PREDICTING THE SECRET PARAMETERS OF A CHAOTIC RANDOM NUMBER GENERATOR FROM TIME SERIES

Salih Ergün

ERGTECH Research Center
Zürich, Switzerland
Email: salih.ergun@ergtech.ch

ABSTRACT

A novel predicting system is proposed to find out the security weaknesses of a chaotic random number generator (RNG). Convergence of the predicting system is proved using auto-synchronization. Secret parameter of the target chaotic RNG is revealed where the public information are the design of the chaotic RNG and a scalar time series observed from the target chaotic system. Simulation and numerical results verifying the feasibility of the predicting system are given such that, next bit can be predicted while the same output bit sequence of the chaotic RNG can be regenerated.

Index Terms— Chaotic system, chaos, random number generator, time series, predicting, security weaknesses, secret parameters

1. INTRODUCTION

Today's technological developments emphasize the necessities in the following field of circuits and systems: Small area occupation, secure architecture design, low power consumption and high speed operation. In connection to this, high speed and more secure random number generators (RNG) [1] are positioned more clearly in the heart of the research as the main components of the security systems [2].

Having any knowledge about the structure of the RNG must not provide a useful prediction of the output bit sequence of the RNG. Even so, fulfilling the requirements for the confidentiality of security systems using RNG requires three privacy criteria as a must: 1. The RNG must fulfill all statistical randomness tests; 2. The preceding and following random bits can not be predicted [3] and; 3. Anyone should not generate the same output bit sequence of the RNG [4].

One of the basic principle of the cryptography is that according to Kerckhoff's hypothesis [2], it is assumed that the overall security of any crypto system is completely dependent on the security of the key, and that all other parameters of the crypto system are publicly observable. Vulnerability analysis is complementary to cryptography. The interaction between these two cryptology branches creates a contemporary cryptography that becomes stronger due to the vulnerability analysis that reveals the weaknesses of the existing crypto systems.

It has been acknowledged nowadays that, continuous-time chaotic oscillators can also be used to implement RNGs [8, 10, 11, 12], such as discrete-time chaotic maps [5, 6, 7]. In particular, a hybrid RNG sourced from a chaotic "true" RNG has been proposed in [8]. In this article, we target the chaotic RNG reported in [8], and propose a predicting system to analyze security vulnerabilities of the targeted RNG.

The robustness of a crypto system depends on the key used, or in other words, the attacker's ability to predict the key. The target RNG [8] defines the deterministic chaos as the true source of randomness, contrary to the latest RNG designs [11, 12] in which the equivalent noise generated by circuit components is analyzed.

The organization of the article is as follows. In Section 2 the chaotic RNG is explained in detail; In the next Section 3 a predicting system is proposed for vulnerability analysis of the targeted chaotic RNG and its feasibility is verified; Section 4 describes the numerical and simulation results that are followed by the conclusion section.

2. TARGET SYSTEM

Chaotic systems can be categorized into two groups: In relation to the evolution of underlying dynamical system, one is discrete time and the other is continuous time.

The target paper [8] proposed a hybrid RNG sourced from a chaotic "true" RNG. The chaotic "true" RNG was developed by using a simple continuous-time chaotic system [9] and implemented in FPGA. The analysis of the chaotic system [9] proposed by J. C. Sprott yields the state equations given in [8] which transforms into the following equation:

$$\begin{aligned} \dot{x_1} &= a_1 x_1 + z_1 \\ \dot{y_1} &= z_1 x_1 - y_1 \\ \dot{z_1} &= -x_1 + y_1 \\ \dot{a_1} &= 0 \end{aligned} \tag{1}$$

The equations in 1 generate chaos for the single-parameter a_1 in a large region. The chaotic attractor used for numerical

analysis is shown in Fig. 1 for $a_1 = 0.40$ using the 5^{th}-order Runge-Kutta Butcher algorithm with fixed step size. Note that, the last term in the given equation was added for the ease of mathematical operations.

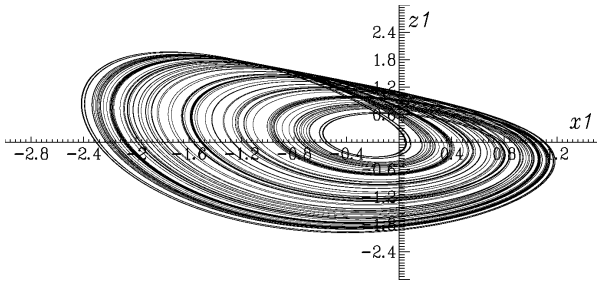

Fig. 1. The chaotic attractor used for numerical analysis of the chaotic system for $a_1 = 0.40$.

