A Letters Journal Exploring the Frontiers of Physics

February 2020

EPL, **129** (2020) 30001
doi: 10.1209/0295-5075/129/30001

www.epljournal.org

Security analysis of a random number generator based on a chaotic hyperjerk system

Kaya Demir and Salih Ergün

TÜBİTAK - Informatics and Information Security Research Center - PO Box 74, Gebze, Kocaeli, 41470, Turkey

received 12 November 2019; accepted in final form 11 February 2020
published online 26 February 2020

PACS 05.45.-a – Nonlinear dynamics and chaos
PACS 89.70.-a – Information and communication theory
PACS 03.67.Dd – Quantum cryptography and communication security

Abstract – This paper analyzes the security of a random number generator (RNG) based on a 4-D chaotic hyperjerk system. An attack system is designed to reveal the security weaknesses of the proposed chaotic RNG. Knowing the structure of the RNG and observing one of the state variables of the chaotic system, convergence between attack and target systems is demonstrated by applying linear continuous coupling in master-slave synchronization scheme. Output bit sequence of the chaotic RNG is identically reproduced. The feasibility of the attack system is verified through numerical simulations. In this paper, a specific continuous-time chaos-based RNG is targeted as a case study. However, the cryptanalysis method presented in this paper is applicable to any continuous-time or discrete-time chaos-based RNGs. Therefore, this study highlights the security vulnerabilities of chaos-based RNGs and underlines that deterministic chaos itself cannot be considered as an entropy source for generation of random numbers.

Introduction. – With the rising number of devices connecting to the internet and exchanging data with each other and the server, ensuring information security becomes more challenging than ever before. Consequently, the design of cryptographic systems is gaining importance to assure the confidentiality, the integrity and the authenticity of information. A cryptographic system is basically a combination of an encryption algorithm and a random number generator (RNG) that produces key values for enciphering/deciphering data, one-time pad [1], cryptographic nonces, padding bytes and blinding values [2]. Cryptographic systems can implement a variety of complex encryption algorithms; however, the strength of a cryptographic system mostly depends on the secrecy and the unpredictability of the key values produced by its RNG [3]. Therefore, to ensure information security, the RNG in a cryptographic system must satisfy the following secrecy criteria: 1) The next bit of a RNG must be unpredictable, 2) it must be impossible to regenerate the output bit sequence of a RNG even if the RNG structure and method is known, and 3) the output bit stream must qualify all statistical tests of randomness such as NIST and Diehard [4]. Accordingly, it is extremely crucial to cryptanalyze a RNG to disclose its security weaknesses before it is deployed in a real cryptographic system.

In general, a RNG is a combination of three components: 1) An entropy source based on an intrinsically random physical process, such as thermal and shot noise or jittered oscillator [5], 2) a sampler such as a comparator or a flip-flop to generate random bits exploiting the entropy source, 3) a statistical post-processing phase such as Von Neumann or XOR to enhance the statistical properties of the RNG output bit stream. Four fundamental methods are frequently use to build RNGs: 1) Amplification of noise [6,7]; 2) using a jittered clock [8], 3) discrete-time chaotic maps [9,10] and 4) continuous-time chaotic oscillators [11–13]. Among these methods, using continous-time chaotic oscillators suggest enabling higher throughput without need for amplification and post-processing [14–16]. Consequently, there is a growing interest in the design of RNGs based on continous-time chaos.

Chaotic systems are defined by a set of deterministic equations. However, due to the positive Lyapunov exponents of the system, small fluctuations in initial conditions lead to hugely diverging results, thus obstructing the long-term predictability of the output [17]. Furthermore, chaotic signals exhibit irregular behavior and noise-like frequency spectrum, and hence appear to be ideal for use in RNGs. However, it should be underlined that

deterministic chaos cannot deliver true randomness. The actual source of randomness in a chaos-based RNG is the non-deterministic drift in initial conditions caused by noise. The unpredictability of the chaotic signals needs to be analyzed as in [10,13] before being used in a RNG system. If the deterministic chaos itself is used as the sole entropy source of the RNG, the output bit stream can be accurately predicted through synchronization of chaotic oscillators, thus information security can be compromised as we have shown previously in [18] for a 3-D continuous-time chaotic system. To address this security vulnerability of chaos-based RNGs, noise analysis has to be performed as we previously presented in [19,20] where the deterministic and non-deterministic components of the entropy source are highlighted. Contrarily, in [21], a chaos-based RNG is developed using a 4-D chaotic hyperjerk equation and the proposed RNG is claimed to be secure to be deployed in a cryptographic system. However, in the continuous-time chaos-based RNG described in [21], the chaotic signal itself is pointed out as the entropy source and numerical solution of the deterministic chaotic system is used for generating the encryption/decryption keys and thus, the impact of non-deterministic noise is discarded. Similar to [21], many studies focus on developing new RNGs based on various chaotic systems whereas they ignore the security issues related to the deterministic nature of chaos. For this reason, there is a compelling need for cryptanalysis of chaos-based RNGs and to disclose their security weaknesses.

