Design of Random Number Generation Algorithm

Dawei Li
Zhejiang University
Institute of VLSI Design
Hangzhou, China
lidw@vlsi.zju.edu.cn

Yier Jin
Zhejiang University
Institute of VLSI Design
Hangzhou, China
jinye@vlsi.zju.edu.cn

Haibin Shen
Zhejiang University
Institute of VLSI Design
Hangzhou, China
shb@vlsi.zju.edu.cn

Xiaolang Yan
Zhejiang University
Institute of VLSI Design
Hangzhou, China
yan@vlsi.zju.edu.cn

Abstract

Based upon the analysis of Random Number Generators (RNGs) which amplify noise directly, the paper proposes a new design theory to generate random number by combining noise source and chaotic transformation in analog circuit. According to the design guideline, the paper analyzes some characteristics of chaotic map, and proves the key character of smoothing. The paper also introduces how to choose parameters when employing these chaotic transformation maps and the test results of chips designed according to this method is given. Also, the proposed design can intrinsically protect the unpredictability of generated random numbers against some attacks on noise sources.

1. Introduction

Random Number Generators (RNGs) are widely used in cryptography to generate random sequences used as cipher keys, so the statistical characteristics of the sequences are important to the security of the cryptosystem. RNGs can be Mainly classified as follows: (i) based on noise amplification [1]; (ii) based on oscillator sampling [2]; (iii) based on chaos [3]. The statistical characteristics of the RNGs based on noise amplification or oscillator sampling depend on circuit noise, which is complicated and is easily affected. These RNGs are difficult to implement in high-speed field so the chaos method is being received ever increasing attention. Still, there are many theoretical problems needed to be solved. In the paper we propose a new design theory of RNGs by combining noise source and chaotic transformation. We also analyze and prove their main characteristics and counter-attack behavior.

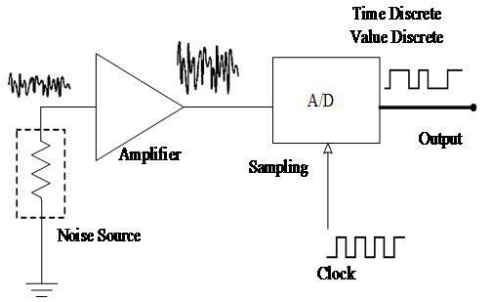

Figure 1. RNG based on noise amplification

2. Design Principles

Figure 1 is a simple RNG based on Noise Amplification: The noise from the source is amplified, sampled in discrete time, and then converted to output sequences of random numbers. It can be seen that the input of sampling is the noise amplified by amplifier, but pure noise cannot fulfill the demand of cryptography. For example, thermal noise and flicker noise of MOS transistor are main noises in CMOS IC[4]. The thermal noise statistically meets Gaussian distribution, while the flicker noise is a 1/f noise whose power spectral density is inverse ratio to frequency and its distribution is log-normal over a broad range[6]. Moreover, in real circuit, there are many interfering facts from output circumstance. So these complex noise conditions will make the final random sequence not fit for cryptography systems.

1-4244-0605-6/06/$20.00 ©2006 IEEE.

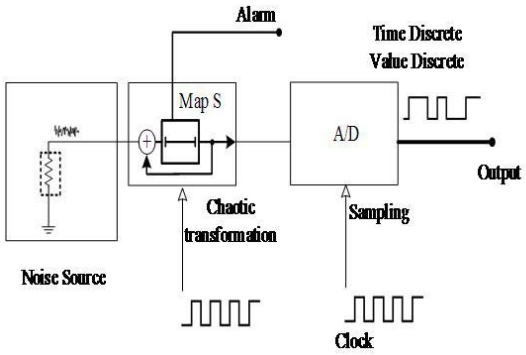

Figure 2. Noise Chaotic Transformation RNG

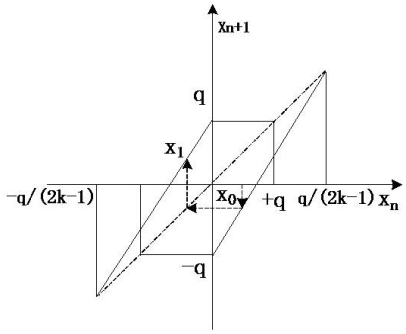

Figure 3. Point attractors and chaotic attractors of piece-wise linear map (1)

Therefore, this paper aims to improve the RNG's architecture and design theory fundamentally: Under the essential demand of RNG, there should be a natural non-deterministic process circuit(for example,noise) to gain true randomness. If the statistical characteristics of the generated random sequence do not fulfill the demand of cryptography, the chaotic transformation in analog circuit can be used for correction. The extra advantage of this transformation used to improve randomness is that real circuit parameters are not quite ideal, and the maps of transformation in chip are often different from those in theory.

