ON THE SECURITY OF A DOUBLE-SCROLL BASED "TRUE" RANDOM BIT GENERATOR

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

This paper is on the security of a "true" random bit generator (RBG) based on a double-scroll attractor. A clone system is proposed to analyze the security weaknesses of the RBG and its convergence is proved using master slave synchronization scheme. All secret parameters of the RBG are revealed where the only information available are the structure of the RBG and a scalar time series observed from the double-scroll attractor. Simulation and numerical results verifying the feasibility of the clone system are given such that the RBG doesn't fulfill NIST-800-22 statistical test suite, not only the next bit but also the same output bit stream of the RBG can be reproduced.

***Index Terms*—** Random number generator, continuous-time chaos, truly random, synchronization of chaotic systems, cryptanalysis

1. INTRODUCTION

In the past fifty years, due to the increasing demand of official and financial electronic transactions, the need for information secrecy has raised. Hence, cryptography which has been used for only diplomatic and military cryptographic applications in the past got expanding usage and became an everyday item used by all citizens.

All crypto systems require unpredictable values, therefore random number generator (RNG) is a fundamental component in 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 truly random number generators (TRNGs). Pseudo-random number generators (PRNGs) generate bits in a deterministic manner. In order to appear to be generated by a TRNG, the pseudo-random sequences must be seeded from a shorter truly random sequence [1].

In order to guarantee the confidentiality of a message, no useful prediction about the output of a TRNG should be made even if its design is known. To fulfill the requirements for secrecy of one-time pad, key generation and any other cryptographic applications, the TRNG must satisfy the following properties: The output bit stream of the TRNG must pass all the statistical tests of randomness; the next random bit must be unpredictable; the same output bit stream of the TRNG must not be able to be reproduced [1]. The best way to generate truly random numbers is to exploit the natural randomness of the real world by finding a random event that happens regularly [1]. Examples of such usable events include elapsed time during radioactive decay, thermal and shot noise, oscillator jitter and the amount of charge of a semiconductor capacitor.

There are few TRNG designs reported in the literature. However four different techniques were fundamentally mentioned for generating random numbers: amplification of a noise source [2], jittered oscillator sampling [3], discrete-time chaotic maps [4, 5] and continuous-time chaotic oscillators [6, 7, 8, 9]. The use of discrete-time chaotic maps in the realization of TRNG has been widely accepted for a long period of time [4, 5]. However, it has been shown during the last decade that continuous-time chaotic oscillators can also be used to realize TRNGs [6, 7, 8, 9].

In particular, a "true" random bit generator based on a continuous-time chaotic oscillator has been proposed in [6]. It is noteworthy that, [6] is the first implementation of a TRNG using a continuous-time chaotic signal which was reported with full empirical tests results. In this work we recall this paper [6] and further propose a clone system to cryptanalyze the target random number generation system [6].

The strength of a crypto system mostly 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 TRNGs [8, 9], where the effect of noise generated by circuit components was analyzed to address security issue, the target random number generation system [6] pointed out the deterministic chaos itself as the source of randomness. Note that, in recent studies [8, 9] inclusion of noise which is a nondeterministic entropy source qualifies chaos based generators to be used as a truly random source.

The organization of the paper is as follows. In Section 2

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

the target random number generation system is described in detail; In Section 3 a clone 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 RANDOM NUMBER GENERATION SYSTEM

Chaotic systems are classified into two types: discrete-time or continuous-time, respectively regarding on the evolution of the dynamical systems. In comparison with TRNGs based on discrete-time chaotic sources it is observed that TRNGs based on continuous-time chaos can be implemented using less complex and more robust structures, particularly due to the absence of successive sample-and-hold and multiplier stages.

In target random number generation system [6], a simple continuous-time chaotic system was utilized as the core of TRNG, which realizes the double-scroll-like third-order chaotic equation. The double-scroll attractor is considered as one of the most famous autonomous continuous time system that exhibit chaos.

The double-scroll attractor used in [6] is obtained from a simple model given in [10], which is expressed by the Eqn. 1. Note that when the nonlinearity is replaced by a continuous nonlinearity, the system is similar to Chua's oscillator.

$$\begin{aligned} \dot{x_1} &= y_1 \\ \dot{y_1} &= z_1 \\ \dot{z_1} &= -a_1 x_1 - a_1 y_1 - a_1 z_1 + a_1 sgn(x_1) \end{aligned} \tag{1}$$

Given third-order chaotic equation is single-parameter-controlled where a_1 is the only parameter which contributes to the chaotic dynamics. When determining parameters for which the system is chaotic, appropriate intervals should be given rather than a single parameter set as it was reported in [6].

