2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Cryptanalysis of a "True" Random Number Generator Based on a Double-Scroll Chaotic System

Salih Ergün†

†ERARGE - Ergünler Co., Ltd. R&D Center
Şair Nedim Cad. No:50/5, 34357, Beşiktaş, İstanbul, Turkey
Email: salih.ergun@erarge.com.tr

Abstract— An algebraic cryptanalysis of a random number generator (RNG) based on a double-scroll chaotic system is introduced. We propose an attack system in order to discover the security weaknesses of the double-scroll chaos-based RNG. Convergence of the attack system is proved using master slave synchronization scheme where the only information available are the structure of the RNG and a scalar time series observed from the chaotic system. Simulation and numerical results verifying the feasibility of the attack system are given. The chaos-based RNG does not fulfill Big Crush and Diehard statistical test suites, the previous and the next bit can be predicted, while the same output bit sequence of the RNG can be reproduced.

1. Introduction

Since people first began to exchange information with each other, they have needed to keep their private data secure. Nowadays, because of the expanding usage of electronic official & financial transactions and digital signature applications, the need for information secrecy has raised. In this manner, as a fundamental component of the secure systems, random number generators (RNGs) which have been used for only diplomatic and military cryptographic applications in the past got increasing demand for uses in a typical communication equipment.

The fact that generation of unpredictable number sequences are the core of any cryptographic system makes RNGs an unseparable part of the cryptographic mechanisms. Generation of public/private key-pairs for asymmetric algorithms and keys for symmetric and hybrid crypto systems require random numbers. The one-time pad, challenges, nonces, padding bytes and blinding values are created by using true random number generators (TRNGs). Although pseudo-random number generators (PRNGs) generate bits in a deterministic manner, pseudo-random sequences must be seeded from a shorter true random sequence in order to appear to be generated by a TRNG [2].

To fulfill the requirements for secrecy of any cryptographic applications, the TRNG must satisfy the following three secrecy criteria even if any knowledge on its design is known: 1. The previous and the next random bit must be unpredictable 2. The same output bit sequence of the TRNG must not be able to be reproduced [2] and; 3. The output bit sequence of the TRNG must pass all the statistical tests of randomness. There are four different types of TRNGs reported in the literature and these are categorized as follows: amplification of a noise source [3, 4] jittered oscillator sampling [5], discrete-time chaotic maps [6] and continuous-time chaotic oscillators [7, 8].

Although the usage of discrete-time chaotic maps for random number generation is well-known [6], it was shown recently that continuous-time chaotic oscillators can also be used to realize TRNGs [7, 8]. In particular, a "True" RNG based on a double-scroll chaotic system is proposed in [8]. In this paper we target the RNG reported in [8] and further propose an attack system to discover the security weaknesses of the targeted system. The strength of a cryptographic system almost depends on the strength of the key used or in other words on the difficulty for an attacker to predict the key. On the contrary to recent RNG design [7], where the effect of noise generated by circuit components was analyzed to address security issue, the target random number generation system [8] pointed out the deterministic chaos itself as the source of randomness.

The organization of the paper is as follows. In Section 2 the target RNG system is described in detail; In Section 3 an attack system is proposed to cryptanalyze the target system and its convergence is proved; Section 4 illustrates the numerical results with simulations which is followed by concluding remarks.

2. Target System

Chaotic systems are categorized into two groups: discrete-time or continuous-time, respectively regarding on the evolution of the dynamical systems. The double-scroll chaotic system is considered as one of the most famous continuous-time chaotic system that have ever been introduced, many designs of which were proposed starting from the use of a structure similar to Chua's oscillator. Double-scroll-like attractor which is used as the core in target random number generation system [8] is obtained from a simple model which is expressed by the Eqn. 1.