Chaotic transformation circuit should fulfill some guidelines as follow. Assuming that S is the map of transformation, the input of S comes from the noise source, and the output of it is sampled subsequently.

(i)S should be a self map on $T \rightarrow T$, $T \subseteq R$, because the output of the map feeds back and is mixed with the input noise to generate next state's output.

(ii) S is time discrete, because the value of the map feed back, and the output of S is connected to discrete sampling circuit in time domain. If S is not time discrete, the statistical characteristic of the random sequence would not be improved, like the amplifier in Figure 1.

(iii) S is value sensitive, so under the effect of small noise, the trajectories of S would have a large separation which improves randomness of generated numbers.

(iv) S must have an interval of noise tolerance. Because the input of S is mixed with random noise and the characteristic of the self-map should not be destroyed.

(v) S has a key characteristic of smoothing the input to uniform distribution, so it could finally improve the statistical characteristic of the random sequence.

Figure 2 shows the structure of our Noise Chaotic Transformation RNG. Note that the alarm signal in figure 2 is used for attack detection and will be introduced later.

3. Chaotic Transformation Map

According to the design guidelines described in Section 2, we choose the following Piecewise-Linear Map (1) to achieve chaotic transformation. The Lyapunov exponent of map (1) is $\lambda = \ln(2k)$. When its trajectories are not stable, there should be $\lambda > 0$, and then $k > 0.5$. The chaotic attractor of the Map (1) is $[-q, q]$, and the point attractor is $\pm q/(2k-1)$. The chaotic attractor should be located at the interval between point attractors, i.e. $q \leq q/(2k-1)$, and then $k \leq 1$.

$$x_{n+1} = \begin{cases} 2kx_n + q, & x_n < 0, \\ 2kx_n - q, & x_n \geq 0, \end{cases} \tag{1}$$

The Map (1) has basic characteristics as follows:

(i) The Map (1) is a self map of $x_n \rightarrow x_{n+1}$.

(ii) The Map (1) is time discrete.

(iii) When $0.5 < k \leq 1$, its Lyapunov exponent $\lambda = \ln(2k) > 0$,The Map (1) is a chaotic map and the trajectories are not stable, so it is value sensitive.

(iv) The chaotic attractor of the Map (1) is $[-q, q]$, and the point attractor is $\pm q/(2k-1)$. So the distance between chaotic attractor and point attractor is $e = q/(2k-1) - q$. According to the characteristic of the Map (1), if the noise amplitude $P < e$, , the total input $x_n \pm P \in (-q-e, q+e)$, we have the next $x_{n+1} \in [-q, q]$, so the input noise will not destroy the self map, and e is the interval of noise tolerance.

(v) The Map (1) can smooth the input to uniform distribution, i.e. any initial distribution would convert to uniform distribution after infinite states. This key characteristic can be proved as below under the evolution of density function in the iterative process.

The chaotic map of (1) is denoted as S, which is a self map, having sufficient initial states: $x_1^0, x_2^0, \ldots, x_N^0$.

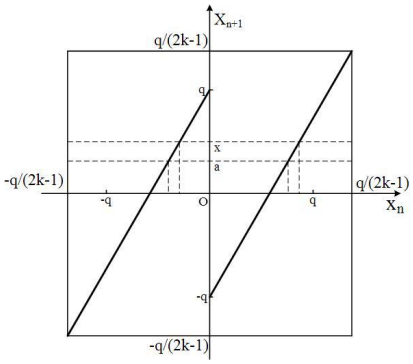

Figure 4. Counterimage of $[a, x]$ under S

The new states are transformed from the initial states under S:

$$x_1^1 = S(x_1^0),\ x_2^1 = S(x_2^0), \ldots,\ x_N^1 = S(x_N^0)$$

The characteristic function help to describe the density function as follow:

$$I_\Delta = \begin{cases} 1,\ x \in \Delta, \\ 0,\ x \notin \Delta, \end{cases} \tag{2}$$

