DOI: 10.25092/baunfbed.742618 *J. BAUN Inst. Sci. Technol., 22(2), 591-599, (2020)*

Cryptanalysis of the chaotic oscillator based random number generator for bank authenticator device

Celal ERBAY*

TÜBİTAK, Informatics and Information Security Research Center, Gebze, Kocaeli

Geliş Tarihi (Received Date): 17.02.2020
Kabul Tarihi (Accepted Date): 16.05.2020

Abstract

In this study, cryptanalysis of a non-equilibrium point chaotic oscillator based random number generator (RNG) that developed as a high security authentication tool for internet banking systems is presented. The security vulnerabilities of the algorithm that generates random bits by using the digits of floating-point numbers have been analyzed and the convergence has been shown by using the master slave synchronization scheme. Simulation and numerical results of the proposed method confirm that both next bit and output bit stream are predictable. Therefore, producing random numbers by using such an algorithm for the authentication tool is very unsecure and master slave synchronization cryptanalysis method is useful to validate chaotic systems.

Keywords: *Cryptanalysis, non-equilibrium chaotic system, random number generator.*

Banka kimlik doğrulayıcı cihaz için kaotik osilatör tabanlı rasgele sayı üretecinin kriptanalizi

Öz

Bu çalışmada, internet bankacılığı sistemleri için yüksek güvenlikli bir kimlik doğrulama aracı olarak geliştirilen, denge noktası olmayan kaotik osilatör tabanlı rasgele sayı üretecinin (RNG) kriptanalizasyonu sunulmuştur. Kayan noktalı sayıların basamaklarını kullanarak rasgele bitler üreten algoritmanın güvenlik açıkları analiz edilmiş ve ana bağımlı senkronizasyon şeması kullanılarak yakınsama gösterilmiştir. Önerilen yöntemin simülasyonu ve sayısal sonuçları, hem sonraki bitin hem de çıkış bit akımının öngörülebilir olduğunu doğrular. Bu nedenle, kimlik doğrulama aracı için

* Celal ERBAY, celal.erbay@tubitak.gov.tr, https://orcid.org/0000-0001-8501-3908

böyle bir algoritma kullanarak rasgele sayılar üretmek çok güvenli değildir ve ana köle senkronizasyonu kriptanaliz yöntemi kaotik sistemleri doğrulamak için yararlıdır.

Anahtar kelimeler: *Kriptanaliz, dengeli olmayan kaotik sistem, rastgele sayı üreteci.*

1. Introduction

The usage of cryptographic applications is increasing every day since information secrecy has significant value for people. Random numbers generator (RNG) is most important block in these kind of applications since they require unpredictable bit streams [1]. Along with the developing technology, structures such as noise sources and chaotic systems, which are quite random, can be implemented easily as analog or digital, have recently started to be used as RNG [2]. Nonlinear and irregular behavior of chaotic systems makes them very sensitive for initial conditions which also makes these systems unpredictable due to the positive Lyapunov exponent [3]. The difference between two signals coming from the noise and chaotic source is not easy with unpredictable behaviors. Therefore, practical applications of chaotic systems such as chaos-based RNGs are possible in security systems [4,5].

There are two different kind of RNGs. Pseudo random number generator (PRNG) produce random numbers deterministically and it needs a unique sequence as seed to generate random numbers. However, if the seed is known then the output sequence can be observed by the attacker. On the other hand, true random number generator (TRNG) generates random bits from unstable entropy sources [6]. It can be mainly analog or digital one. Analog TRNGs use the physical phenomena to obtain the source such as radioactive decay time spent, phase, shot and thermal noises [7]. Since they depend on the device to produce physical source, their usage can be limited. TRNGs based on digital circuits are commonly used with the platforms like FPGA [8-10]. Because of the weaknesses in the calibration of physical variables, the quality is a significant issue for the design of digital TRNGs.

Noise source amplification, discrete-time chaotic maps, dual oscillator sampling, and continuous-time chaotic oscillators are four fundamental methodologies to generate random bit sequences [11]. Even though discrete-time chaotic maps based TRNGs are generally used in the literature, continuous-time chaos-based TRNGs have been started to use recently. In particular, example of continuous-time chaotic oscillator is given in [12] which is a “novel” chaos-based non-equilibrium chaotic system with coexisting attractors to generate random numbers for a bank authenticator device. In this work, we propose a master and slave synchronization method to cryptanalyze the proposed “novel” non-equilibrium chaotic system in [12]. The strength of the key makes security systems powerful and strong for an attacker. Therefore, if the system is proposed to generate random numbers must confirm the next bit and output bit streams cannot be predictable.