Random number generation method was explained in [8] where the mechanism is fundamentally based on analysis of the chaotic system by using a numerical method. Initially given chaotic system is implemented in Virtex-6 evaluation platform by Xilinx ISE design suite using 5^{th}-order Runge-Kutta Butcher algorithm with fixed step size τ.

By this way time series data are obtained for x_1, y_1 and z_1 chaotic state variables in τ steps. Then, the threshold values denoted by σ are adaptively calculated for x_1, y_1 and z_1 and used in the following equation to convert time series data into random bits RS where $RS(x_1, y_1, z_1) = 0$ for $x_1, y_1, z_1 < \sigma$ and $RS(x_1, y_1, z_1) = 1$ for $x_1, y_1, z_1 \geq \sigma$.

Finally, bitwise XOR operation is applied to the random bits and the state matrix given in [8] in order to generate the chaotic RNG output binary sequence S_{bit}. The authors of [8] have preferred to use NIST 800-22 [13] statistical test suite in order to analyze output randomness of their chaotic RNG design.

However, Big Crush [14] and Diehard [15] statistical test suites weren't applied to output bit stream of the RNG. Note that, the target RNG [8] do not fulfill the first secrecy criteria, which states that "TRNG must pass all the statistical tests of randomness."

3. PREDICTING SYSTEM

Since the ground-breaking paper of Pecora and Carroll, the synchronization of chaotic systems has become an increasingly sought-after field of research [16]. In this article, the convergence of the predicting and target systems is proven using the auto-synchronization, (synchronization of chaotic systems with secret parameters) [17]. In order to analyze vulnerability of the target chaotic RNG, a predicting system given by the following equation 2 is proposed:

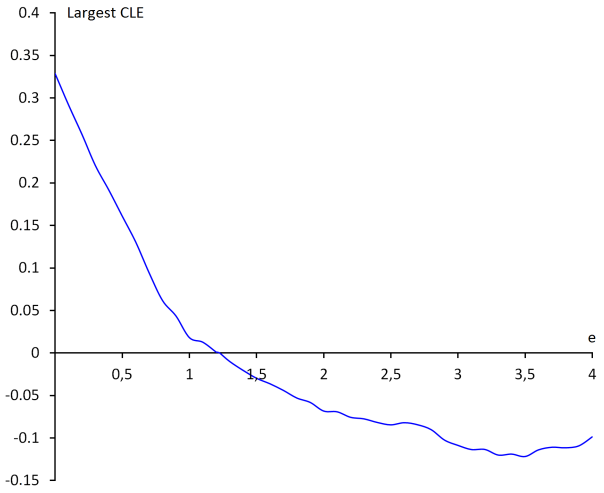

Fig. 2. Largest Conditional Lyapunov Exponents as a function of coupling strength e.

$$\begin{aligned} \dot{x_2} &= a_2 x_2 + z_2 + e(x_1 - x_2) \\ \dot{y_2} &= z_2 x_2 - y_2 \\ \dot{z_2} &= -x_2 + y_2 \\ \dot{a_2} &= y_2(x_1 - x_2) \end{aligned} \tag{2}$$

where e is the coupling strength between the target and predicting systems and a_2 is the secret control parameter of the target system to be revealed. The information available are the structure of the target RNG system and a scalar time series given by a observable where x_1 is the observable chaotic signal given in 2.

For analyzing the stability of auto-synchronization, we numerically calculate the Conditional Lyapunov Exponents (CLE) using standard 4^{th}-order Runge-Kutta algorithm with fixed step size. CLEs for the predicting system are calculated from the set of ordinary differential equations given in Eqn. 2 where QR decomposition method [18] is used. Numerical Jacobian is exploited which is calculated numerically by using finite differences. Offset for numerical Jacobian = $10^{-0.008}$ and integration time step is 0.004 while integration steps per Jacobian map is 50.

In Fig.2, we plot largest CLEs as a function of coupling strength e. As shown in this figure, when e is greater than 1.22 then the largest CLE is negative and hence auto- synchronization of target and predicting systems is achieved and stable. For any e less than or equal to 1.22, largest CLE is positive and auto-synchronization is unstable.