For every interval (not too small) $\Delta_0 \subset [-q, q]$, the density function $f_0(x)$ of initial state $x_1^0, x_2^0, \ldots, x_N^0$ acts as:

$$\int_{\Delta_0} f_0(u)du \approx \frac{1}{N}\sum_{j=1}^{N} I_{\Delta_0}(x_j^0) \tag{3}$$

Likewise the density function of $x_1^1, x_2^1, \ldots, x_N^1$ is:

$$\int_{\Delta} f_1(u)du \approx \frac{1}{N}\sum_{j=1}^{N} I_{\Delta}(x_j^1) \tag{4}$$

To find a relationship between f_1 and f_0, the counterimage is introduced. For $\Delta \subset [-q, q]$, the counterimage is described as $S^{-1}(\Delta) = \{x :\ S(x) \in \Delta\}$. In the Figure 4, the counterimage of $[a, x]$ under S is the union of the two intervals.

For any $\Delta \subset [-q, q]$, we have $x_j^1 \in \Delta$, if and only if $x_j^0 \in S^{-1}(\Delta)$.

Thus we acquire the useful relation

$$I_\Delta(x) = I_{S^{-1}(\Delta)}(x) \tag{5}$$

Rewrite (4):

$$\int_{\Delta} f_1(u)du \approx \frac{1}{N}\sum_{j=1}^{N} I_{S^{-1}(\Delta)}(x_j^0) \tag{6}$$

Because Δ and Δ_0 are arbitrary intervals, it could be simply written as $\Delta_0 = S^{-1}(\Delta)$, so from (3) and (6) we can get:

$$\int_{\Delta} f_1(u)du = \int_{S^{-1}(\Delta)} f_0(u)du \tag{7}$$

When the interval $\Delta = [a, x]$, the expression of f_1 is:

$$\int_{a}^{x} f_1(u)du = \int_{S^{-1}([a,x])} f_0(u)du \tag{8}$$

Differentiate with respect to x:

$$f_1(u) = \frac{d}{dx}\int_{S^{-1}([a,x])} f_0(u)du \tag{9}$$

Hence f_1 will depend on f_0, (9) could be described as $f_1 = Pf_0$, so that:

$$Pf = \frac{d}{dx}\int_{S^{-1}([a,x])} f(u)du \tag{10}$$

According to (1), S could be transformed to $S^{-1}([a, x]) = [(a - q)/2k, (x - q)/2k] \cup [(a + q)/2k, (x + q)/2k]$, substitute (10) for $Pf = (1/2)(f(x/2k - q/2k) + f(x/2k + q/2k))$.

Likewise, P operator could be used twice for previous two states:

$$\begin{aligned} P(Pf) = P^2 f =& (1/2)^2(f(x/(2k)^2 - q/(2k)^2 - q/(2k)) \\ &+ f(x/(2k)^2 - q/(2k)^2 + q/(2k)) \\ &+ f(x/(2k)^2 + q/(2k)^2 - q/(2k)) \\ &+ f(x/(2k)^2 + q/(2k)^2 + q/(2k))) \end{aligned}$$

so that P operator could be used for previous n states:

$$P^n f = \frac{1}{2^n}\sum_{a_1, a_2, \ldots, a_n} f\left(\frac{x}{(2k)^n} + \sum_{i=1}^{n}(-1)^{a_i}\frac{q}{(2k)^i}\right), a_i \in \{0, 1\} \tag{11}$$

Equation (11) is the average of the 2^n term of the density function of counterimage, whose upper limit is $Max = q/(2k - 1)$ and lower limit is $Min = -q/(2k - 1)$. When $n \to \infty$, the counterimage will fill $[-q/(2k-1), q/(2k-1)]$ fully, and the density function of one point in $[-q, q]$ at present is equal to the average of the density functions of all points in $[-q/(2k - 1), q/(2k - 1)]$ infinite states ago. So the density function of every point in $[-q, q]$ is equal statistically, i.e. considering any distributions of initial states $x_1^0, x_2^0, \ldots, x_N^0$, after iterations of (1), the afterward states will intend to be uniform.

