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6 –21, quarter 2001.

[5] S. Ergün, "Regional random number generator from a cross-coupled chaotic oscillator," *Midwest Symposium on Circuits and Systems*, pp. 1–4, Aug. 2011.

DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012

[6] A. Hodgkin and A. Huxley, "A quantitative description of membrane current and its application to conduction and excitation in nerve," *J. Physiol*, vol. 117, pp. 550–554, 1952.

1 Introduction

Random numbers are integral to numerous applications such as data encryption, information compression, spread spectrum systems, etc. The computations in emerging technologies such as compressive sampling involve random matrices [1]. The random numbers can be generated by using either hardware or software based random number generators (RNGs). Hardware-based RNGs utilize the randomness that occurs in physical phenomena [2], which can be used to generate random numbers [3].

Chaotic systems, which are known for deterministic randomness, can be utilized as a hardware based RNG [4]. The random nature of the chaotic signal can be exploited to obtain true random numbers [3, 5]. Since random numbers are frequently used in cryptography applications, it is necessary that they are unpredictable. A set of statistical tests are used to measure the unpredictability of random numbers. The tests defined by the Federal Information Processing Standards (FIPS)-140-1 [2] specify these requirements for randomness.

In this paper, we present a low-power biologically inspired chaotic silicon neuron based pseudo-random number generator (PRNG). The procedure for extracting random data from the chaotic output is explained. The random data generated by the chaotic circuit is tested using the FIPS-140-1 tests. The entire circuit is designed using 0.13-μm CMOS technology. Subthreshold transistors and current reuse techniques are used to achieve ultra-low-power operation.

2 Chaotic silicon neuron-based PRNG

Among several silicon neuron architectures existing in literature, the Hodgkin-Huxley (H-H) model is known to have the most accurate representation of

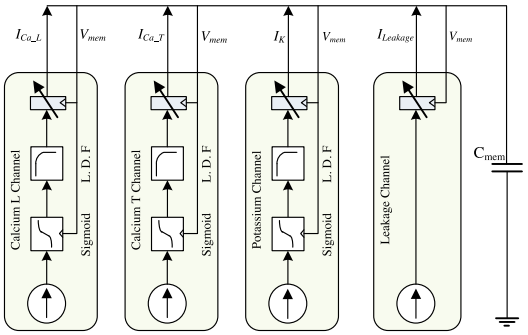


Fig. 1. Block diagram of the H-H silicon neuron-based random number generator.

DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012

the ionic dynamics present in real neurons [6]. In addition to that, the H-H model is also capable of generating chaotic signal. The H-H silicon neuron model consists of four ionic current channels, L-type and T-type calcium (Ca) channels, Potassium (K) channel, and a leakage current channel. The current channels represent the ionic flow in the cell. In our design, we modify the H-H silicon neuron model to form an autonomous chaotic oscillator, instead of an excitable silicon neuron circuit.

The block diagram representation of the H-H silicon neuron is shown in Fig. 1. The K and Ca channels are designed using a sigmoid function circuit, a low-pass filter circuit and a linear transconductance circuit. The leakage current channel, which represents current other than the ionic currents, consists only of a transconductance block. The signmoid-function circuit models the sigmoid-function like relationship between the channel current and membrane potential observed in real neurons [6]. The low-pass filter adds delay to the output current from the sigmoid-function circuit. Finally, the output current from the log domain filter manipulates the transconductance value of the linear transconductance circuit which controls the current level in the channel. The circuit schematic for the current channels in the silicon neuron circuit is shown in Fig. 2. The building blocks of each ionic current channel, the sigmoid function, log domain filter, and linear transconductance circuits are indicated using dotted area in the figure.