This paper introduces a significant contribution to the aforementioned previous studies by presenting a comprehensive cryptanalysis study of the RNG based on the continuous-time 4-D chaotic hyperjerk system described in [21] in order to draw attention to security issues arising from using deterministic chaos as an entropy source for generation of random numbers. Although this paper targets the specific chaos-based RNG described in [21], this study presents a synchronization-based cryptanalysis method in details which can be applied to any continuous-time or discrete-time chaos-based RNG. Furthermore, this paper exemplifies that the strength of a cryptographic system depends on the secrecy of the key values generated by its associated RNG rather than the type of encryption/decryption method. Therefore, different from our previous studies [18–20], this paper presents a detailed study combining the theory behind synchronization of chaos and application of it on the security analysis of a RNG based on a 4-D chaotic hyperjerk system. This paper is organized as follows: the second section introduces the details of the target RNG and the cryptographic system given in [21]. The third section describes the mathematical analysis and the design of the attack system based on the master-slave synchronization between chaotic oscillators. The theory behind synchronization of chaotic systems through continuous linear coupling is revisited in that section and the concept of conditional Lyapunov exponents (CLE) corresponding to the eigenvalues of the Jacobian matrix of the difference system between target and attack systems is analytically described. The fourth section presents the numerical simulation results illustrating the convergence of target and attack RNG systems by adjusting the strength of coupling between the target and attack systems such that the largest CLE becomes negative, followed by the conclusions of this paper.

Target system. – RNGs can be based on either discrete-time or continous-time chaotic oscillators. However, the implementation of continuous-time chaotic systems as an electrical circuit is simpler due to the absence of sample-and-hold stages, amplifiers and switched-capacitors which are required in discrete-time chaotic systems [10,22]. In [21] a continuous-time chaotic system named as a new 4-D chaotic hyperjerk system is used as a basis for designing a RNG due to its nonlinear dynamic features and wide-band noise-like frequency spectrum. The values of the chaotic state variables x, y, z and w are used to derive the crypto keys to be used in the XOR-based image encryption/decryption algorithm. The set of equations defining the 4-D chaotic system is given as [21,23]

$$\begin{aligned} \dot{x}_1 &= y_1, \\ \dot{y}_1 &= z_1, \\ \dot{z}_1 &= w_1, \\ \dot{w}_1 &= -cx_1 - by_1 - \exp(y_1) - \exp(z_1) - aw_1. \end{aligned} \tag{1}$$

The initial conditions and parameters in [21] are given as

$$\begin{aligned} &x_0 = 0, \quad y_0 = -0.5, \quad z_0 = 0.1, \quad w_0 = -1, \\ &a_1 = 2, \quad b_1 = 4, \quad c_1 = 6. \end{aligned} \tag{2}$$

Using the initial conditions and parameters from (2), the equation system in (1) is solved using a 4th-order Runge-Kutta algorithm with a fixed step size $h = 0.001$. The 3-D phase portraits corresponding to combinations of x_1-y_1-z_1-w_1 state variables are shown in fig. 1.

The Jacobian matrix of a nonlinear system is defined as

$$\begin{aligned} J &= \begin{bmatrix} \frac{\partial \dot{x}_1}{\partial x_1} & \frac{\partial \dot{x}_1}{\partial y_1} & \frac{\partial \dot{x}_1}{\partial z_1} & \frac{\partial \dot{x}_1}{\partial w_1} \\ \frac{\partial \dot{y}_1}{\partial x_1} & \frac{\partial \dot{y}_1}{\partial y_1} & \frac{\partial \dot{y}_1}{\partial z_1} & \frac{\partial \dot{y}_1}{\partial w_1} \\ \frac{\partial \dot{z}_1}{\partial x_1} & \frac{\partial \dot{z}_1}{\partial y_1} & \frac{\partial \dot{z}_1}{\partial z_1} & \frac{\partial \dot{z}_1}{\partial w_1} \\ \frac{\partial \dot{w}_1}{\partial x_1} & \frac{\partial \dot{w}_1}{\partial y_1} & \frac{\partial \dot{w}_1}{\partial z_1} & \frac{\partial \dot{w}_1}{\partial w_1} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -c_1 & (-b_1 - \exp(y_1)) & -\exp(z_1) & -a_1 \end{bmatrix}. \end{aligned} \tag{3}$$

For the given parameters, using the QR decomposition-based numerical method on (3), the Lyapunov exponents