4. Implementation

According to section 3, in order to have a low redundancy, the value of k should be close to 1. If so, however,

Table 1. Comparison of pass rates with and without chaotic transformation in the aspects of Frequency, Block-Frequency, Cumulative-sums and Runs

NIST Test bench	Length of sequences: n	Number of sequences: m	Pass rate without transformation	Pass rate with transformation
Frequency	1000	1000	0.5250	0.9920
Block-Frequency	1000	1000	0.6530	0.9900
Cumulative-sums	1000	1000	0.5320	≥ 0.9910
Runs	1000	1000	0.7470	0.9890

the noise protection side-band $e = q/(2k-1) - q = 0$, which means the map (1) can not resistant against noise. In our implementation, we choose $k = 0.95$ and $q = 0.9$, hence, the point attractors are $q/(2k-1) = 1$ and $-q/(2k-1) = -1$, the chaotic attractor is $[-0.9, 0.9]$ and $e = 0.1$, which means the map (1) can resistant against 10% of the noise.

We use switched capacitor circuit to achieve the chaotic transformation map. The test chip was taped out under SMIC $0.18\mu m$ technology and the random number generation rate is 20 Mbps. The result of test is listed in Table 1 in which we can find that the main shortages enclosed with RNGs based on noise amplifying such as frequency, block-frequency, cumulative-sums, runs, etc. are improved significantly.

5. Conclusion

In the paper we propose a new method using analog chaotic transformation map other than digital circuit to construct a random number generator and explained its main design guidelines. To generic, this is a design by combing chaotic and noise to generate true random numbers in analog circuit. An example of piecewise linear chaotic map is given and taped out with SMIC $0.18\mu m$ process. Further work will be taken in this field. Mathematical transformation such as chaotic map will be of greater theoretical meaning in our method definitely.

References

[1] Y. H. Wang, H. G. Zhang, Z. D. Shen and K. S. Li, "Thermal Noise Random Number Generator Based on SHA-2," *Machine Learning and Cybernetics*, vol 7, 2005.

[2] N. Stefanou, S. R. Sonkusale, "High speed array of oscillator-based truly binary random number generators," *Circuits and Systems*, ISCAS '04. vol. 1, pp. I-505-8, 2004.

[3] M. E. Yalcin, J. A. K. Suykens and J. Vandewalle, "True Random Bit Generation from a Double Scroll Attractor," *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 51, no. 7, pp. 1395-1404, 2004.

[4] *Star-Hspice Mannual. Avanti Corporation*, Chapter 11 pp. 11-14, Chapter 19 pp. 102-104, 2000.

[5] C. S. Hsu and M. C. Kim, "Construction of maps with generating partitions for entropy evaluation," *Physical Review A*, 31(5): 3253-3265, 1985.

[6] E. W. Montroll and M. F. Shlesinger, "On 1/f noise and other distributions with long tails," In proceedings of the National Academy of Sciences 79:3380-3383, 1982.

[7] W. Schindler and W. Killmann, "Evaluation criteria for true random number generators used in cryptographic applications," *CHES 2002, LNCS 2523*, pp. 431-449, 2003.

[8] T. Kohda and A. Tsundeda, "Information sources using chaotic dynamics," in Chaotic Eletronics in Telecommunications, M. P. Kennedy, R. Rovatti, and G. Setti, Eds., chapter 4. CRC International Press, 2000.

[9] "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special publication 800-22, NIST, 2001.

[10] T. Tkacik, "A hardware random number generator," *CHES 2002, LNCS 2523*, pp. 450-453, 2003.

[11] V. Bagini and M. Bucci, "A design of reliable true random number generator for cryptographic applications," *1st Int. Workshop Cryptographic Hardware and Embedded Systems*, LCNS 1717, pp. 204C218, 1999.

[12] S. Callegari, R. Rovatti and G. Setti, "Efficient chaos-based secret key generation method for secure communications," *NOLTA*, 2002.

[13] F. Dachselt, K. Kelber and W. Schwarz, "Discrete-time chaotic encryption systems. III. Cryptographical analysis," *IEEE Trans. Circuit Syst.*, vol. 45, no. 9, pp. 983C988, 1998.

[14] S. Ozoguz, O. Ates and A. S. Elwakil, "An integrated circuit chaotic oscillator and its application for high speed random bit generation," *Circuits and Systems, ISCAS 2005*, vol. 5, pp. 4345-4348, 2005.

[15] A. J. Johansson and H. Floberg, "Random number generation by chaotic double scroll oscillator on chip," *Circuits and Systems, ISCAS '99*, vol. 5, pp. 407-409, 1999.

[16] M. Bucci and R. Luzzi, "Design of Testable Random Bit Generators," *CHES 2005, LNCS 3659*, pp. 147-156, 2005.