This paper is organized as follows. The target chaos-based RNG is presented in the next section. The master and slave synchronization attack method is defined in Section 3. Numerical results are explained in Section 4 and conclusions is given in the last section (Section 5).

2. Target system

Continues time chaos-based RNGs have advantage over discrete time chaos-based RNGs since they can be applied with less complex and more robust constructions. The target RNG uses continues time chaotic system to generate random bits [12]. Their encryption device is based on a no equilibrium point chaotic oscillator. Proposed chaotic system is expressed by using normalized magnitudes that are a, b, c, d, e, and f, by the following set of differential equations Eqn. 1:

$$\begin{aligned} \dot{x_1} &= ay_1 - x_1 + z_1 y_1 \\ \dot{y_1} &= -bx_1 z_1 - cx_1 + y_1 z_1 + d \\ \dot{z_1} &= e - f x_1 y_1 - x_1^2 \end{aligned} \tag{1}$$

The given equation creates chaos with multiple attractors for different set of values. The attractor given in Figure 1 is depicted by the numerical simulation of the system with a = 2.8, b = 0.2, c = 1.4, d = 1, e = 10, and f = 2.

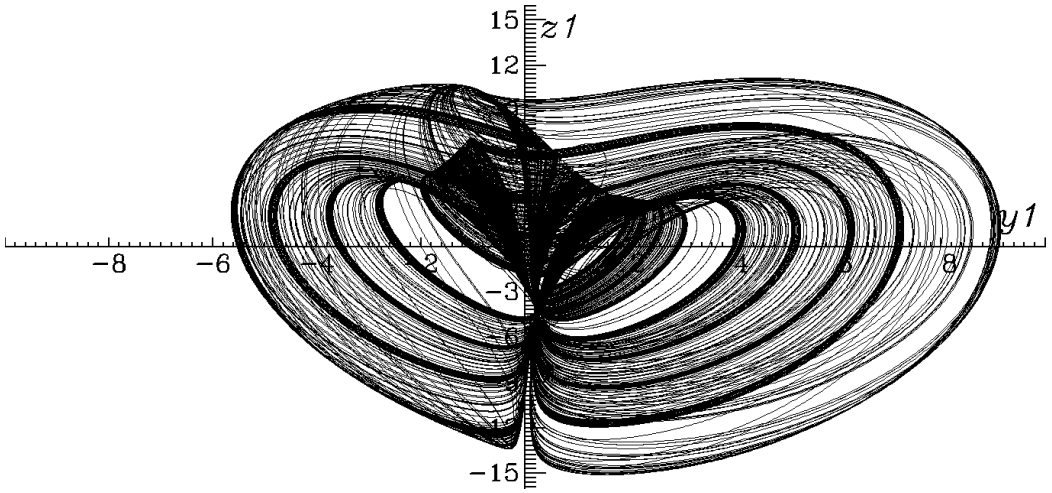

Figure 1. Simulation of the system with a = 2.8, b = 0.2, c = 1.4, d = 1, e = 10, and f = 2.

Proposed chaotic system [12] is based on the chaos-based RNG where x_1, y_1, and z_1 chaotic state variables of Eqn. 1 are used. Initially, numerical analysis of the given chaotic system is performed with the given set of parameters (a = 2.8, b = 0.2, c = 1.4, d = 1, e = 10, and f = 2) by using a 4th-order Runge-Kutta algorithm with a fixed step size. Then, floating point numbers are obtained from chaotic state variables and they were converted to thirty-two bits binary numbers by using the IEEE 754 standard. Since these bits are not able to pass the NIST-800-22 test suite, each thirty second bits were taken from each thirty-two binary numbers to create random bit streams and it was shown that they pass the test suite. However, if the chaotic state variables are known in the target design, the produced random bits of the RNG and all chaotic values can be predictable which result in obtaining customers' secret key for the bank authenticator device. We show in the next sections how it is possible with master slave synchronization attack method to obtain secret keys.