Given double-scroll chaotic system is single-parameter-controlled where a is the only parameter which contributes to the chaotic dynamics. The equations in 1 generate chaos

for the single-parameter a over a wide range ($0.48 < a < 1$) which points out that there is enough clearance for the latter. For analyzing the target RNG, the chaotic attractor is obtained from the numerical analysis of the system with $a = 0.53$ using a 4^{th}-order Runge-Kutta algorithm with an adaptive step size.

$$\begin{aligned} \dot{x_1} &= y_1 \\ \dot{y_1} &= z_1 \\ \dot{z_1} &= -ax_1 - ay_1 - az_1 + asgn(x_1) \end{aligned} \tag{1}$$

Target RNG is illustrated in Fig.1 where bit generation method is based on jittered oscillator sampling technique. As depicted in Fig.1 output of a fast oscillator is sampled on the rising edge of a jittered slower clock using a D flip-flop where the jittered slow clock is realized by the sum of triangular wave and a chaotic signal.

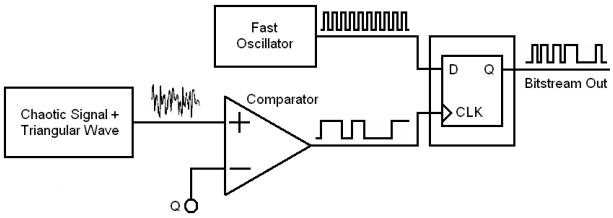

Figure 1: Target random number generation system.

In this design, if the fast and the slower clock frequencies are known as well as the starting phase difference ΔT, the output of the fast oscillator, sampled at the rising edge of the jittered slower clock, can be predicted. It can be shown that the output bit sequence $S_{(bit)i}$ is the inverse of least significant bit of the ratio between the total periods of the jittered slower clock and period of the fast clock:

$$S_{(bit)i} = \left(\frac{\lfloor \frac{(\sum_{j=1}^{i} T_{slow\ j}) - \Delta T}{T_{fast}/2} \rfloor mod 2}{(2d_{fast})}\right)' \tag{2}$$

where $T_{fast} = \frac{1}{f_{fast}}$, f_{fast}, d_{fast} are the period, frequency and the duty cycle of the fast clock, respectively, and the periods of the jittered slower clock $T_{slow\ j}$ are obtained at times t satisfying:

$$s(t) = x_1(t) + t(t) = Q with \frac{ds}{dt} > 0 \tag{3}$$

where $x_1(t)$ is the chaotic signal, $t(t)$ is the triangular wave signal and Q is the threshold value used to generate slower clock. We have numerically verified that, for high $\frac{f_{fast}}{f_{slow\ center}}$ ratios, the effect of ΔT becomes negligible and the mean value (m_{output}) of the output sequence S_{bit} approaches the fast clock duty cycle d_{fast} where frequency of the triangular-wave, corresponding to mean frequency of the jittered slower clock $f_{slow\ center}$, determines the throughput data rate (f_{rng}). It should be noted that, anyone who knows the chaotic signal output can reproduce the same output bit sequence.

The authors of [8] have preferred to use NIST 800-22 [9] statistical test suite in order to analyze output randomness of their double-scroll chaos-based RNG design. It was reported in [8] that a bit sequence of $700 \times 100 KBits$ was acquired and subjected to the NIST 800-22 statistical test suite. However, a sequence length of at least 1000000 bits is recommend in [9] and actually, a statistical test will not provide reliable results for all apparently valid input parameters such as the sequence length.

Additionally, Big Crush [10] and Diehard [11] statistical test suites which are available at the publication date of target paper [8] weren't applied to output bit stream of the target RNG. It should be noted that, the target random number generation system [8] doesn't satisfy the third secrecy criteria, which states that "RNG must pass all the statistical tests of randomness."