2.1 Bit generation

The chaotic signal is converted to a sequence of binary data using thresholding. For the chaotic signal x and threshold c, we define a threshold function

$$\sigma_c(x) = \begin{cases} 0 & \text{if } x < c \\ 1 & \text{if } x \geq c. \end{cases} \tag{1}$$

For the chaotic signal generated by our chaotic silicon neuron circuit, we use a threshold value of $c = 0.27\,V$. Since hardware-based RNGs produce biased or correlated bits [2], it is necessary to deskew the data to get unbiased random data. We use Neumann's technique to deskew the binary sequence, which can be explained by

$$b_i(\sigma_i, \sigma_{i-1}) = \begin{cases} 0 & \text{if } \sigma_i = 0 \wedge \sigma_{i-1} = 1 \\ 1 & \text{if } \sigma_i = 1 \wedge \sigma_{i-1} = 0. \end{cases} \tag{2}$$

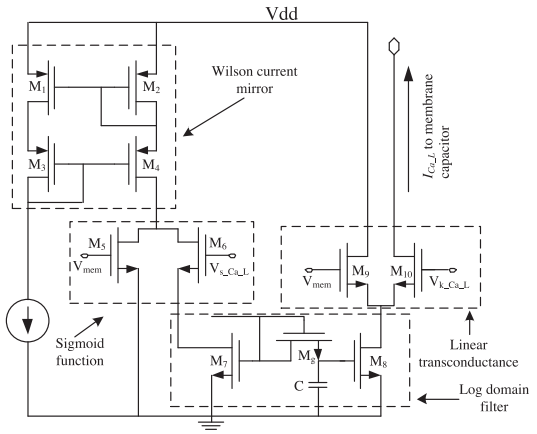
2.2 FIPS-140-1 statistical tests

The random number generated are subjected to the standardized tests specified by FIPS-140-1, which require a sequence of 20,000 bits to be tested for the mono bit, poker, runs and long-run test [2].

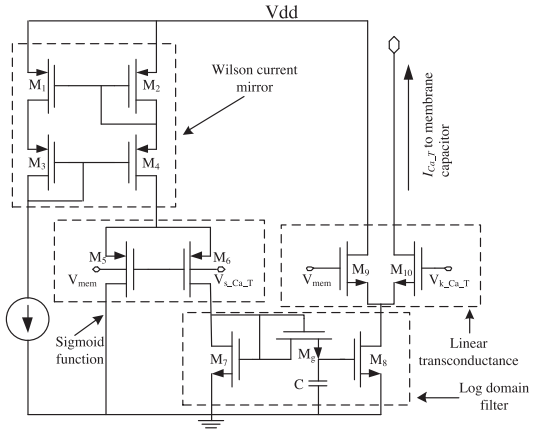
3 Results

The chaotic silicon neuron circuit has four chaotic outputs, L-type and T-type calcium currents, potassium current, and membrane potential. We utilize the chaotic membrane potential output for random number generation. Fig. 3 (a)

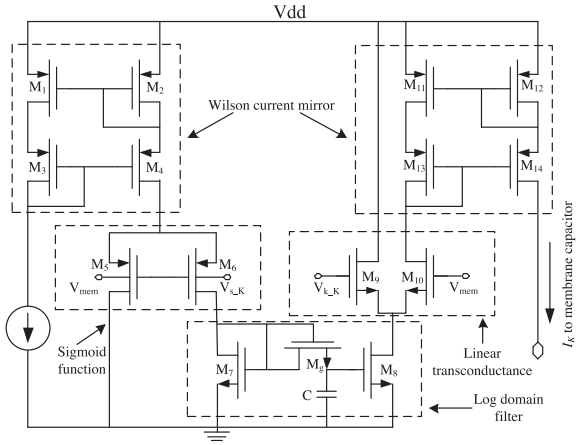
DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012



(a)



(b)