3. Clone systems

The convergence of target and clone chaotic system is explained with the master slave synchronization attack model. Three different clone systems are presented to cryptanalyze of the target chaos-based RNG. The clone systems given by the Eqn. 2, Eqn. 3, and Eqn. 4 are constructed these synchronizes $x_2 \rightarrow x_1$, $y_2 \rightarrow y_1$, and $z_2 \rightarrow z_1$ for $t \rightarrow \infty$ (t is the normalized time). The error signals are defined as $e_x = x_1 - x_2$, $e_y = y_1 - y_2$, and $e_z = z_1 - z_2$ where the purpose of the cryptanalysis is to find out the coupling strength such that $|e(t)| \rightarrow 0$ as $t \rightarrow \infty$. The identical synchronization of clone and target systems is verified by the Conditional Lyapunov Exponent (CLE) and can be achieved if the largest CLE is bigger than zero. Otherwise, if the largest CLE is smaller than zero, the identical synchronization becomes unstable. CLEs are calculated for the subsystem where continuous coupling method is performed.

The first clone system is given by the following Eqn. 2 for coupling to variable x_1.

$$\begin{aligned} \dot{x_2} &= ay_2 - x_2 + z_2y_2 + s(x_1 - x_2) \\ \dot{y_2} &= -bx_2z_2 - cx_2 + y_2z_2 + d \\ \dot{z_2} &= e - fx_2y_2 - x_2^2 \end{aligned} \tag{2}$$

In the equation, s is the coefficient that shows the strength of coupling to variable x_1, and the only public information is the design of non-equilibrium algorithm and a scalar time series obtained from x_1. When s is bigger than 0,46 and smaller than 1,6 then the largest CLE becomes negative as shown in Figure 2 and therefore the stable synchronization method of clone and target systems beginning with unlike states is achievable.

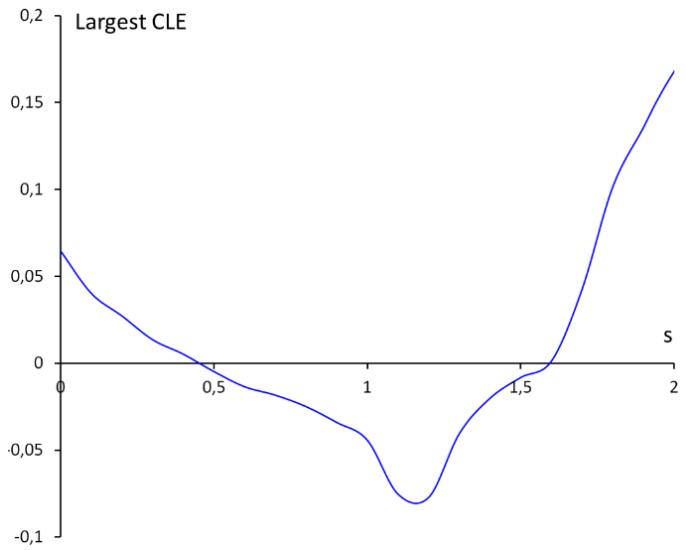

Figure 2. The largest CLE while coupling to variable x_1.

The second clone system is given by the given Eqn. 3 for coupling to variable y_1.

$$\begin{aligned} \dot{x_2} &= ay_2 - x_2 + z_2y_2 \\ \dot{y_2} &= -bx_2z_2 - cx_2 + y_2z_2 + d + s(y_1 - y_2) \\ \dot{z_2} &= e - fx_2y_2 - x_2^2 \end{aligned} \tag{3}$$

The largest CLE is illustrated in Figure 3 while coupling to variable y_1. The Largest CLEs values for coupling to variable y_1 are negative after s is larger than 0,5 as shown in Figure 3 and so the stable synchronization method of the target and clone systems can be determined at that point.

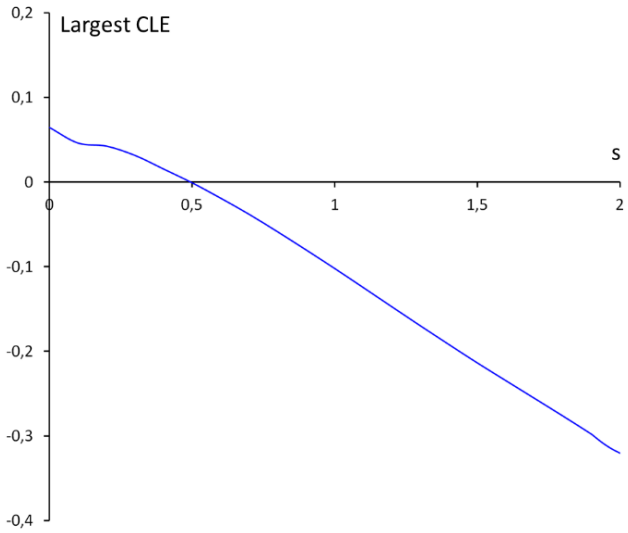

Figure 3. The largest CLE while coupling to variable y_1.