4. NUMERICAL RESULTS

In this article, we numerically demonstrate the proposed predicting system using standard 5^{th}-order Runge-Kutta Butcher

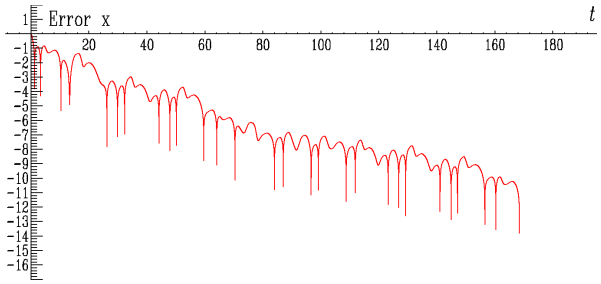

Fig. 3. Synchronization error Log $|e_x(t)|$ (red line).

algorithm with fixed step size. The predicting system expressed by the Eqn. 2 is designed that converges to target system as $x_2 \rightarrow x_1, y_2 \rightarrow y_1, z_2 \rightarrow z_1$ where $t \rightarrow \infty$ and t is the normalized time. Error signal a, x, y, and z of the auto-synchronization are defined as $e_a = a_1 - a_2$, $e_x = x_1 - x_2$, $e_y = y_1 - y_2$ and $e_z = z_1 - z_2$ respectively. Here proposed predicting system aims to find out appropriate coupling strengths such that $|e(t)| \rightarrow 0$ when $t \rightarrow \infty$.

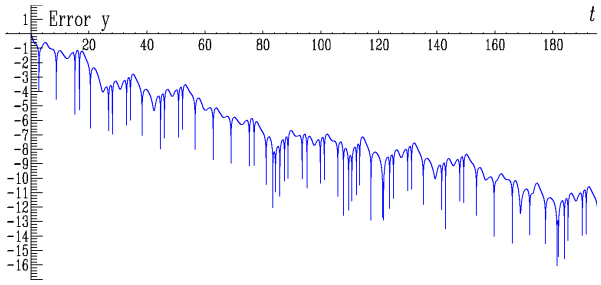

Fig. 4. Synchronization error Log $|e_y(t)|$ (blue line).

Log $|e_x(t)|$, Log $|e_y(t)|$, Log $|e_z(t)|$ and Log $|e_a(t)|$ are given as a function of normalized time t in Fig.3, Fig.4, Fig.5, and Fig.6, respectively, for $e = 3$. It is observed from the given figure that the auto-synchronization is achieved in less than $170t$, where the synchronization effect is better than that of $e = 1.23$.

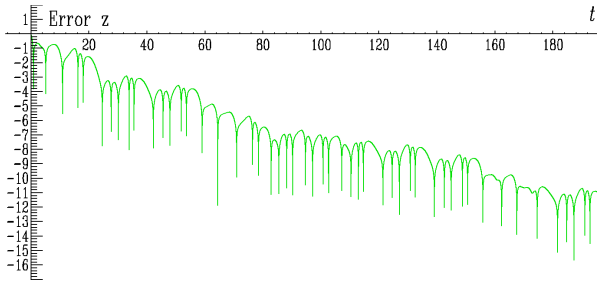

Fig. 5. Synchronization error Log $|e_z(t)|$ (green line).

Auto-synchronization of the predicting system is shown in Fig.7 where the convergence of the recovered parameter values a2 of the predicting systems to the known values a1 of the target system is illustrated. As shown from the given figure that, the proposed predicting system converges to the parameter a1 of the target system (for $a_1 = 0.35$, $a_1 = 0.40$, and $a_1 = 0.45$) and auto-synchronization is achieved in less than $170t$.

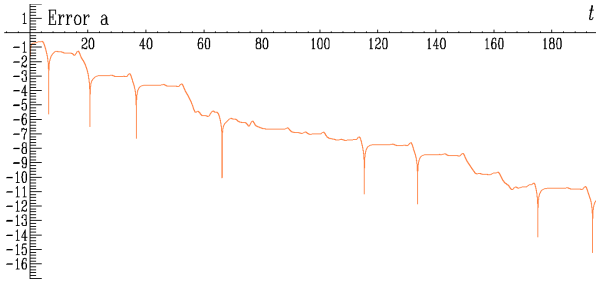

Fig. 6. Synchronization error Log $|e_a(t)|$ (orange line).

Simulation results of $x_1 - x_2$, $y_1 - y_2$ and $z_1 - z_2$, are depicted in Fig. 8, Fig. 9 and Fig. 10, which show non-synchronized behavior and synchronization of target and predicting systems.

From the figures it is observed that stable identical synchronization can be achieved. A synchronized phenomenon has not been observed initially but the proposed predicting system approaches the target system in less than $170t$ and the stable identical synchronization is obtained. These synchronized phenomenon are shown by colored lines in Fig. 8, 9 and Fig. 10, respectively.