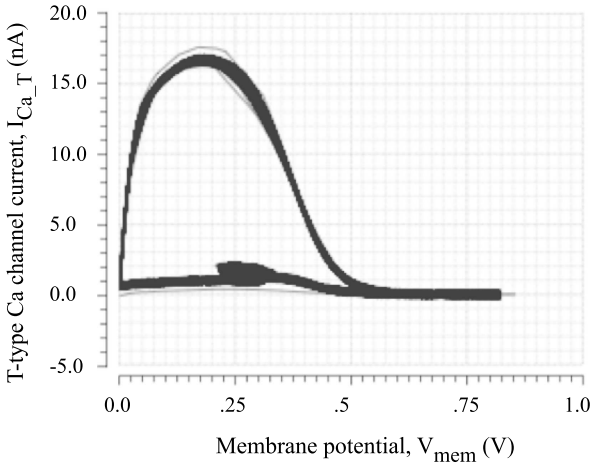


(c)

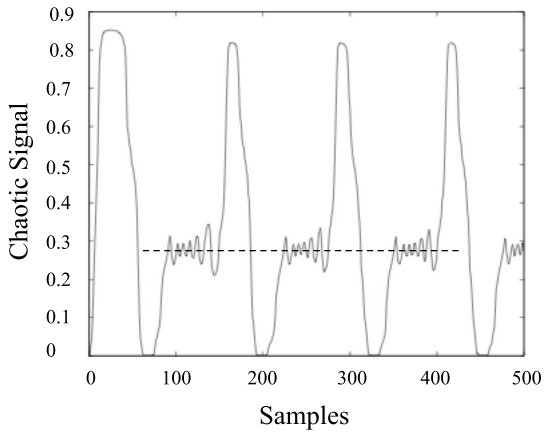
Fig. 2. Circuit schematic for the ionic current channel in the silicon neuron showing (a) L-type Ca channel (b) T-type Ca channel (c) Potassium (K) channel.

shows a scroll pattern in the phase plane plot for T-type Ca current and membrane potential, which characterizes chaotic systems. The chaotic membrane potential signal is shown in Fig. 3 (b). The rapidly changing portion of the

DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012



(a)



(b)

Fig. 3. (a) Phase plane plot for T-type Ca current against membrane potential showing a scroll pattern which characterizes chaotic systems (b) The membrane potential as the chaotic output of the random number generator circuit. This chaotic signal is used to generate random numbers using a threshold voltage of 0.27 V, indicated by the dotted line.

chaotic signal was used for random number generation using the thresholding voltage indicated by the dotted line in the figure.

The proposed chaotic circuit was simulated for a time span of 20 minutes. The binary sequence generated after thresholding was deskewed five times to get unbiased random data. A sequence of 20,000 bits was then subjected to the FIPS-140-1 tests. The random data generated by our system successfully passed those tests. Deskewing was performed five times based on empirical results as the random data passed the FIPS test only after deskewing five times. The outcomes of the FIPS-140-1 tests along with a comparison with expected outcomes, specified in [2], are shown in Tables I and II.

In Table I, N_1 refers to the number of 1's in the random sequence and

DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012

Table I. Results for the mono bit, poker and long-run tests.

Test Name	Results	
	Expected	Observed
Monobit	$9,654 < N_1 < 10,346$	$N_1 = 9,959$
Poker	$1.03 < X_3 < 57.4$	$X_3 = 22.60$
Long-run	No gaps/blocks of length ≥ 34	None

Table II. Results for the runs test.

Length of Run	Required Interval	Observed Interval	
		Gaps	Blocks
1	2267 - 2733	2599	2600
2	1079 - 1421	1268	1279
3	502 - 748	607	620
4	223 - 402	297	303
5	90 - 223	163	137
6+	90 - 223	156	151

X_3 refers to the statistic used for poker test. In Table II, a gap refers to a run of consecutive 0's and a block refers to a run of consecutive 1's.

4 Conclusion

This paper presented a biologically inspired Hodgkin-Huxley silicon neuron-based ultra-low-power random number generator. The chaotic membrane potential output from the silicon neuron circuit is utilized for random number generation. The random data generated by our system successfully passed the statistical tests required by the Federal Information Processing Standard. The proposed system consumes 180 nW and provides an ultra-low-power, biologically inspired alternative for pseudo-random number generation.

DOI: 10.1587/elex.9.1756
Received October 31, 2012
Accepted November 05, 2012
Published November 28, 2012