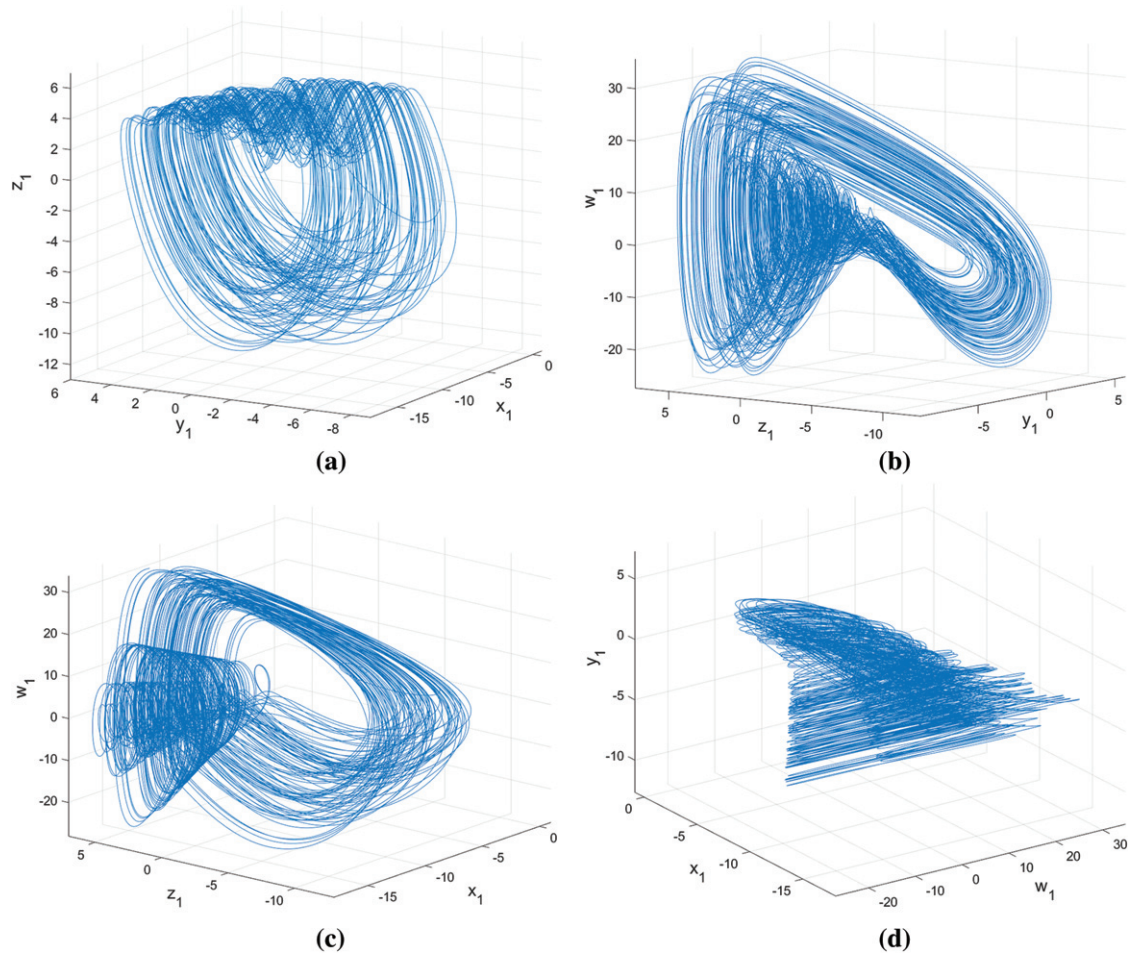

Fig. 1: 3-D phase portraits of the 4-D chaotic hyperjerk system: (a) x_1-y_1-z_1, (b) y_1-z_1-w_1, (c) x_1-z_1-w_1, (d) w_1-x_1-y_1.

of this system for these given parameters can be found approximately as $(0.31, 0, -0.16, -2.15)$. The system has only one positive Lyapunov exponent indicating that the system is in chaos. The bit generation method described in [21] is based on the calculation of the float type x_1, y_1, z_1 and w_1 state variables with a fixed step size Δh and converting them into 32-bit binary arrays. Then random bit sequences are generated by taking 2 least significant bits of x_1, y_1, w_1 and 5 least significant bits of z_1. Following this method 1 MBit length series is generated for each phase and subjected to the NIST-800-22 statistical tests of randomness. The step size Δh or the number of least significant bits is adjusted until bit sequences corresponding to each phase pass NIST test. It is asserted that as each bit sequence satisfies NIST 800-22 tests, this shows that the bit sequences have adequate randomness. Then as a demonstration in [21], a sample image is encrypted using an XOR-based algorithm. The image is converted to pixel-based binary form and subjected to XOR operation with the bit array obtained from the z-phase of the RNG. The decryption process is also shown by subjecting the encrypted image to another XOR operation with the same bit array. Therefore, a chaos-based RNG and its use in an encryption algorithm are shown in [21]. Due to the sensitivity of chaotic systems to initial conditions, it is claimed that this chaos-based encryption is impossible to decrypt.