3. Attack System

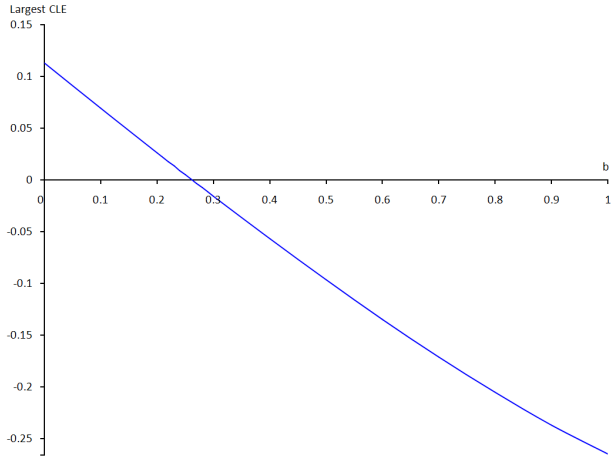

Figure 2: Largest CLEs as a function of coupling strength b.

After the seminal work on chaotic systems by Pecora and Carroll [12], synchronization of chaotic systems has been an increasingly active area of research [13]. In this paper, convergence of attack and target systems is numerically demonstrated using master slave synchronization scheme by means of feedback method [13]. In order to provide an algebraic cryptanalysis of the target random number generation system an attack system is proposed which is given by the following Eqn. 4:

$$\begin{aligned} \dot{x_2} &= y_2 \\ \dot{y_2} &= z_2 + b(y_1 - y_2) \\ \dot{z_2} &= -ax_2 - ay_2 - az_2 + asgn(x_2) \end{aligned} \tag{4}$$

where b is the coupling strength between the target (master) and attack (slave) systems and the only information available are the structure of the target random number generation system and a scalar time series observed from y_1.

In this paper, we are able to construct the attack system expressed by the Eqn. 4 that synchronizes ($x_2 \rightarrow x_1$ for

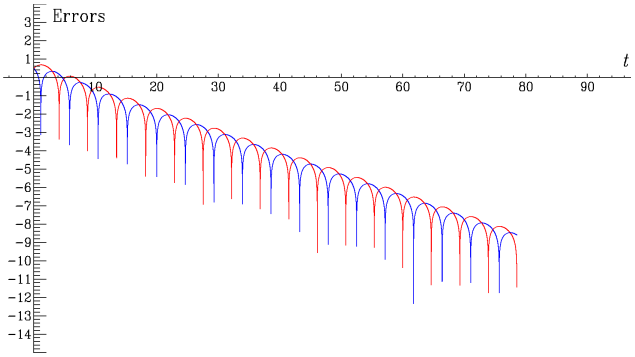

Figure 3: Synchronization errors Log $|e_x(t)|$ (red line) and Log $|e_y|$ (blue line).

$t \to \infty$) where t is the normalized time. We define the error signals as $e_x = x_1 - x_2$ and $e_y = y_1 - y_2$ where the aim of the attack is to design the coupling strength such that $|e(t)| \to 0$ as $t \to \infty$.

The master slave synchronization of attack and target systems is verified by the conditional Lyapunov Exponents (CLEs), and as firstly reported in [12], is achievable if the largest CLE is negative. In Fig.2, largest CLE graph is drawn as a function of coupling strength b while a scalar time series is observable from y_1. As drawn in the figure, when b is greater than 0.26 then the largest CLE is negative and hence identical synchronization of target and attack systems starting with different initial conditions is achieved and stable [12].(Largest CLE is -0.264907 for $b = 1$). However for b is equal to or less than 0.26, largest CLE is positive and identical synchronization is unstable.

Log $|e_x(t)|$ and Log $|e_y(t)|$ are shown in Fig.3 (for $b = 1$, where the synchronization effect is better than that of $b = 0.27$), which indicate that the identical synchronization is achieved in less than $80t$.

4. Numerical Results

We numerically demonstrate the proposed attack system using a 4^{th}-order Runge-Kutta algorithm with adaptive step size and its convergence is illustrated in Fig.3. Numerical results of $x_1 - x_2$, $y_1 - y_2$ and $z_1 - z_2$ are also given in Fig. 4, Fig. 5, and Fig. 6, respectively illustrating the unsynchronized behavior and the synchronization of target and attack systems.

It is observed from the given figures that, master slave synchronization is achieved and stable. As shown by black lines in these figures, no synchronous phenomenon is observed before $80t$. In time, the proposed attack system converges to the target system and identical synchronization is achieved where colored lines depict synchronized behaviors of chaotic states in Fig. 4, Fig. 5, and Fig. 6, respectively.