Since the identical synchronization of predicting and target systems is achieved in less than $170t$ ($x_2 \rightarrow x_1, y_2 \rightarrow y_1, z_2 \rightarrow z_1$), the secret parameters of the target random number generation system are accurately revealed and the recovered values of x_1, y_1, z_1, and S_{bit} converge to their corresponding fixed values. As a result, it is clear that chaotic systems have achieved the identical synchronization and therefore the output bitstreams of the target and predicting systems are completely synchronized.

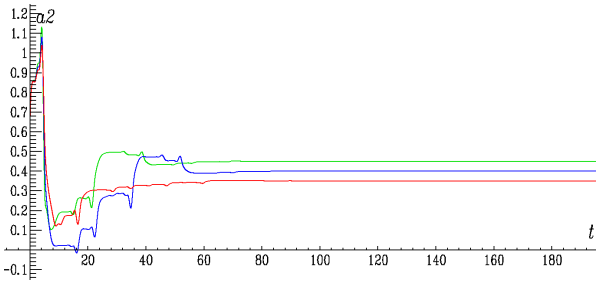

Fig. 7. Convergence of the parameter value a_2 of the predicting system to the fixed value a_1 of the target system for $a_1 = 0.35$, $a_1 = 0.40$, and $a_1 = 0.45$.

As a result, the proposed predicting system has not only reached the identical synchronization at the level of the

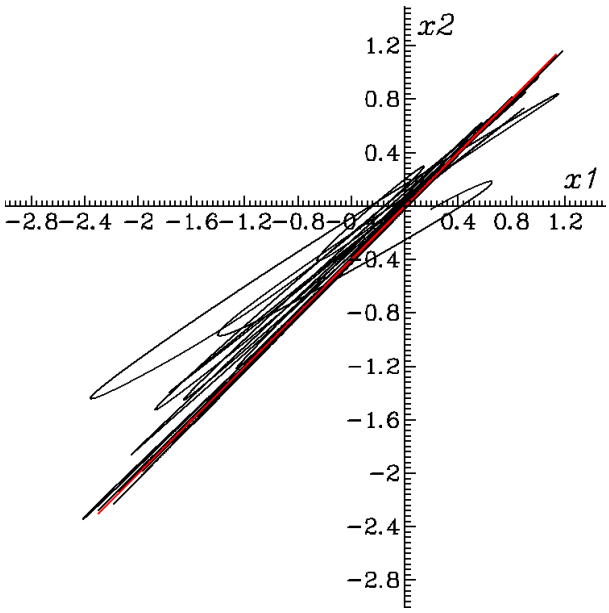

Fig. 8. Numerical results of $x_1 - x_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

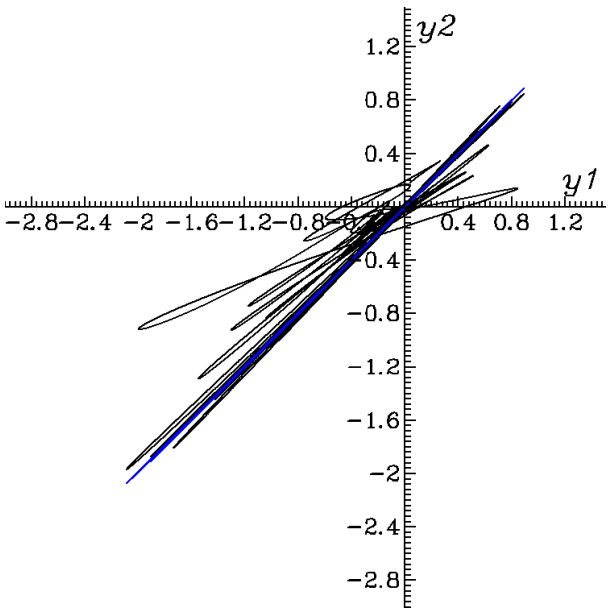

Fig. 9. Numerical results of $y_1 - y_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

chaotic state variables but also synchronized at the level of the generated bit sequence. Proposed system not only reveals the preceding and following bits of the target RNG but also shows that the predicting system can generate the same output bit sequence of the target RNG. The target RNG [8] satisfies neither the second nor third secrecy criteria that an RNG must fulfill. In conclusion, it has been verified that deterministic chaos can not be the true source of randomness.