Attack method. – The aperiodic behavior of continuous-time chaotic signals makes them appear random and attractive to use for the generation of random numbers. However, the short-term predictability of chaotic systems raises concern over the RNG security [24,25]. There have been a number of cryptanalysis studies on the security chaos-based systems implementing various attack methods, such as return-map attacks [26], prediction attacks [27], synchronization attacks [28], and parameter identification attacks [29]. In this paper, the attack method is based on synchronization of chaotic oscillators as described in the pioneering work by Pecora [30] and Carroll [31]. The convergence of target and attack systems is accomplished by applying a simple linear continous feedback to the attack system following the master-slave synchronization method. To provide an algebraic cryptanalysis of the target RNG, four clone systems are proposed each corresponding to each observed state variable of the target chaotic system. The synchronization of target and attack RNGs is achieved by adjusting the feedback

coupling coefficient such that the largest CLE of the difference system becomes negative. The continuous-time chaos-based RNG given in [21] is targeted by the clone systems while the information available is the structure of the RNG and the scalar time series of the corresponding chaotic state variable. In this paper, all parameters a, b and c of the target RNG are assumed to be known. There are mathematical methods to extract the parameter values which is beyond the scope of this paper and they will be investigated in a future study [29].

Clone system for observable x_1. Assuming scalar time series corresponding to the chaotic state variables x_1 is observable, then the equations defining the clone system can be given as [32]

$$\begin{aligned} \dot{x}_2 &= y_2 + k(x_1 - x_2), \\ \dot{y}_2 &= z_2, \\ \dot{z}_2 &= w_2, \\ \dot{w}_2 &= -cx_2 - by_2 - \exp(y_2) - \exp(z_2) - aw_2, \end{aligned} \tag{4}$$

where k is the coupling strength between the target (master) and clone (slave) systems for continuous linear feedback. In this study it is assumed that the parameters of the clone RNG system and the target one are equal. The error signals are defined as $e_x = x_1 - x_2$, $e_y = y_1 - y_2$, $e_z = z_1 - z_2$, $e_w = w_1 - w_2$ and the purpose is to adjust k so that $|e_x(t)|, |e_y(t)|, |e_z(t)|, |e_w(t)| \to 0$, as $t \to \infty$. To find the range of k values where the master-slave synchronization is stable, the CLEs of the difference system are calculated using the 4th-order Runge-Kutta algorithm and the QR decomposition method. The equations defining the difference system can be obtained by subtracting (4) from (1):

$$\begin{aligned} \dot{e}_x &= (y_1 - y_2) - k(x_1 - x_2), \\ \dot{e}_y &= z_1 - z_2, \\ \dot{e}_z &= w_1 - w_2, \\ \dot{e}_w &= -c_1(x_1 - x_2) - b_1(y_1 - y_2) \\ &\quad -(\exp(y_1) - \exp(y_2)) - (\exp(z_1) - \exp(z_2)) \\ &\quad -a_1(w_1 - w_2). \end{aligned} \tag{5}$$

The derivatives of $\dot{e}_x$ with respect to e_x, e_y and e_z can be found by

$$\frac{\partial \dot{e}_x}{\partial e_x} = -k, \quad \frac{\partial \dot{e}_x}{\partial e_y} = 1, \quad \frac{\partial \dot{e}_x}{\partial e_z} = 0, \quad \frac{\partial \dot{e}_x}{\partial e_w} = 0, \tag{6}$$

$$\frac{\partial \dot{e}_y}{\partial e_x} = 0, \quad \frac{\partial \dot{e}_y}{\partial e_y} = 0, \quad \frac{\partial \dot{e}_y}{\partial e_z} = 1, \quad \frac{\partial \dot{e}_y}{\partial e_w} = 0, \tag{7}$$

$$\frac{\partial \dot{e}_z}{\partial e_x} = 0, \quad \frac{\partial \dot{e}_z}{\partial e_y} = 0, \quad \frac{\partial \dot{e}_z}{\partial e_z} = 0, \quad \frac{\partial \dot{e}_z}{\partial e_w} = 1, \tag{8}$$

$$\begin{aligned} \frac{\partial \dot{e}_w}{\partial e_x} &= -c_1, \quad \frac{\partial \dot{e}_w}{\partial e_y} = -b_1 - \exp(y_1), \\ \frac{\partial \dot{e}_w}{\partial e_z} &= -\exp(z_1), \quad \frac{\partial \dot{e}_w}{\partial e_w} = -a_1. \end{aligned} \tag{9}$$

During the calculation of the derivatives, the following assumptions are made: $\exp(y_1) - \exp(y_2) = \exp(y_1) - \exp(y_1 - e_y)$ and assuming e_y is small to calculate the derivation $\partial \dot{e}_w / \partial e_y$, it can be written that $\exp(y_1) - \exp(y_1 - e_y) = \exp(y_1)(1 - \exp(-e_y) = \exp(y_1)(1 - (1 - e_y)) = \exp(y_1)e_y$. The calculation of $\partial \dot{e}_w / \partial e_z$ also follows similarly.

