Analysis and Simulation of a Chaos-Based Random Number Generator for Applications in Security

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 presents analysis and simulation of a chaos-based random number generator (RNG) for applications in security. An attack system is proposed to discover the security weaknesses of the chaos-based RNG. Convergence of the attack system is proved using master-slave synchronization scheme. Future evaluation of the RNG is derived in which the only available information is the structure of the RNG and a scalar time series observed from the chaotic oscillator. Simulation and numerical results confirming the feasibility of the attack system are given. It has been verified that the deterministic chaos itself can not be represented as a source of random generators.

1. Introduction

In recent years there has been an increasing emphasis on the use of information security. Of course, random number generators (RNGs) have been positioned as research focal points as the key components of more specific secure systems [1]. Although many people are even unaware that they are using them, we use RNGs in our daily business. If we ever obtained money from a bank's cash dispenser, 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 crypto-systems, one-time pad, nonces and padding bytes are created by using RNGs [2].

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 dictate 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 and; 3. The same output bit sequence of the RNG must not be able to be reproduced [1].

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. Cryptanalysis is the complementary of cryptography. Interaction between these two branches of cryptology form 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 [3, 4], 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 truly 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 was 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 analysis results with simulations which is followed by randomness analysis and concluding remarks.

2. Target System

Chaotic systems are divided into two groups: discrete-time or continuous-time, respectively in terms of the evolution of dynamic systems. In target random number generation system [5], a simple non-autonomous continuous-time chaotic oscillator is used as the core component.

The aforementioned chaotic oscillator offers significant advantages over existing ones. The oscillator uses a differential pair to achieve the required nonlinearity, which is the most commonly used basic analog block due to its high IC performance. Moreover, this chaotic oscillator is balanced; Therefore, it provides better power supply rejection and noise immunity.

Using the normalized quantities in [5], the equations of the chaotic oscillator transforms into following normalized equations Eqn. 1:

$$
\begin{aligned}
&\dot{x_1} = -y_1 \\
&\dot{y_1} = (x_1 - z_1) \\
&\epsilon\dot{z_1} = (y_1 - (\alpha+\beta)z_1 + \alpha sgn(sin(\omega t)) + \\
&K\begin{cases} c_0 & if\ x_1 \geq \sqrt{\frac{c_0}{b_0}} \\ b_0 x_1\sqrt{\frac{2c_0}{b_0} - x_1{}^2} & if\ \sqrt{\frac{c_0}{b_0}} > x_1 \geq -\sqrt{\frac{c_0}{b_0}} \\ -c_0 & if\ x_1 < -\sqrt{\frac{c_0}{b_0}} \end{cases})
\end{aligned}
\tag{1}
$$

To analyze the target RNG, the chaotic attractor is obtained from the numerical analysis of the system with the ideal parameter set, which is determined as the centers of the widest parameter ranges where the system is chaotic. These ideal parameters are $c_0 = 1.9$, $\alpha = 3$, $\beta = 8$, $\omega = 1.11$, $b_0 = 0.5$, $\epsilon = 0.1$ and $K = 15$.

The target RNG obtains binary random bits using the stroboscopic Poincaré map of the chaotic system given in Eqn. 1. In the target paper [5], distribution of x_1 values in the stroboscopic Poincaré map were initially examined along one period of the external periodical pulse signal.

For different parameter set, appropriate Poincaré sections were determined where the distribution of x_1 has two regions. Following this direction, appropriate Poincaré map was obtained for $\omega t mod 2\pi = 0.55$, and corresponding bit sequence $S_{(top)i}$, $S_{(bottom)i}$ were generated from regional x_1 values for regional thresholds according to the Eqn. 2:

$$
\begin{aligned}
&S_{(top)i} = sgn(x_1 i - q_{top}) && when\ x_1 i \geq q_{middle} \\
&S_{(bottom)i} = sgn(x_1 i - q_{bottom}) && when\ x_1 i < q_{middle} \\
&S_{(xor)i} = S_{(top)i} \bigotimes S_{(bottom)i}
\end{aligned}
\tag{2}
$$

where $x_1 i$'s are the values of x_1 at the Poincaré section, q_{top} and q_{bottom} are appropriately chosen thresholds for top and bottom distributions, 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 outputs x_1 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 [5] while TRNG circuit fulfill the NIST-800-22 statistical test suite [5]. It should be noted that, the target random number generation system satisfies the first secrecy criteria, which states that "TRNG must pass all the statistical tests of randomness."