The last clone system is given by the following equation (Eqn. 4) for coupling to variable z_1.

$$\begin{aligned} \dot{x_2} &= ay_2 - x_2 + z_2 y_2 \\ \dot{y_2} &= -bx_2 z_2 - cx_2 + y_2 z_2 + d \\ \dot{z_2} &= e - fx_2 y_2 - x_2^2 + s(z_1 - z_2) \end{aligned} \tag{4}$$

When s is greater than 0,2, the largest CLE is smaller than zero and therefore the stable synchronization method of the clone and target systems with particular starting states is achievable for coupling to variable z_1.

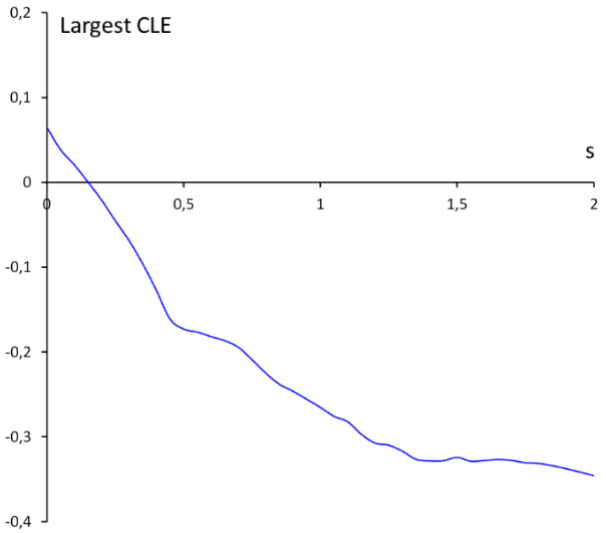

Figure 4. The largest CLE while coupling to variable z_1.

The synchronization errors ($\text{Log}|e_x(t)|$, $\text{Log}|e_y(t)|$ and $\text{Log}|e_z(t)|$) are given in Figure 5, Figure 6, and Figure 7, respectively for coupling to variable x_1, y_1, and z_1. Coupling

strength s = 0,46, 0,5, and 0,2 for coupling to variable x_1, y_1, and z_1 respectively, where the synchronization effects are better than threshold values. As shown in the figures, indistinguishable synchronization is obtained in less than 190t, 82t, and 75t, respectively for coupling to variable x_1, y_1, and z_1.

4. Numerical results

The clone systems were shown numerically by using fourth-order Runge-Kutta algorithm with fixed step size and their approaching are shown in Figure 5, Figure 6, and Figure 7. Numerical results of $x_1 - x_2$, $y_1 - y_2$, and $z_1 - z_2$ are also shown in Figure 8, Figure 9, and Figure 10 that gives the asynchronous and synchronous behavior of the target and clone systems.