Then the Jacobian of the difference system becomes

$$J = \begin{bmatrix} -k & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -c_1 & -b_1 - \exp(y_1) & -\exp(z_1) & -a_1 \end{bmatrix}. \tag{10}$$

As the Jacobian of the difference system is 4 dimensional, the CLE spectrum consists of 4 components. If the largest of these exponents is negative, then synchronization is accomplished and stable. In fig. 2(a) the variation of CLE with respect to coupling strength k is shown when x_1 is the observed chaotic state variable. It is observed that the largest CLE of the difference system does not become negative for a wide range of k coupling strength. Therefore, synchronization between target and clone RNG is not possible when the observable chaotic state variable is x_1 [30,31].

Clone system for observable y_1. Similarly, assuming the available scalar time series is y_1, then the clone system for cryptanalysis of the target RNG is given as

$$\begin{aligned} \dot{x}_2 &= y_2, \\ \dot{y}_2 &= z_2 + k(y_1 - y_2), \\ \dot{z}_2 &= w_2, \\ \dot{w}_2 &= -cx_2 - by_2 - \exp(y_2) - \exp(z_2) - aw_2. \end{aligned} \tag{11}$$

Then similarly, to calculate CLEs, the Jacobian of the difference system can be written as

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -k & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -c_1 & -b_1 - \exp(y_1) & -\exp(z_1) & -a_1 \end{bmatrix}. \tag{12}$$

The relationship between the largest CLE and the coupling strength k for the observable y_1 is shown in fig. 2(b). It is observed that when $k \geq 0.8$, the CLE immediately becomes negative, hence the synchronization between the target and clone RNG is possible and stable.

Clone system for observable z_1. When the observable chaotic state variable is z_1, the equations defining the attack system can be defined as

$$\begin{aligned} \dot{x}_2 &= y_2, \\ \dot{y}_2 &= z_2, \\ \dot{z}_2 &= w_2 + k(z_1 - z_2), \\ \dot{w}_2 &= -cx_2 - by_2 - \exp(y_2) - \exp(z_2) - aw_2. \end{aligned} \tag{13}$$

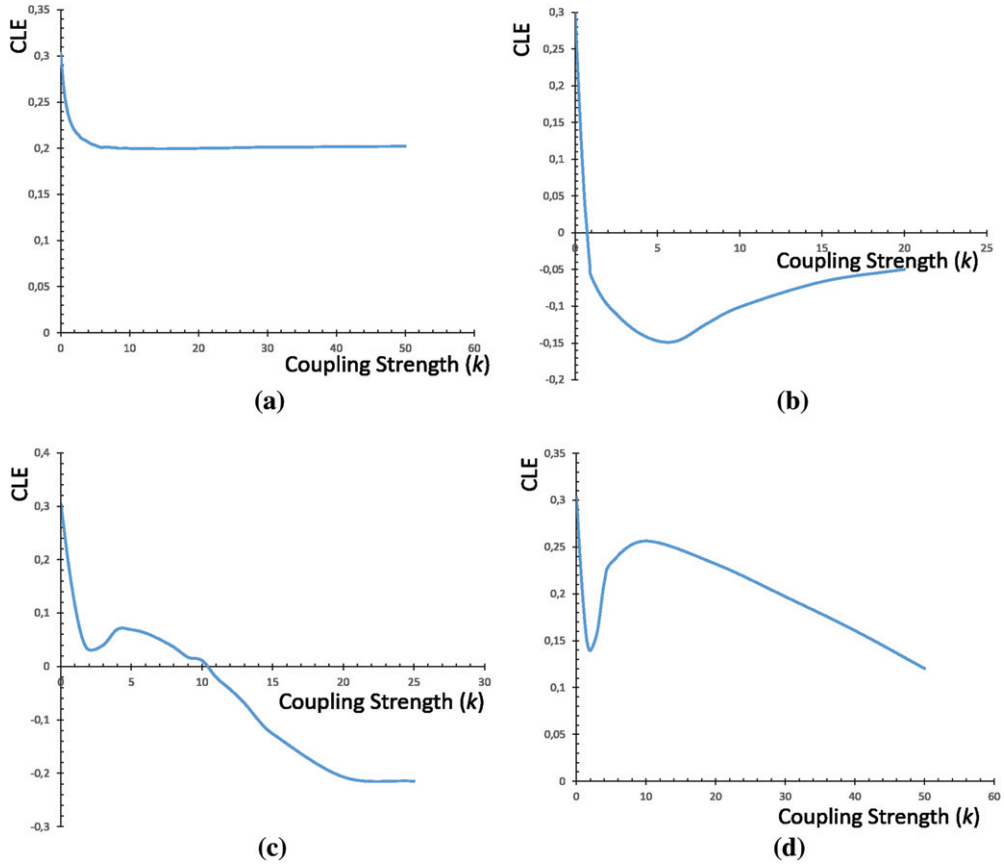

Fig. 2: Largest Conditional Lyapunov Exponent(CLE) as a function of the coupling strength k when the observed chaotic state variable is (a) x_1, (b) y_1, (c) z_1, (d) w_1.

