CRYPTANALYSIS OF A RANDOM NUMBER GENERATOR BASED ON A FRACTIONAL-ORDER CHAOTIC MEMCAPACITOR OSCILLATOR

KAYA DEMİR

TUBITAK Informatics and Information Security Research Center, PO 74, 41470, Gebze, Kocaeli, Turkey
E-mail: kayademir@tubitak.gov.tr

Received July 29, 2022

Abstract. The cryptanalysis of a random number generator (RNG) based on a fractional-order chaotic memcapacitor oscillator is presented. A RNG is proposed to attack the target RNG with the purpose of revealing the security vulnerabilities. It is numerically demonstrated that if the design of the target RNG is known and if it is possible to probe a state variable of the fractional-order chaotic system for a time interval, then it is possible to achieve synchronization between the attack and the target RNGs through application of linear continuous feedback in a master-slave scheme. It is numerically shown that the identical output of the target RNG is generated by the attack RNG thanks to the synchronization between the attack and the target RNGs. In this paper, a specific fractional-order chaotic RNG is chosen as the target RNG for demonstration of the cryptanalysis method; however, the method presented in this study can be applied similarly to various RNGs based on either fractional-order or integer order and either continuous-time or discrete-time chaotic systems. Therefore, the purpose of this paper is to draw attention to the security vulnerabilities associated with RNGs based on fractional-order chaotic systems and to emphasize the error in assuming the deterministic fractional-order chaos as the sole entropy source for designing a RNG.

Key words: Cryptanalysis, fractional-order chaotic systems, random number generators, nonlinear systems, information security.

1. INTRODUCTION

The difficulty of protecting the information secrecy continues to increase with ever growing number of connected devices. Consequently, the importance of cryptographic systems is rising while they ensure the confidentiality, the integrity and the authenticity of information. In general, a cryptographic system is the combination of a ciphering/deciphering method and a random number generator (RNG) which generates crypto-keys to be used by the associated algorithm or crypto-nonces [1, 2]. A cryptosystem can choose an encryption/decryption algorithm from a vast number of available algorithms with varying complexities; however, the strength of a cryptographic system depends on the difficulty to hide the crypto-key values generated by its RNG [3]. Thus, to be considered cryptographically secure, the RNG of a cryptosystem must satisfy the following fundamental requirements: 1) It must be
impossible to predict the following output bit of a RNG with a possibility of higher than 0.5 even if all details about the target RNG is public information such as its internal design and bit generation method and even if all its previous output bit stream is known, 2) Similarly, generating the identical output bit stream of the RNG must be improbable, furthermore the RNG itself must generate an unpredictable and different bitstream whenever it is restarted, and 3) The RNG output has to fulfill the standardized randomness test suits such as NIST and Diehard to name a few [4]. Therefore, it is extremely important to expose the security vulnerabilities of a RNG through cryptanalysis studies.

Basically, a RNG can be considered as a combination of three main sections: 1) An entropy source to generate randomness, such as the intrinsic noise of a circuit element or the jittered oscillations of an oscillator with varying periods [5], 2) An element to take samples from the entropy source, 3) A post-processing section such as Von Neumann or XOR to remove statistical imperfections in RNG output, for instance the ratio of 1s and 0s in the bitstream. In literature, there are generally four basic methods which are commonly used for generation of random bits from a chaotic system. One of the methods is to amplify the output signal of a physical noise source which is usually an analog circuit [6, 7]. A second method is to use a jittered oscillator in a dual oscillator architecture where either a regular signal is sampled by a jittered clock, or a jittered signal is regularly sampled [8]. Another method depends on the exploitation of discrete-time chaotic maps [9]. The fourth method is based on using continuous-time chaos generating circuits [10–12]. Among these fundamental random bit generation methods, using continuous-time chaotic systems propose reaching higher data throughput compared to the other methods and meanwhile it removes the need for amplification of noise and statistical post-processing of the RNG output as shown previously in [13, 14]. Therefore, there is a growing interest on the application of continuous-time chaotic systems to design RNGs. As a further extension of integer order chaotic systems, recently fractional-order chaotic systems are also used for design of RNGs as they provide some advantages compared to their integer order counterparts such as the possibility of lower system degree [15, 16].

