2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Security Analysis of a Chaos Based Random Number Generator

Salih Ergün[†]

†TÜBİTAK-Informatics and Information Security Research Center
PO Box 74, 41470, Gebze, Kocaeli, Turkey
Email: salih.ergun@tubitak.gov.tr

Abstract— This paper introduces security analysis of a chaos based random number generator (RNG). An attack system is proposed to discover the security weaknesses of the chaos-based RNG. Convergence of the attack system is proved using auto-synchronization scheme (synchronization with unknown parameters). Secret parameters of the RNG are recovered from a scalar time series where the only information available are the structure of the RNG and a scalar time series observed from the chaotic oscillator. Simulation and numerical results verifying the feasibility of the attack system are given. It is shown that deterministic chaos itself cannot be pointed out as the source of randomness.

1. Introduction

Over the last decades there has been an increasing emphasis on using tools of information secrecy. Certainly, random number generators (RNGs) have more prominently positioned into the focal point of research as the core component of the secure systems [1]. Although many people are even unaware that they are using them, we use RNGs in our daily business. If we ever drew money from a bank, ordered goods over the internet with a credit card, or watched pay TV we have used RNGs. Public/private key-pairs for asymmetric algorithms, keys for symmetric and hybrid cryptosystems, one-time pad, nonces and padding bytes are created by using RNGs [4].

Being aware of any knowledge on the design of the RNG should not provide a useful prediction about the output bit sequence. Even so, fulfilling the requirements for secrecy of cryptographic applications using the RNG dictates three secrecy criteria as a “must”: 1. The output bit sequence of the RNG must pass all the statistical tests of randomness; 2. The previous and the next random bit must be unpredictable [2] and; 3. The same output bit sequence of the RNG must not be able to be reproduced [3].

An important principle of modern cryptography is the Kerckhoff’s assumption [1], states that the overall security of any cryptographic system entirely depends on the security of the key, and assumes that all the other parameters of the system are publicly known. Security analysis is the complementary of cryptography. Interaction between these two branches of cryptology forms modern cryptography which has become strong only because of security analysis revealing weaknesses in existing cryptographic systems.

Although the use of discrete-time chaotic maps in the realization of RNG has been widely accepted for a long period of time, it has been shown during the last decade that continuous-time chaotic oscillators can also be used to realize RNGs [5, 6]. In particular, a so-called RNG based on a continuous-time chaotic oscillator has been proposed in [5]. In this paper we target the RNG reported in [5] 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 [6], where the effect of noise generated by circuit components is analyzed to address security issue, the target random number generation system [5] 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 [5] 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 $a = 0.666$ using a 4^{th}-order Runge-Kutta algorithm with an adaptive step size.

$$\begin{aligned} \dot{x_1} &= y_1 \\ \dot{y_1} &= z_1 \\ \dot{z_1} &= -a_1x_1 - a_1y_1 - a_1z_1 + a_1sgn(x_1) \end{aligned} \qquad (1)$$

Target RNG is based on periodic sampling of chaotic oscillator. Periodic samples of the state variable x_1 in Equation 1 were used. These samples are obtained at the rising edges of an external periodical pulse signal, that is at times t satisfying $wtmod2\pi = 0$ where w is the frequency of the pulse signal.

In target RNG, the distribution of periodically sampled x_1 values was initially examined to determine appropriate sections where the distribution looks like random signal. For different values of a_1 given in Equation 1, various sections were determined where the distribution of x_1 has two regions. Following this direction, bit sequence $S_{(top)i}$ and $S_{(bottom)i}$ were generated for $a = 0.666$ from regional x_1 values for regional thresholds according to the Equation 2:

$$\begin{array}{ll} S_{(top)i} = sgn(x_1i - q_{top}) & when\ x_1i \geq q_{middle} \\ S_{(bottom)i} = sgn(x_1i - q_{bottom}) & when\ x_1i < q_{middle} \\ S_{(xor)i} = S_{(top)i} \bigotimes S_{(bottom)i} & \end{array} \qquad (2)$$

where x_1i's are the values of x_1 at the 1-dimensional section, q_{top} and q_{bottom} are the thresholds for top and bottom distributions, respectively, q_{middle} is the boundary between the distributions and $\bigotimes$ is the exclusive-or operation used to generate random bit streams. It should be noted that, anyone who knows the chaotic signal output can reproduce the same output bit sequence $S_{(xor)i}$.