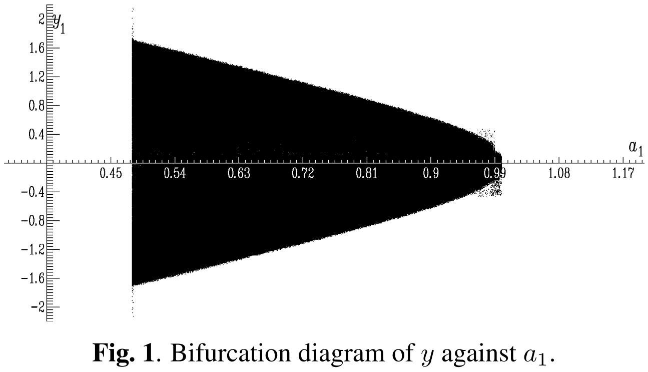

Fig. 1. Bifurcation diagram of y against a_1.

A practical design will always show parameter deviations and one should be sure that there is enough clearance for the latter. For this purpose, bifurcation diagram against the single-parameter a_1 is constructed.

As shown in Fig. 1, the equations in 1 generate chaos for the single-parameter a_1 over a wide range ($0.48 < a_1 < 1$) which points out that the non-ideal effect on the performance of the chaotic system is not critical. For example, the chaotic attractor shown in Fig.2 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.

Random number generation mechanism is also depicted in Fig.2 where bit generation method basically characterize the jumps in chaotic signal from one scroll to the other or staying at the same scroll. For this purpose, the state-space of the chaotic attractor is partitioned into three subspaces, S_0, S_M and S_1 (see Fig.2) determined by two planes located at p_0 and p_1. A bit 1 is generated when the trajectory passes from region S_M to region S_1 and a bit 0 is generated when the trajectory passes to region S_0 from region S_M.

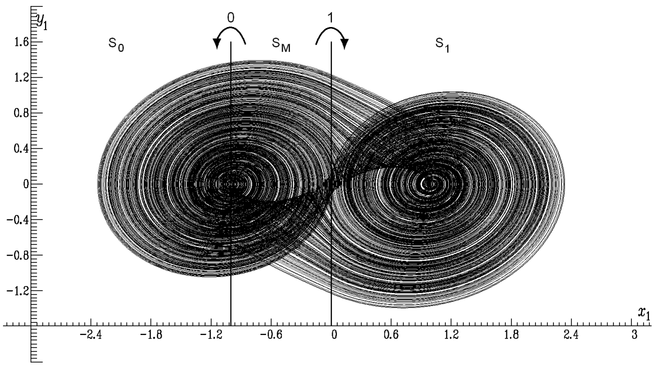

Fig. 2. Partitioning the state space into subspaces for random number generation.

However, the binary sequence thus obtained typically consists of one or two 0 for hundreds of 1, consequently it is biased. In order to remove the unknown bias in this sequence, the well-known Von Neumann's de-skewing technique is employed. Von Neumann's technique consists of converting the bit pair 01 into output 0, 10 into output 1 and of discarding bit pairs 00 and 11.

V_{p_0} and V_{p_1} are the threshold values corresponding to the dividing planes p_0 and p_1, respectively. During the experiments, V_{p_1} was set to 0 while V_{p_0} was considered as a design parameter to adjust a threshold value such that the measured entropy of the output was maximal.

In order to be robust against external interference, parameter variations and attacks aimed to force the throughput, feedback method for bias removal is a must. This is one of the major issues in TRNG circuits. The acquired raw bit sequences in [6], before postprocessing, don't present a random behavior because of too biased nature, while processed sequences can pass the test suite of Diehard thanks to Von Neumann's technique. Consequently, necessary offset compensation loop is not feasible for the reported design.

Additionally, the sample bit sequence given at http://www.esat.kuleuven.ac.be/~mey/Ds2RbG/Ds2RbG.html fails in Block-frequency, Runs and ApEn tests of NIST-800-22 test suite [11]. It should be noted that, the target random number generation system [6] doesn't satisfy the first secrecy criteria, which states that "TRNG must pass all the statistical tests of randomness."

3. CLONE SYSTEM

Since the seminal work on chaotic systems by Pecora and Carroll [12], synchronization of chaotic systems has attracted much attention. In this paper, the synchronization of target and clone systems is numerically demonstrated using the master slave synchronization scheme by means of feedback method [13]. In order to provide an algebraic cryptanalysis of the target random number generation system a clone system is proposed which is given by the following Eqn. 2:

$$\begin{aligned} \dot{x_2} &= y_2 + c(x_1 - x_2) \\ \dot{y_2} &= z_2 \\ \dot{z_2} &= -a_2x_2 - a_2y_2 - a_2z_2 + a_2sgn(x_2) \end{aligned} \tag{2}$$

where the only information available are the structure of the target random number generation system and a scalar time series observed from x_1 and c is the coupling strength between the target (master) and clone (slave) systems.