3. Attack System

After the seminal work on chaotic systems by Pecora and Carroll [7], synchronization of chaotic systems has been an increasingly active area of research. In this paper, convergence of attack and target systems is numerically demonstrated using master-slave synchronization scheme [8]. In order to provide cryptanalysis of the target random number generation system an attack system is proposed which is given by the following Eqn. 3:

$$
\begin{aligned}
&\dot{x_2} = -y_2 + a(x_1 - x_2) \\
&\dot{y_2} = (x_2 - z_2) \\
&\epsilon\dot{z_2} = (y_2 - (\alpha+\beta)z_2 + \alpha sgn(sin(\omega t)) + \\
&K\begin{cases} c_0 & if\ x_2 \geq \sqrt{\frac{c_0}{b_0}} \\ b_0 x_2\sqrt{\frac{2c_0}{b_0} - x_2{}^2} & if\ \sqrt{\frac{c_0}{b_0}} > x_2 \geq -\sqrt{\frac{c_0}{b_0}} \\ -c_0 & if\ x_2 < -\sqrt{\frac{c_0}{b_0}} \end{cases})
\end{aligned}
\tag{3}
$$

where a is the coupling strength between the target and attack systems. The only information available are the structure of the target random number generation system and a scalar time series observed from x_1.

In this paper, we are able to construct the attack system expressed by the Eqn. 3 that synchronizes ($x_2 \rightarrow x_1$ for $t \rightarrow \infty$) 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 $|e(t)| \rightarrow 0$ as $t \rightarrow \infty$.

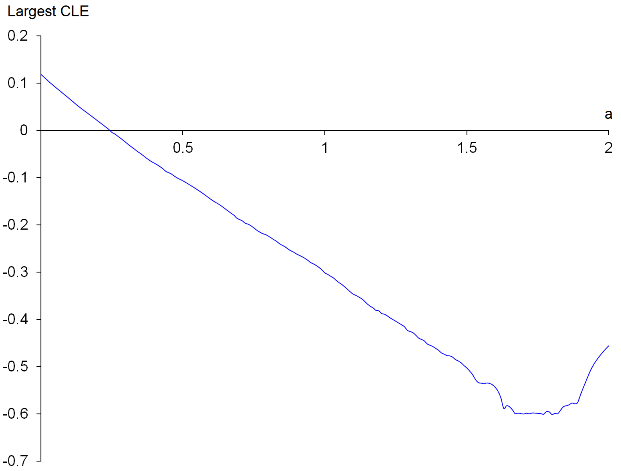

Figure 1: Largest CLE chart as a function of coupling strength a.

The master-slave synchronization of attack and target systems is verified by the conditional Lyapunov Exponents (CLEs), and as firstly reported in [7], is achievable if the largest CLE is negative. Largest CLE chart is plotted in Fig.1 as a function of coupling strength a. When a is greater than 0.24 then the largest CLE is negative and hence identical synchronization of target and attack systems starting with different initial conditions is achieved and stable [7]. (Largest conditional Lyapunov Exponent is -0.0257856 for $a = 0.3$). However for a is equal to or less than 0.24, largest CLE is positive and identical synchronization is unstable.

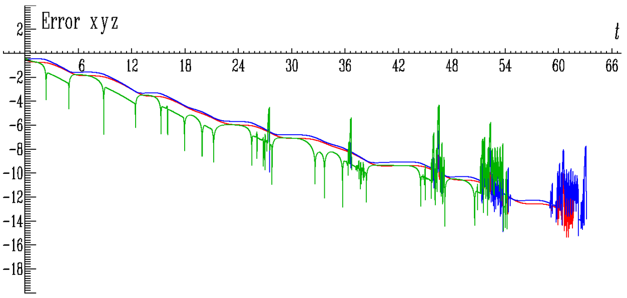

Figure 2: Synchronization errors Log $|e_x(t)|$, Log $|e_y(t)|$ and Log $|e_z(t)|$.

Log $|e_x(t)|$, Log $|e_y(t)|$ and Log $|e_z(t)|$ are shown in Fig.2 by red, blue and green lines respectively, for $a = 2$, where the synchronization effect is better than that of $a = 0.3$. As shown in the given figure, the attack system converges to target system and master-slave synchronization is achieved in less than 65 normalized time.

4. Numerical Results

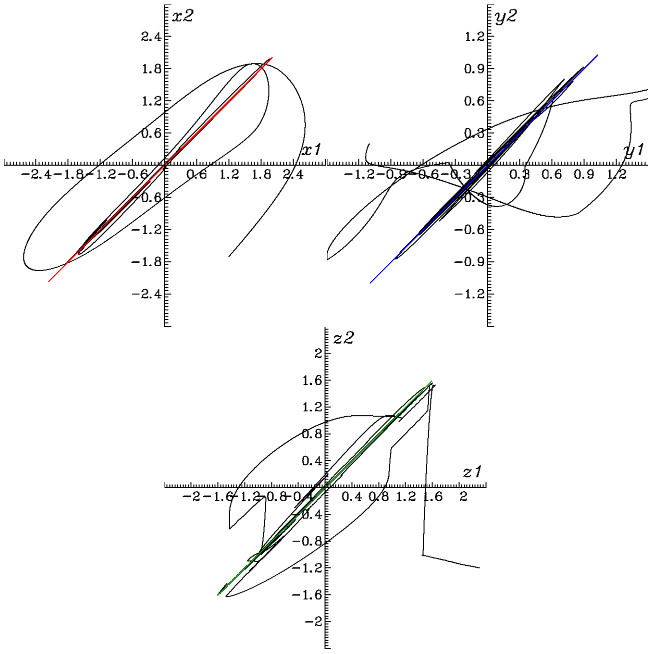

Figure 3: Numerical result of $x_1 - x_2$ and $y_1 - y_2$ illustrating the unsynchronized behavior and the synchronization of target and attack systems.