Numerical and experimental results verifying the correct operation of the proposed RNG were presented in [5] such that numerically generated binary sequences fulfill FIPS-140-2 test suite [7] while TRNG circuit fulfill the NIST-800-22 statistical test suite [8]. It should be noted that, the target random number generation system [5] satisfies the first secrecy criteria, which states that "TRNG must pass all the statistical tests of randomness."

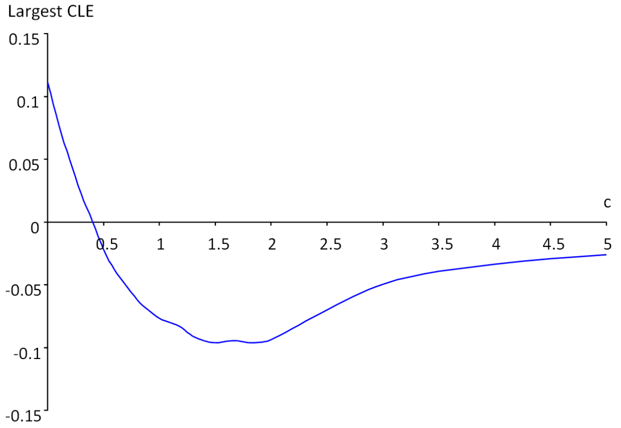

Figure 1: Largest CLEs as a function of coupling strength c.

3. Attack System

After the seminal work on chaotic systems by Pecora and Carroll [9], synchronization of chaotic systems has been an increasingly active area of research [10]. In this paper, convergence of attack and target systems is numerically demonstrated using auto-synchronization scheme [11] which is known as synchronization of chaotic systems with unknown parameters. In order to provide security analysis of the target random number generation system an attack system is proposed which is given by the following Eqn. 3:

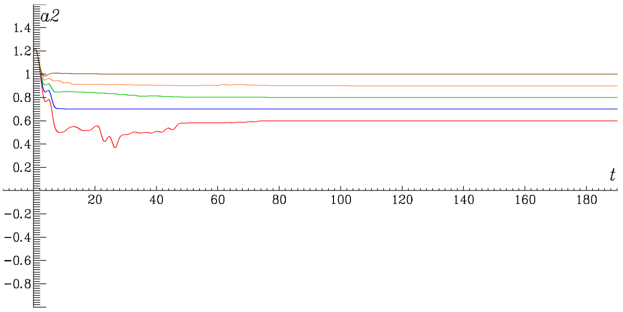

Figure 2: Convergence of the recovered parameter value a_2 of the attack system to the fixed value a_1 of the target system.

$$\begin{aligned} \dot{x_2} &= y_2 \\ \dot{y_2} &= z_2 + c(y_1 - y_2) \\ \dot{z_2} &= -a_2x_2 - a_2y_2 - a_2z_2 + a_2sgn(x_2) \\ \dot{a_2} &= -y1(y1 - y2) \end{aligned} \qquad (3)$$

where c is the coupling strength between the target and attack systems a_2 is the unknown control parameter of the target system to be estimated. The only information available are the structure of the target random number generation system and a scalar time series observed from y_1.