Here, we are able to construct the clone system expressed by the Eqn. 2 that synchronizes ($x_2 \to x_1$ for $t_n \to \infty$) if $a_2 = a_1$ where t_n is the normalized time. We define the error signal as $e = x_1 - x_2$, where the aim of the cryptanalysis is to design the coupling strength such that $|e(t_n)| \to 0$ as $t_n \to \infty$.

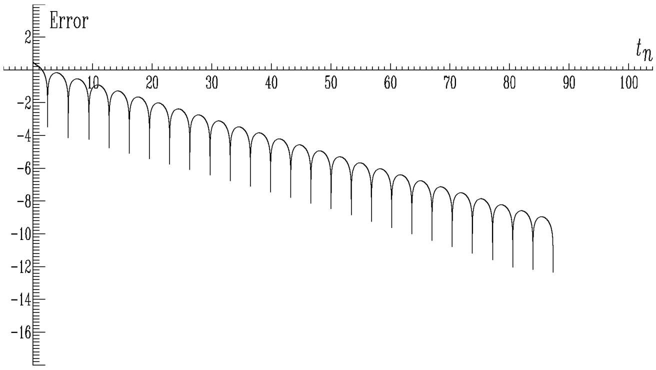

Fig. 3. Synchronization error of target and clone systems.

When c is greater than 0.33 then the largest conditional Lyapunov Exponent is negative and hence identical synchronization of target and clone systems starting with different initial conditions is achieved and stable [12]. (Largest conditional Lyapunov Exponent is -0.0380356 for $c = 0.5$ and $a_2 = a_1 = 0.666$). However for c equal to or less than 0.33, largest conditional Lyapunov Exponent is positive and identical synchronization is unstable. Log $|e(t_n)|$ is shown in Fig.3 (for $a_2 = a_1 = 0.666$ and $c = 2$, where the synchronization effect is better than that of $c = 0.5$), which indicates that the identical synchronization is achieved in less than $90t_n$.

4. NUMERICAL RESULTS

The core of random number generation system targeted in this paper is conjectured as a simple chaotic system which generate double-scroll-like chaos in the single range stated above. In order to provide identical synchronization of target and clone systems, we introduce a practical method for estimating the control parameter a_2 of the clone system.

Note that, the other information available are the possible range of a_2 ($0.48 < a_2 < 1$) and that the identical synchronization is achieved for $a_2 = a_1$. Starting from the initial condition $a_2 = 0.48$, synchronization errors of target and clone systems are investigated for a period of $90t_n$. If we observe the identical synchronization inside this period then corresponding estimation of a_2 is determined as the true value of a_1. However, if the identical synchronization cannot be achieved then corresponding estimation is increased until $a_2 = 1$.

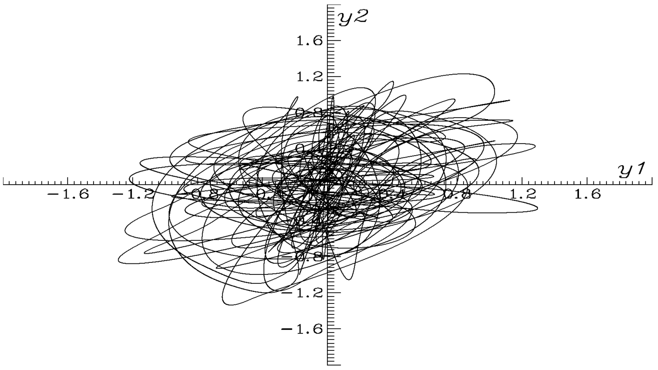

Fig. 4. Numerical result of $y_1 - y_2$ illustrating the unsynchronized behavior of target and clone systems.

We numerically demonstrate this practical method. To make clone and target systems synchronized, we continuously increase a_2 (from 0.48 to 1). As shown in Fig. 4, no synchronous phenomenon is observed when $a_2 \neq a_1$. When $a_2 = a_1$, the synchronization error is shown in Fig. 3 and numerical result of $y_1 - y_2$ is given in Fig. 5, illustrating the identical synchronization of target and clone systems.