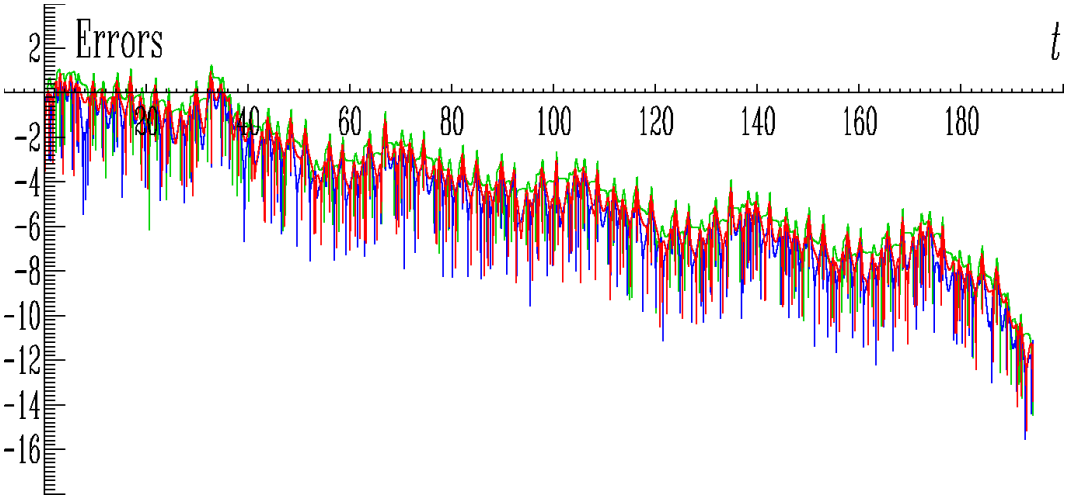

Figure 5. Log|e x(t)| (red), Log|e y(t)| (blue) and Log|e z(t)| (green) while coupling to variable x_1.

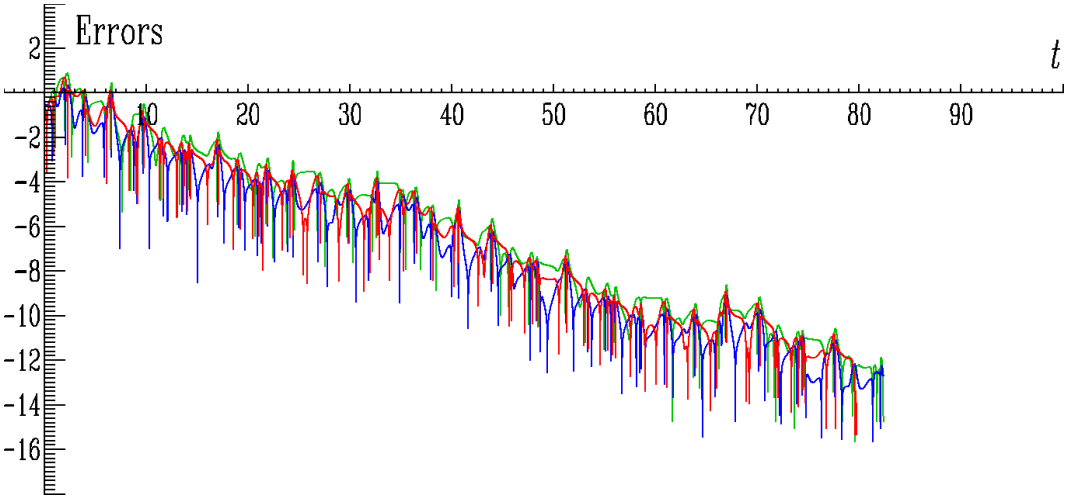

Figure 6. Log|e x(t)| (red), Log|e y(t)| (blue) and Log|e z(t)| (green) while coupling to variable y_1.

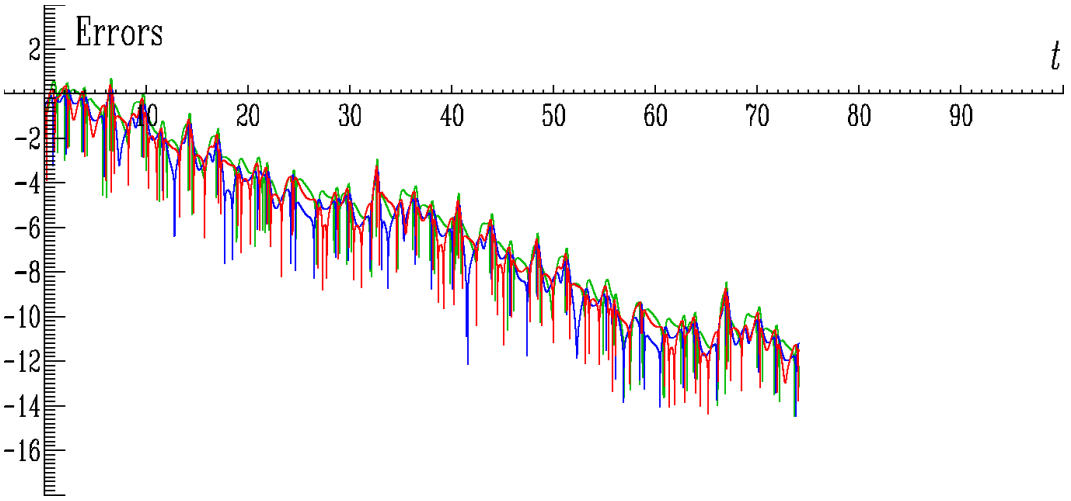

Figure 7. Log|e x(t)| (red), Log|e y(t)| (blue) and Log|e z(t)| (green) while coupling to variable z_1.