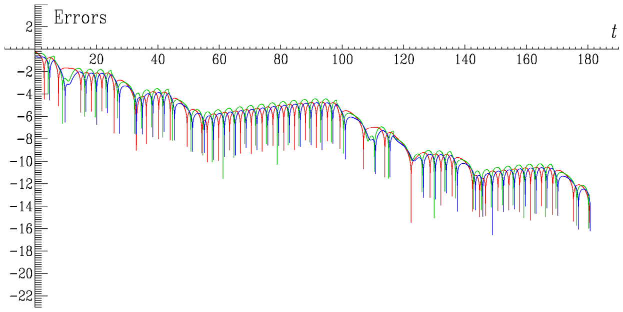

Figure 3: Synchronization errors Log $|e_x(t)|$ (red line), Log $|e_y|$ (blue line) and Log $|e_z|$ (green line).

In this paper, we are able to construct the attack system expressed by the Eqn. 3 that synchronizes ($x_2 \to x_1$ for $t \to \infty$) where t is the normalized time. We define the error signals as $e_x = x_1 - x_2$, $e_y = y_1 - y_2$ and $e_z = z_1 - z_2$ where the aim of the attack is to design the coupling strength such that $|e(t)| \to 0$ as $t \to \infty$.

The auto-synchronization of attack and target systems is verified by the conditional Lyapunov Exponents (CLEs), and as firstly reported in [9], is achievable if the largest CLE is negative. In Fig.1, largest CLE graph is drawn as a function of coupling strength c while a scalar time series is observable from y_1. As drawn in the figure, when c is greater than 0.4 then the largest CLE is negative and hence identical synchronization of target and attack systems starting with different initial conditions is achieved and stable [9]. However for c is equal to or less than 0.4, largest CLE is positive and identical synchronization is unstable.

As shown in Fig.2, the attack system converges to the parameter a_1 of the target system and auto-synchronization is achieved in less than $70t$. Log $|e_x(t)|$, Log $|e_y(t)|$ and Log $|e_z(t)|$ are shown in Fig.3 for $c = 2$, where the synchronization effect is better than that of $c = 0.4$.

4. Numerical Results

We numerically demonstrate the proposed attack system using a 4^{th}-order Runge-Kutta algorithm with fixed 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, auto-synchronization is achieved and stable. As shown by black lines in these figures, no synchronous phenomenon is observed before $70t$. 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.

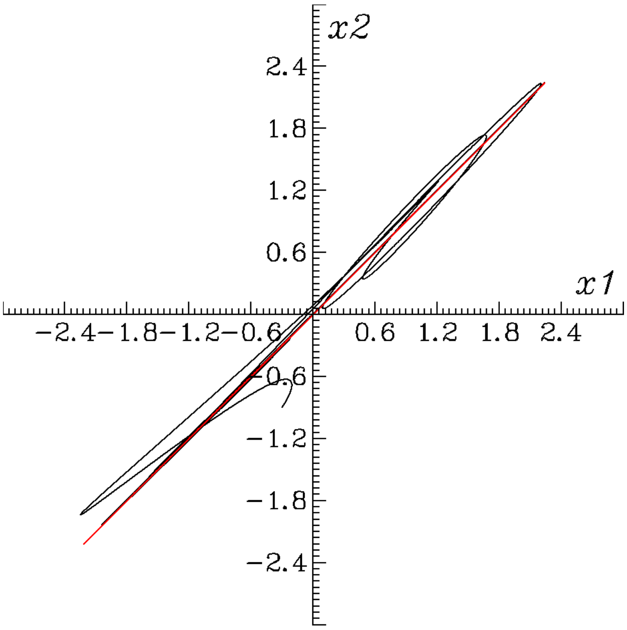

Figure 4: Numerical result of $x_1 - x_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

Since the identical synchronization of attack and target systems is achieved ($x_2 \to x_1$) in $70t$, the estimated value of $S_{(xor)i}$ bit which is generated according to the procedure 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.

It is clearly shown auto-synchronization of proposed attack system is achieved. Hence, output bit sequences of target and attack systems are synchronized. As a result, security analysis 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. Although the target random number generation system [5] satisfies the first secrecy criteria, it satisfies neither the second, nor the third secrecy criteria that a RNG must satisfy. In conclusion, deterministic chaos itself cannot be pointed out as the source of randomness.