Then following the same methodology, the Jacobian of the difference system can be written as

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -k & 1 \\ -c_1 & -b_1 - \exp(y_1) & -\exp(z_1) & -a_1 \end{bmatrix}. \quad (14)$$

The change of the largest CLE with coupling strength k for the observable z_1 is shown in fig. 2(c). It is observed that for $k \geq 10.5$, the largest CLE is negative, thus the synchronization of target and clone systems is possible and stable.

Clone system for observable w_1. Following a similar method, when w_1 is observable, the system of equations for the clone system can be defined as

$$\begin{aligned} \dot{x}_2 &= y_2, \\ \dot{y}_2 &= z_2, \\ \dot{z}_2 &= w_2, \\ \dot{w}_2 &= -cx_2 - by_2 - \exp(y_2) - \exp(z_2) \\ &\quad -aw_2 + k(w_1 - w_2). \end{aligned} \quad (15)$$

The Jacobian matrix of the difference system becomes

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -c_1 & -b_1 - \exp(y_1) & -\exp(z_1) & -a_1 - k \end{bmatrix}. \quad (16)$$

The relation between the largest CLE and the coupling strength in this case is shown in fig. 2(d). As can be observed, similar to observable x_1 case, the CLE of the difference system stays positive for a wide range of coupling strengths. Thus, the synchronization of target and clone systems is not possible by linear continuous coupling to w_1.

Numerical results. – Using the proposed attack method, clone systems defined by (4), (11), (13) and (15) are numerically simulated using the 4th-order Runge-Kutta algorithm and the coupling strength k parameter is adjusted according to the CLE *vs.* k graphs shown in fig. 2. The numerical simulations are run from $t = 0$ to $t = 1000$ with a fixed step size $h = 0.001$ as given in [21]. For each observed chaotic state variable, the numerical simulations approximately took 6 seconds using MATLAB R2018a on a desktop PC with 2.4GHz Intel