A synchronized phenomenon has not been shown before 190t, 82t, and 75t, respectively for coupling to variable x_1, y_1, and z_1, as shown by the black lines. Later, the clone systems converge to the target system and the identical line is achieved where other lines (red, blue, and green lines) represent the synchronized behavior of chaotic states in Figure 8, Figure 9, and Figure 10.

Since $x_2 \rightarrow x_1$, $y_2 \rightarrow y_1$, and $z_2 \rightarrow z_1$, the synchronous motion for clone and target systems can be obtained and the predicted parameters of RNG output and chaos-based RNG values which are produced based on the target system described in Section 2 converge to their corresponding fixed values. Thus, it confirms that the indistinguishable synchronization of the chaos-based systems is obtained and therefore the generated bit streams of the proposed target-clone systems are integrated.

The cryptanalysis of the proposed target RNG is resulted in both predicting the next bit stream, and showing the same output random bits of the target RNG can be reproduced by the master slave synchronization method. Therefore, the target system [12] cannot be used as RNG in cryptographic applications.

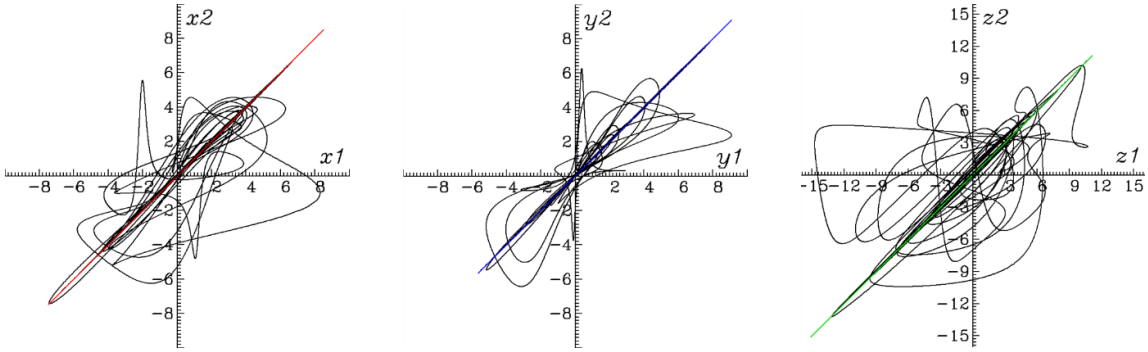

Figure 8. Numerical results of $x_1 - x_2$, $y_1 - y_2$, and $z_1 - z_2$ while coupling to variable x_1.

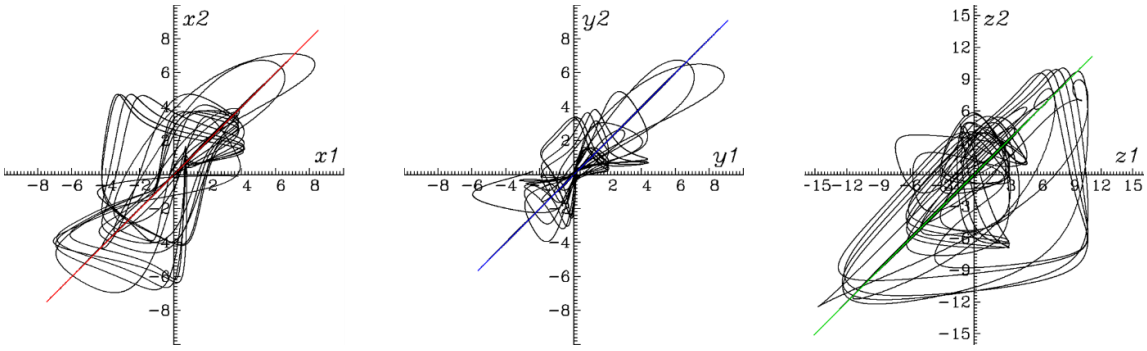

Figure 9. Numerical results of $x_1 - x_2$, $y_1 - y_2$, and $z_1 - z_2$ while coupling to variable y_1.