5. CONCLUSIONS

In this paper, a predicting system is proposed to discover the security weaknesses of a chaotic random number generator (RNG). It is shown that secret parameters of the chaotic RNG can be recovered by the proposed predicting system using auto-synchronization scheme. Although the only information available is the structure of the chaotic RNG and a scalar time series, auto-synchronization of the predicting system is achieved and hence not only next bit but also whole output bit sequences are synchronized. The predicting system, makes the output bit sequences predictable and thus makes the targeted chaotic RNG indeed unusable for cryptographic applications.

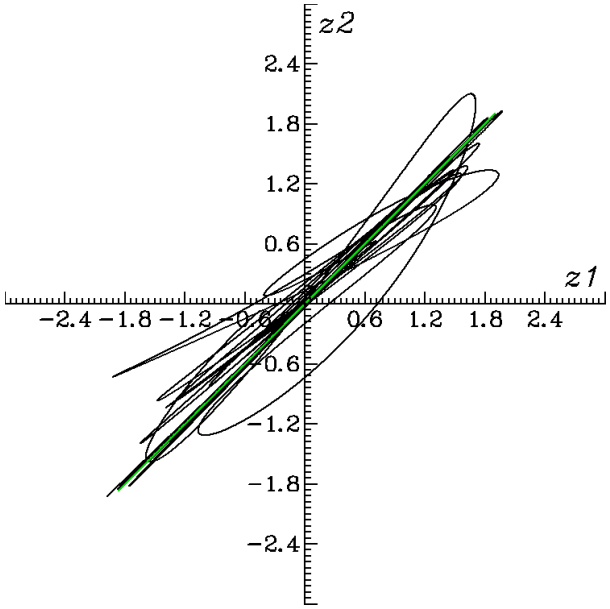

Fig. 10. Numerical results of $z_1 - z_2$ showing the synchronized and unsynchronized behaviors of target and estimate systems.

6. REFERENCES

[1] Ferguson, N., Schneier, B., Kohno, T.: Cryptography engineering: design principles and practical applications, Wiley Publishing, Inc. (2011)

[2] Martin., K.: Everyday Cryptography: Fundamental Principles and Applications, 2^{nd} Edition, Oxford University Press (2017)

[3] N.C. Göv, M.K. Mıhçak, and S. Ergün, "True Ran-

dom Number Generation Via Sampling From Flat Band-Limited Gaussian Processes," IEEE Trans. Circuits and Systems I, vol. 58, no. 5, pp. 1044-1051, May 2011.

[4] Schneier, B.: Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley Publishing, Inc. (2015)

[5] F. Pareschi, G. Setti, R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, 12 (2010) 3124-3137.

[6] J. L. Valtierra, E. Tlelo-Cuautle, A. Rodrguez-Vzquez, "A switched-capacitor skew-tent map implementation for random number generation", International Journal of Circuit Theory and Applications, vol. 45, 2 (2017) 305315.

[7] M. Kim, U. Ha, K. J. Lee, Y. Lee, H.J. Yoo, "A 82-nW Chaotic Map True Random Number Generator Based on a Sub-Ranging SAR ADC", IEEE Journal of Solid-State Circuits, vol. 52, 7 (2017) 1953-1965.

[8] E. Avaroğlu, I. Koyuncu, A.B. Özer, M. Türk, "Hybrid pseudo-random number generator for cryptographic systems", Nonlinear Dynamics, DOI 10.1007/s11071-015-2152-8, vol. 82. pp. 239248, 2015.

[9] J. C. Sprott, "Some simple chaotic flows," Physical Review E, vol. 50, no. 2, pp. R647 - R650, 1994.

[10] S. Ergün, "Modeling and Analysis of Chaos-Modulated Dual Oscillator-Based Random Number Generators," Proc. European Signal Processing Conference, pp. 1-5, Aug. 2008.

[11] 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

[12] S. Ergün, "Random numbers generation using continuous-time chaos" US Patent, Patent No US 008738675, May. 2014

[13] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, N. Heckert, J. Dray , "SP 800-22 Rev. 1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Apr. 2010, http://doi.org/10.6028/NIST.SP.800-22r1a Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-22r1a.pdf

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

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

[16] L.M. Pecora, T.L. Carroll, "Synchronization of chaotic systems," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 25, no. 9, 097611 pp. 1-12, Apr. 2015. https://doi.org/10.1063/1.4917383

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

[18] J. P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," American Physical Society, Reviews of Modern Physics, vol. 57, no. 3, 1, (1985), pp. 617-656. https://doi.org/10.1103/RevModPhys.57.617