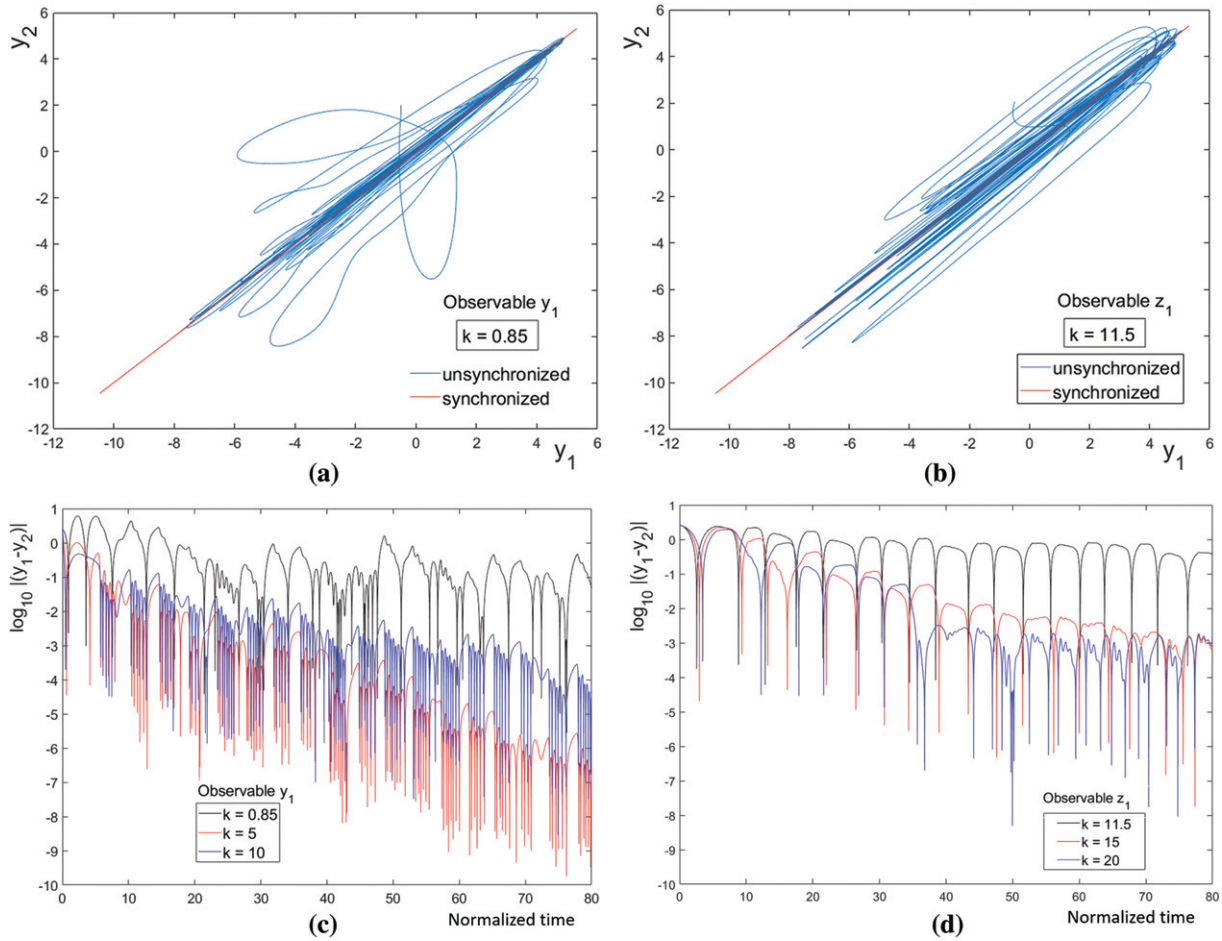

Fig. 3: a) Asynchronous (blue line) and synchronous (red line) motions of clone and target systems when (a) y_1 is observable, (b) z_1 is observable. Time evolution of $\log|e_y|$ while (c) y_1 is observable and the coupling strength $k = 0.85$ (black), 5 (red) and 10 (blue); (d) z_1 is observable and the coupling strength $k = 11.5$ (black), 15 (red) and 20 (blue).

Xeon Processor and 64GB DDR4 Ram. Therefore, the method described in this paper is not computationally intensive. Based on the discussion from the previous section and as shown in fig. 2, if the observable scalar time series is from either x_1 or w_1, it is not possible to achieve a stable synchronization due to positive CLE values. On the other hand, for the coupling strength k values greater than associated thresholds, the synchronization of target and clone system is possible when the available scalar time series is from either y_1 or z_1. In fig. 3(a) and (b) the coupling strengths are set as $k = 0.85$ and $k = 11.5$ and the available scalar time series correspond to y_1 and z_1, respectively. Despite different initial conditions, it is observed that as the coupling strength k is greater than the corresponding threshold values 0.8 and 10.5 for y_1 and z_1 variables, respectively, a synchronized behavior is achieved and stable. As illustrated in fig. 3(a) and (b), two systems are initially not synchronized as shown by the blue line, however, with time the clone RNG converges to the target RNG shown as the red line.

In fig. 3(c), the error function $\log|e_y|$ is shown when y_1 is the available scalar time series, linear continuous feedback is applied according to (11) and the coupling strength values 0.85, 5 and 10 are applied as shown by black, red and blue lines, respectively. It is observed that it takes shorter time to reach synchronization with $k = 5$ compared to $k = 10$ as the magnitude of the largest CLE is higher as seen in fig. 2(b). In fig. 3(d), the time evolution of $\log_{10}|e_y|$ is shown when the available time series is from z_1 and the coupling strength k is 11.5, 15 and 20 corresponding to black, red and blue lines, respectively. It is observed that synchronization is achieved faster for a higher k value which corresponds to a higher magnitude of the negative largest CLE, as shown in fig. 2(c).

In [21], the float value obtained from each variable is converted into a 32-bit binary number, and the 2 least significant bits of x_1, y_1, w_1 and 5 least significant bits of z_1 are added to the bit sequence. Furthermore, in [21] as a demonstration of image encryption, a sample image is first turned into a pixel-based binary form and then subjected to a bitwise XOR operation with this bit sequence. By repeating the XOR operation with the same bit sequence, the image is decrypted. The quality of this encryption process is evaluated and found to be close to

optimal according to various metrics. However, in this paper, the synchronization of the clone RNG to target RNG is demonstrated by observing a chaotic state variable and applying a simple linear continuous feedback. Therefore, it is possible to reproduce the exact same bitstream used in the encryption of the image which then can be used in the decryption of the encrypted image.

This study demonstrates that the strength of an encryption algorithm depends strongly on the unpredictability of the crypto key values produced by the RNG. The RNG output can satisfy statistical tests of randomness such as NIST 800-22. However, if the RNG output is predictable as in [21], the RNG cannot satisfy the second and third criteria of secrecy, thus the RNG proposed in [21] is not secure to be deployed in a cryptograhic system.

Conclusions. – The security analysis of a random number generator (RNG) based on a chaotic hyperjerk system is described. An attack method is proposed to reveal security vulnerabilities of the continuous-time chaos-based RNG. Using the master-slave synchronization scheme, stable synchronization between target and clone RNGs is numerically verified. By knowing the target RNG structure and observing the scalar time series from a chaotic state variable of the target RNG, the output of the bit stream of the target and clone RNGs can be reproduced by adjusting the magnitude of the coupling strength. Therefore, cryptokeys used in the XOR-based encryption algorithm are accurately predicted and thus information security is compromised. Although the target RNG is built on a 4-D chaotic hyperjerk system, the described method in this paper can be used for the cryptanalysis of any continuous-time or discrete-time chaos-based RNGs. This study demonstrates the security vulnerabilities arising from using deterministic chaos as the sole entropy source of a RNG without considering the impact of noise.