The only parameter of the target system left to be estimated is the V_{p_0} threshold value. In order to estimate true value of V_{p_0} to make output bit streams of clone and target systems synchronized, 20 bit streams of length 1000000 bits were generated with the corresponding entropy measures for 20 candidate thresholds values. True value of V_{p_0} is therefore determined as the corresponding threshold (-1.44 in [6])

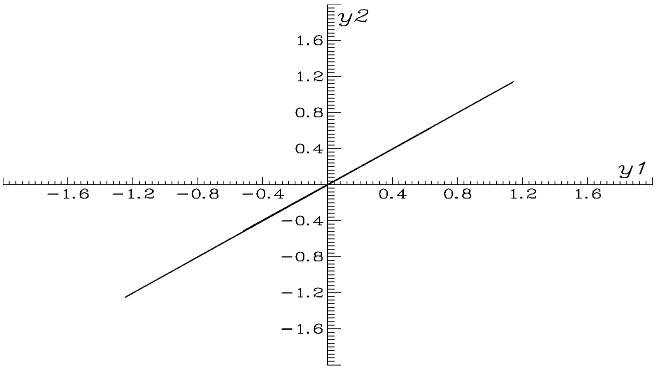

Fig. 5. Numerical result of $y_1 - y_2$ illustrating the synchronization of target and clone systems.

while the measured entropy of the output is maximal.

As a result, we show that all the secret parameters of the target random number generation system can be revealed. So it is obvious that identical synchronization of chaotic systems is achieved and hence output bit streams of target and clone systems are synchronized. In conclusion, cryptanalysis of the target random number generation system not only predicts the next random bit but also demonstrates that the same output bit stream of the target random number generation system can be reproduced by means of a proposed clone system. In this manner, the target system [6] satisfies neither the second, nor the third secrecy criteria that a TRNG must satisfy.

5. CONCLUSIONS

In this paper, we analyze the security weaknesses of a “true” random bit generator (RBG) based on a double-scroll attractor. We show that all the secret parameters can be revealed by means of a proposed clone system using master slave synchronization scheme. Although the only information available are the structure of the target RBG and a scalar time series observed from the target chaotic system, identical synchronization of target and clone 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 cryptanalysis but also encourage its use for the security analysis of the other chaos based RBG designs.

6. REFERENCES

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

[2] N.C. Göv, M.K. Mıhçak, and S. Ergün, “True Random Number Generation Via Sampling From Flat Band-Limited Gaussian Processes,” IEEE Transactions on Circuits and Systems I, vol. 58, no. 5, pp. 1044-1051, May 2011.

[3] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, “A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC”, IEEE Transactions on Computers, vol. 52, pp. 403-409, Apr. 2003.

[4] T. Stojanovski, J. Pihl, and L. Kocarev, “Chaos-Based Random Number Generators-Part II: Practical Realization,” IEEE Transactions on Circuits and Systems I, vol. 48, no. 3, pp. 382-385, Mar. 2001.

[5] S. Callegari, R. Rovatti, G. Setti, “Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos”, IEEE Transactions on Signal Processing, vol. 53, pp. 793-805, n. 2, Feb. 2005.

[6] M.E. Yalcin, J.A.K. Suykens, and J. Vandewalle “A Double Scroll Based True Random Bit Generator”, Proc. IEEE International Symposium on Circuits and Systems (ISCAS ’04), pp. 581-584, May 2004.

[7] S. Ergün, “Modeling and Analysis of Chaos-Modulated Dual Oscillator-Based Random Number Generators,” Proc. European Signal Processing Conference (EUSIPCO ’08) pp. 1-5, Aug. 2008.

[8] S. Ergün, Ü. Güler, and K. Asada, “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, pp.180-190, Jan. 2011

[9] S. Ergün, Ü. Güler, and K. Asada, “IC Truly Random Number Generators Based on Regular & Chaotic Sampling of Chaotic Waveforms” Nonlinear Theory and Its Applications, IEICE transactions, vol. 2, no. 2, pp. 246-261, 2011.

[10] A.S. Elwakil, K.N. Salama, and M.P. Kennedy, “An equation for generating chaos and its monolithic implementation,” Int. J. Bifurcation Chaos, vol. 12, no. 12, pp. 2885-2896, 2002.

[11] National Institute of Standard and Technology, “A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications”, NIST 800-22, May 2001, Available at http://csrc.nist.gov/rng/SP800-22b.pdf

[12] L.M. Pecora, T.L. Carroll, “Synchronization in chaotic systems,” Physical Review Letters, vol. 64, no. 8, pp. 821-824, Feb. 1990.

[13] M. Hasler, “Synchronization principles and applications,” Tutorials IEEE International Symposium on Circuits and Systems (ISCAS ’94), C. Toumazou, Ed., London, England, pp. 31427, 1994.