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.2.

Numerical results of $x_1 - x_2$, $y_1 - y_2$ and $z_1 - z_2$ are also given in Fig. 3, 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 initially (before $65t$). Afterwards, 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. 3, respectively.

Since the identical synchronization of attack and target systems is achieved ($x_2 \rightarrow x_1$) in $65t$, the estimated values of x_1, and $S_{(xor)i}$ bit which is generated according to the procedure explained in Section 2 converge to their corresponding fixed values. 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 master-slave synchronization of proposed attack system is achieved. Hence, output bit sequences of target and attack systems are synchronized. As a result, analysis and simulation 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, there is ambiguity at the point of satisfying the second, and the third secrecy criteria that a RNG must satisfy. In conclusion, the deterministic chaos itself can not be represented as a source of random generators.

5. Randomness Analysis

As opposed to previous RNG designs [5] where deterministic chaos itself was identified as the source of randomness, this work investigates the effect of noise on the chaotic trajectories and addresses it as the nondeterministic entropy source of a chaos based RNG. Here, it has been seen that initial values of voltages and currents of circuit components are definitely random. Starting from a random initial condition chaotic trajectory, which also contains a nondeterministic component that is comprised of noise, alters exponentially.

Circuit realization of the target chaotic oscillator is depicted in [5], where random numbers are generated by converting the voltage V_1 (which corresponds to the variable x_1) into binary sequences (given in Fig. 15 of [5]). LM211 comparators are used for this analog to digital conversion process. An FPGA based hardware which has a PCI interface was designed to upload the binary data to the computer.

To obtain x_1 values in the stroboscopic Poincaré section, external periodical pulse signal $v_p(t)$ was used. In an appropriate Poincaré section, that is $35\mu s$ before the rising edges of $v_p(t)$, output bit stream of the comparators were sampled and stored in binary format. Exclusive-or operation was also implemented inside the FPGA and after exclusive-or operation, random numbers were uploaded to the computer through the PCI interface.

The effect of equivalent noise on the chaotic waveform V_1 is analyzed for addressing security issues and evaluating unpredictability of the generator. AC response of the target chaotic oscillator circuit (given in Fig. 1 of [5]) realized by using discrete components is obtained by CAD simulations and f_C which limits the bandwidth of the chaotic waveform V_1 is determined as 36 MHz. Then, equivalent noise generated by the RNG core on V_1 is analyzed which results $V_{noise(1)} = 48\mu V_{rms}$ noise voltage on V_1 under given bandwidth.

Having a positive Lyapunov exponent, making the chaotic system starting at $V_1(0) \pm 48\mu V_{rms}$ ends up with completely different output. Initial values of capacitor voltages given in Fig. 1 of [5] are regarded to be random. The chaotic trajectory, which starts from a random initial condition and contains a non-deterministic component, which is comprised of $\pm 48\mu V_{rms}$, alters exponentially. Finally, transient analysis results show the effect of equivalent noise voltage on the chaotic waveform V_1. From a time $\tau_x = 23ns$ on, since $V_{noise(1)}$ is non-deterministic chaotic waveform V_1 ends up with completely different output. By this way, the generated bit stream becomes non-deterministic.

In [5], frequency of $v_p(t)$ which is the sampling rate of V_1 was reported as $17.66kHz$ where the sampling period effectively becomes $56.625\mu s$ which is $\approx 2460\tau_x$. By including equivalent noise $V_{noise(1)}$ generated by circuit components, generated bit streams become unpredictable, and therefore the proposed number generator is qualified as a truly RNG. In conclusion, deterministic chaos itself cannot be identified as the source of randomness but the equivalent noise generated by circuit components. As a result, any one who considers deterministic methods of producing random numbers is on the wrong track.

6. Conclusions

In this paper, we propose a method for security analysis and simulation of 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 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. Moreover, the effect of equivalent noise on the chaotic trajectory is analyzed. Although the target RNG is based on deterministic chaos, which means that an observer can predict the future evolution of the chaotic system, it is shown in this paper that inclusion of noise renders the subsequent bit unpredictable. Analysis and simulation results presented in this paper not only verify the feasibility of the proposed method but also encourage its use for the cryptanalysis of the other chaos based RNG designs.

References

[1] Schneier, B.: Applied Cryptography. 2. edn. John Wiley & Sons (1996)

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

[3] Stojanovski, T., Kocarev, L. "Chaos-Based Random Number Generators-Part I: Analysis", IEEE Trans. Cir. and Sys. I, Vol. 48, 3 (2001) 281-288

[4] 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

[5] Ergün, S., Özoğuz, S., "Truly Random Number Generators Based On Non-Autonomous Continuous-time Chaos," Int. J. Circ. Theor. Appl., DOI: 10.1002/cta.520, (2008) 1-24

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

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