REFERENCES

[1] Shannon C. E., *Bell Syst. Tech. J.*, **28** (1949) 656.

[2] Jun B. and Kocher P., *The Intel® Random Number Generator* (Cryptography Research Inc.) White Paper, 1999.

[3] Stamp M., *Information Security: Principles and Practice* (John Wiley & Sons) 2011.

[4] Schneier B., *Foundations in Applied Cryptography*, second edition (John Wiley & Sons, Inc.) 2015, pp. 1–18.

[5] Menezes A., van Oorschot P., Vanstone S. and Vanstone S. A., *Handbook of Applied Cryptography, Discrete Mathematics and Its Applications Series* (CRC Press) 1996.

[6] Bagini V. and Bucci M., *A design of reliable true random number generator for cryptographic applications,* in *Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems* (Springer), 1999, pp. 204–218.

[7] Petrie C. S. and Connelly J. A., *IEEE Trans. Circuits Syst. I: Fundam. Theory Appl.*, **47** (2000) 615.

[8] Bucci M., Germani L., Luzzi R., Tommasino P., Trifiletti A. and Varanonuovo M., *IEEE Trans. Circuits Syst. I*, **50** (2003) 1373.

[9] Callegari S., Rovatti R. and Setti G., *IEEE Trans. Signal Process.*, **53** (2005) 793.

[10] Drutarovský M. and Galajda P., *Radioengineering*, **16** (2007) 121.

[11] Ozouz S., Elwakil A. and Ergun S., *IEE Proc. Circuits Devices Syst.*, **153** (2006) 506.

[12] Ergün S., *Method and hardware for generating random numbers using dual oscillator architecture and continuous-time chaos* (U.S. Patent 8,612,501, 17 Dec. 2013).

[13] Petrzela J. and Polak L., *IEEE Access*, **7** (2019) 17561.

[14] Ergün S. and Özoguz S., *Int. J. Circuit Theory Appl.*, **38** (2010) 1.

[15] Ergün S., *Regional random number generator from a cross-coupled chaotic oscillator,* in *Proceedings of IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)* (IEEE) 2011, pp. 1–4.

[16] Ergün S., *Compensated true random number generator based on a double-scroll attractor,* in *Proceedings of the International Symposium on Nonlinear Theory and Its Applications (NOLTA'06)* (IEICE (Institute of Electronics, Information and Communication Engineers)) 2006, pp. 391–394.

[17] Sprott J. C. and Sprott J. C., *Chaos and Time-Series Analysis*, Vol. **69** (Citeseer) 2003.

[18] Ergün S., *Cryptanalysis of a double scroll based "true" random bit generator,* in *Proceedings of 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)* (IEEE) 2015, pp. 1–4.

[19] Ergun S., Guler U. and Asada K., *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, **94** (2011) 180.

[20] Ergün S., Güler Ü. and Asada K., *Nonlinear Theory Appl., IEICE*, **2** (2011) 246.

[21] Vaidyanathan S., Akgul A., Kaçar S. and Çavuşoğlu U., *Eur. Phys. J. Plus*, **133** (2018) 46.

[22] Delgado-Restituto M. and Rodríguez-Vázquez Á., *Proceedings of the IEEE*, **90** (2002) 747.

[23] Dalkiran F. Y. and Sprott J. C., *Int. J. Bifurcat. Chaos*, **26** (2016) 1650189.

[24] Farmer J. D. and Sidorowich J. J., *Phys. Rev. Lett.*, **59** (1987) 845.

[25] Casdagli M., *Phys. D: Nonlinear Phenom.*, **35** (1989) 335.

[26] Li S., Chen G. and Alvarez G., *Int. J. Bifurcat. Chaos*, **16** (2006) 1557.

[27] Zhou C. and Lai C.-H., *Phys. Rev. E*, **60** (1999) 320.

[28] Alvarez G., Montoya F., Romera M. and Pastor G., *IEEE Trans. Circuits Syst. II: Express Briefs*, **51** (2004) 505.

[29] Alvarez G., Li S., Montoya F., Pastor G. and Romera M., *Chaos Solitons Fractals*, **24** (2005) 775.

[30] Pecora L. M., Carroll T. L., Johnson G. A., Mar D. J. and Heagy J. F., *Chaos: Int. J. Nonlinear Sci.*, **7** (1997) 520.

[31] Carroll T. L. and Pecora L. M., *IEEE Trans. Circuits Syst.*, **38** (1991) 453.

[32] Aguirre L. A. and Letellier C., *Chaos Solitons Fractals*, **83** (2016) 242.