Since the identical synchronization of attack and target systems is achieved ($x_2 \to x_1$) in $80t$, the estimated value of $S_{(bit)i}$ bit which is generated according to the procedure

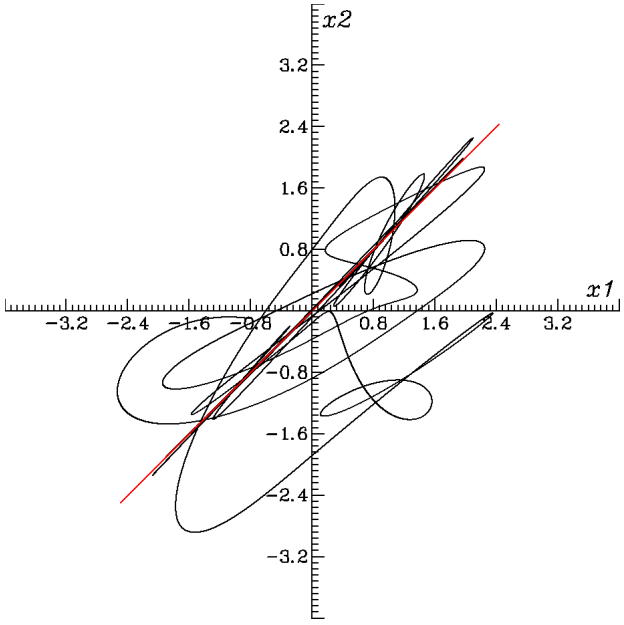

Figure 4: Numerical result of $x_1 - x_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

explained in Section 2 converges to its fixed value. As a result, it is obvious that identical synchronization of chaotic systems is achieved and hence output bit streams of target and attack systems are synchronized.

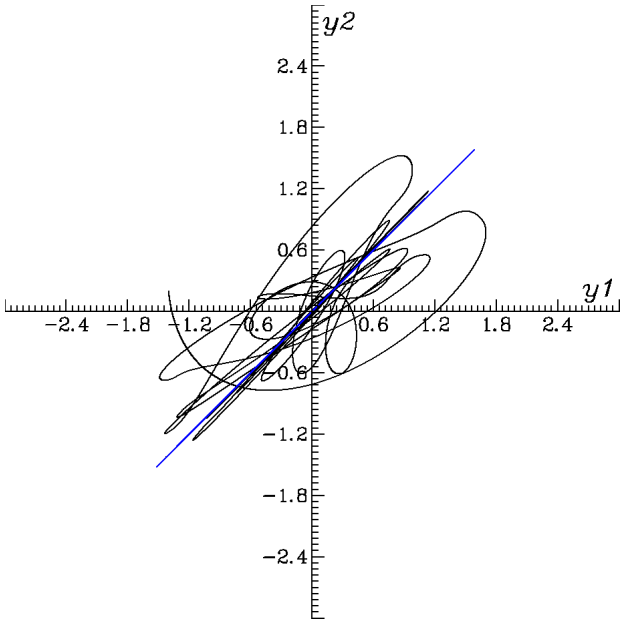

Figure 5: Numerical result of $y_1 - y_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

It is clearly shown that master slave synchronization of proposed attack system is achieved. Hence, output bit sequences of target and attack systems are synchronized. As

a result, cryptanalysis of the target random number generation system not only predicts the previous and the next random bit but also demonstrates that the same output bit sequence of the target random number generation system can be reproduced. In conclusion, the target system [8] satisfies neither the first, nor the second secrecy criteria that a RNG must satisfy.