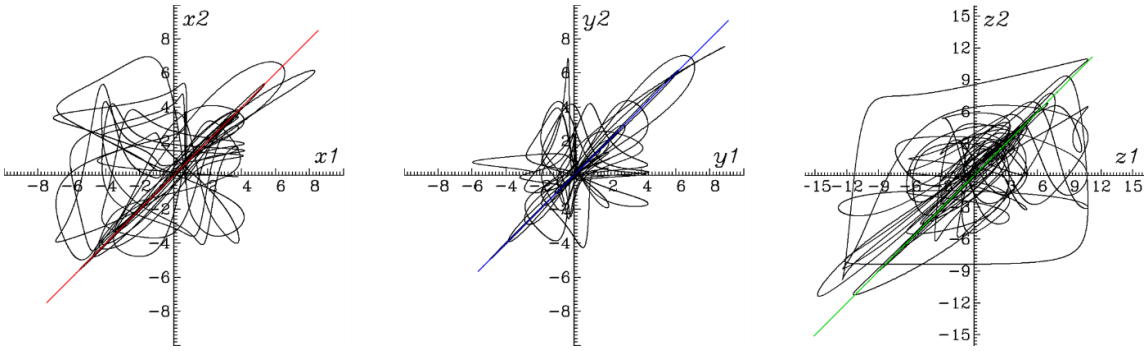

Figure 10. Numerical results of $x_1 - x_2$, $y_1 - y_2$, and $z_1 - z_2$ while coupling to variable z_1.

5. Conclusions

The establishment of the bridge between the customer and the bank as a third party by the GSM operators causes security weakness. Considering the various risks for these reasons, the use of the password-enabled device, rather than individual user and small-scale enterprises, will provide an important security requirement, especially for large-scale service provider companies with a large number of mobile, web and remote desktop access service subscribers or customers. However, designing non-secure systems may create very big issues and security risks for the customers. This work cryptanalyzes the "novel" chaos-based RNG designed as bank authenticator device by using master slave synchronization attack model. All the results show that the device is not secure since the produced random bits of the RNG is predictable which means the attacker can reach secret keys easily and therefore proposed target RNG cannot be used in any cryptographic applications indeed.

References

[1] Petrie, C.S. and Connelly, J.A., A noise-based IC random number generator for applications in cryptography, **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, 47(5), 615-621, (2000).

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

[3] Chen, W.C., Nonlinear dynamics and chaos in a fractional-order financial system, **Chaos, Solitons & Fractals**, 36(5), 1305-1314, (2008).

[4] Stojanovski, T. and Kocarev, L.,Chaos-based random number generators-part I: analysis [cryptography], **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, 48(3), 281-288, (2001).

[5] Stojanovski, T., Pihl, J. and Kocarev, L., Chaos-based random number generators. Part II: practical realization, **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, 48(3), 382-385, (2001).

[6] Kwok, S.H.M. and Lam, E.Y., FPGA-based High-speed True Random Number Generator for Cryptographic Applications, **TENCON 2006 IEEE Region 10 Conference**, Hong Kong, 1-4, (2006).

[7] Herrero-Collantes, M. and Garcia-Escartin, J.C., Quantum random number generators, **Review of Modern Physics**, 89, (2017).

[8] Wieczorek, P.Z., An FPGA Implementation of the Resolve Time-Based True Random Number Generator With Quality Control, in **IEEE Transactions on Circuits and Systems I: Regular Papers**, 61(12), 3450-3459, (2014).

[9] Şarkışla, M.A. and Ergün, S., An Area Efficient True Random Number Generator Based on Modified Ring Oscillators, **2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)**, Chengdu, 274-278, (2018).

[10] Wold, K. and Tan, C.H., Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings, **2008 International Conference on Reconfigurable Computing and FPGAs**, Cancun, 385-390, (2008).

[11] Ergün, S., On the Security of Chaos Based True Random Number Generators, **IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences**, E99.A(1), 363-369, (2016).

[12] Akkaya, S., Pehlivan, İ., Akgül, A., Varan, M., The design and application of bank authenticator device with a novel chaos based random number generator, **Journal of the Faculty of Engineering and Architecture of Gazi University**, 33(3), 1171-1182, (2018).