5. Conclusions

In this paper, we propose a numerical attack on a chaos based random number generator (RNG). An attack system is introduced to discover the security weaknesses of the chaos-based RNG and its convergence is proved using auto-synchronization scheme. Although the only information available are the structure of the target RNG and a scalar time series ob-

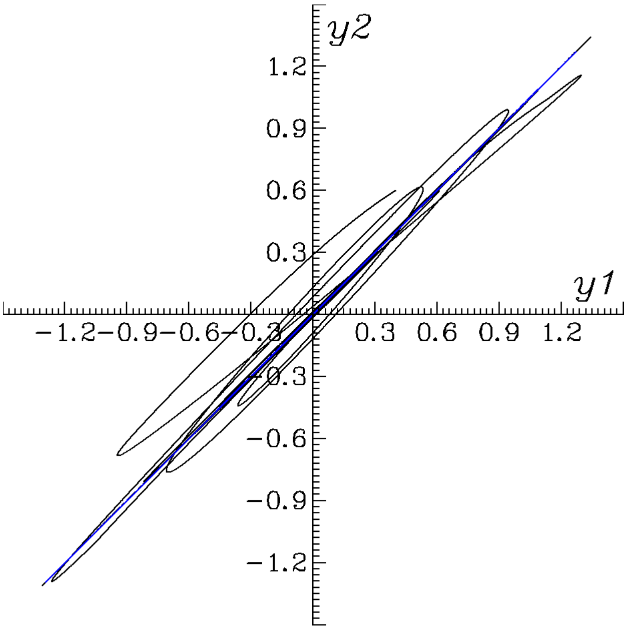

Figure 5: Numerical result of $y_1 - y_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

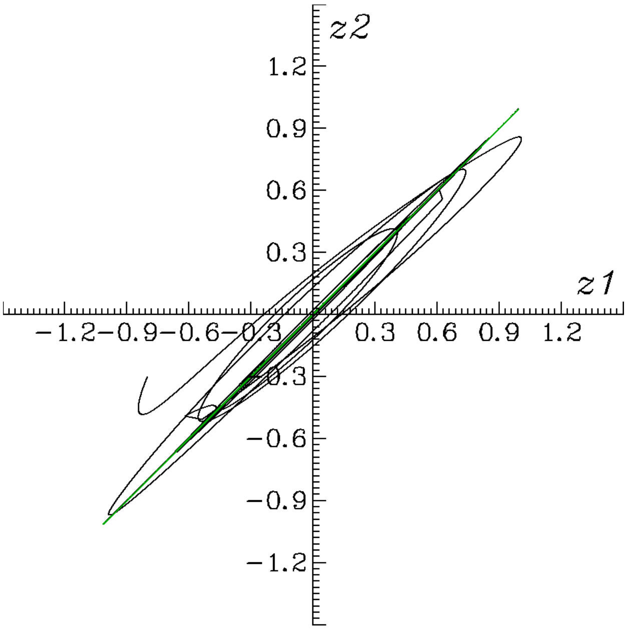

Figure 6: Numerical result of $z_1 - z_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

served from the target chaotic system, identical synchronization of target and attack systems is achieved and hence output bit streams are synchronized. Moreover, it is shown that secret parameters can be recovered by using auto-synchronization scheme. 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.

References

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

[2] Schrift, A. W., Shamir, A.: On the Universality of the Next Bit Test. Proceeding of the CRYPTO. (1990) 394-408.

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

[4] 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

[5] Ergün, S., Özoğuz, S., "Compensated True Random Number Generator Based On a Double-Scroll Attractor", International Symposium on Nonlinear Theory and its Applications, (2006) 391-394

[6] 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

[7] National Institute of Standard and Technology, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, NIST, Gaithersburg, MD 20899, (2001)

[8] 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

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

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

[11] Liu, Y., Tang W., and Kocarev L., "An Adaptive Observer Design for Auto-Synchronization of Lorenz System," International Journal of Bifurcation and Chaos, vol. 18, no. 8, (2008) 2415-2423