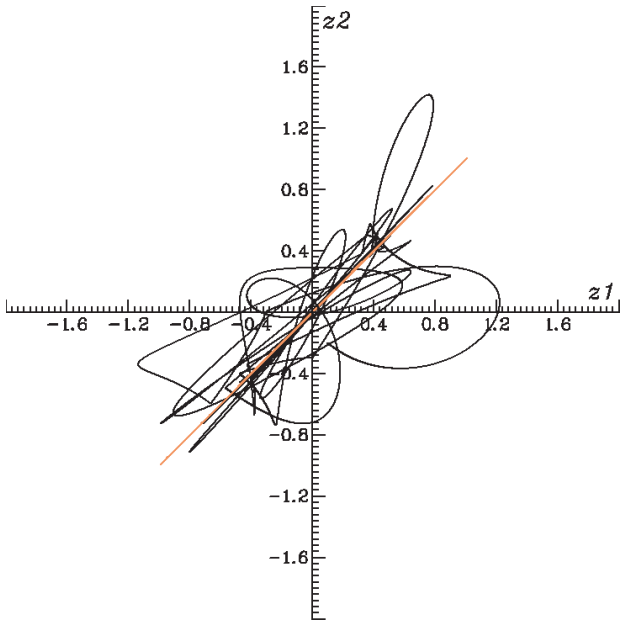

Figure 6: Numerical result of $z_1 - z_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

5. Conclusions

In this paper, we propose an algebraic attack on a random number generator (RNG) based on a double-scroll chaotic system. An attack system is introduced to discover the security weaknesses of the double-scroll chaos-based RNG and its convergence is proved using master slave synchronization scheme. Although the only information available are the structure of the target RNG and a scalar time series observed from the target chaotic system, identical synchronization of target and attack systems is achieved and hence output bit streams are synchronized. Simulation and numerical results presented in this work not only verify the feasibility of the proposed attack but also encourage its use for the security analysis of the other chaos based RNG designs. Proposed attack, renders generated bit streams predictable, thereby qualifying the target RNG to be used as a not true but pseudo random source.

References

[1] Menezes, A., Oorschot, P.van, Vanstone, S.: Handbook of Applied Cryptology. CRC Press (1996)

[2] Schneier, B.: Applied Cryptography. 2^{nd} edn. John Wiley & Sons (1996)

[3] Göv, N.C., Mıhçak, M.K. and Ergün, S.: True Random Number Generation Via Sampling From Flat Band-Limited Gaussian Processes. IEEE Trans. Circuits and Systems I, Vol. 58. 5 (2011) 1044-1051

[4] Petrie, C.S., Connelly, J.A.: A Noise-Based IC Random Number Generator for Applications in Cryptography. IEEE Trans. Circuits and Systems I, Vol. 47. 5 (2000) 615-621

[5] Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M.: A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC. IEEE Trans. Comput., Vol. 52. (2003) 403-409

[6] Callegari, S., Rovatti, R., Setti, G.: Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos. IEEE Transactions on Signal Processing, Vol. 53, 2 (2005) 793-805

[7] Ergün, S., Güler, Ü., and Asada, K., "A High Speed IC Truly Random Number Generator Based on Chaotic Sampling of Regular Waveform" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E94-A, no.1, (2011) 180-190

[8] Kılınç S., Özoğuz, S., Özdemir K., "True Random Number Generation Based on Double-Scroll Chaotic System", International Conference on Applied Electronics, Pilsen, Czech Republic, (2008) 99-102

[9] National Institute of Standard and Technology, "A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications", Available at http://csrc.nist.gov/groups/ST/toolkit/rng

[10] L'Ecuyer, P., Universit'e de Montr'eal., "Empirical Testing of Random Number Generators", 2002, Available at http://www.iro.umontreal.ca/ lecuyer/

[11] Marsalgia, G., "Diehard: A Battery of Tests of Randomness", 1997, Available at http://stat.fsu.edu/~geo/diehard.htm

[12] Pecora, L.M., Carroll, T.L., "Synchronization in chaotic systems," Physical Review Letters, vol. 64, no. 8, (1990) 821-824

[13] Hasler, M., "Synchronization principles and applications," Tutorials IEEE International Symposium on Circuits and Systems (ISCAS '94), C. Toumazou, Ed., London, England, (1994) 314-327