A cryptographic system can be only acknowledged as safe only if it stays impossible at all times for an attacker to predict the output of its RNG even if that all the details related to the RNG, such as its internal structure or the bit generation method. Providing that the RNG output is unpredictable, then even if the ciphering algorithm is publicly known, it is still impossible to predict the encrypted information [17]. The details of the RNG and the encryption/decryption algorithm should be considered as publicly known when designing a cryptographic system. However, it should always be emphasized that despite being either integer-order or fractional-order, chaotic systems are expressed by a set of nonlinear equations which have deterministic solutions. Hence, if a RNG merely uses deterministic chaos as a source of randomness to ge-
generate random bits, the RNG output can be precisely predicted through means of synchronization between chaotic systems, thus the cryptographic can become unsafe as shown previously for integer order chaotic systems in [18–21].

On the other hand, for the chaotic RNGs proposed in [22, 23], the impact of intrinsic noise acting on the nodes of the chaotic circuit is studied to mitigate this security vulnerability. The physical noise present on the circuit nodes lead to fluctuations in electrical parameters, which eventually lead to divergent results due to the nature of the chaotic system. On the contrary, the RNG based on a fractional-order memcapacitor given in [15] treats the deterministic chaos as the complete source of randomness to produce the output bits. Numerical solutions of the fractional-order chaotic system is wrongly used to design a RNG and the effect of non-deterministic and random physical noise on the circuit nodes is completely avoided. In [15] and in [16], a novel RNG based on a fractional-order chaotic system is presented where the chaotic signals originating from a memcapacitor oscillator are exploited with the purpose of producing the key values required for the cryptographic algorithm. Furthermore, the proposed RNG is claimed to be one of the first applications of a fractional-order chaotic system in order to design a RNG.

This paper presents a security analysis conducted on the fractional-order chaos based RNG proposed in detail in [15, 16]. In this paper, the fractional-order chaos based RNG is chosen to highlight the security weaknesses stemming from the predictability of chaos and the drawbacks of considering deterministic chaos as the single source of randomness of a RNG. A cryptanalysis method is proposed which is based on implementing a clone of the target RNG and exploiting the drive-response synchronization scheme with linear continuous feedback to predict the target RNG output as described in [24]. Therefore, this paper presents the first study on the security vulnerabilities of fractional-order chaos based RNGs and draws attention to the importance of exploring the security weaknesses of RNGs that use fractional-order chaotic systems. The paper is organized as follows: Section 2 briefly describes the target RNG system and the solution methodology. In section 3, the attack approach to cryptanalyze the target RNG based on drive-response configuration is presented along with three attack RNGs matching each observable dimension of the chaotic system. In Section 4, the results of numerical simulations demonstrating the convergence between the drive and response RNGs are presented, and conclusions are given in Section 5.

2. TARGET SYSTEM

Either discrete-time or continuous-time chaotic systems can be used for designing RNGs. Furthermore, either integer order or fractional-order chaotic oscillators can be utilized. Fractional-order chaotic systems are basically obtained by
changing the integer-order of nonlinear differential equations with fractional orders. One of the advantages of using fractional-order chaotic systems is that when the order becomes fractional, then the value of the fractional order can be used as another chaos-controlling parameter in addition to other parameters in the equation set. Thus, the fractional order increases the key space in a RNG application. Additionally, using fractional-order systems, it is possible to generate chaos for systems of order less than three. Therefore, it is relatively easier to design a chaotic oscillator using a fractional-order system. In this paper, a fractional-order chaotic memcapacitor oscillator is analyzed in terms of its security. In [15], a novel fractional-order memcapacitor based chaotic system is used for random number generation exploiting the irregular and noise-like dynamic features of chaotic signals. The chaotic signals corresponding to the scalar time series of state variables $x$, $y$ and $z$ obtained through numerical simulations are used to generate random bits. The generated output bitstream is shown to satisfy NIST statistical randomness tests.

The novel fractional-order memcapacitor based oscillator is described in detail in [15, 16, 25]. The schematic of the proposed memcapacitor based oscillator is shown in Fig. 1. Briefly, in Fig. 1, $R$, $L$, $G$ and $C$ correspond resistance, inductances, conductance and capacitance, respectively whereas $C_M$ corresponds to the memcapacitor. Applying the Kirchhoff’s law to the currents of the circuit shown on Fig. 1 and using the analytical memcapacitor model given in [15], the fractional-order chaotic system can be defined by a set of equations. Actually, the set of equations representing the memcapacitor oscillator can be made either integer order or fractional-order by adjusting the circuit parameters; however, in this paper the focus is on the fractional-order form of the proposed chaotic system. The set of equations defining the fractional-order chaotic system proposed in [15] is given as:
\[
\frac{d^\alpha x_1}{dt^\alpha} = a_1 x_1 + a_2 x_1^2 + a_3 y_1 \\
\frac{d^\alpha y_1}{dt^\alpha} = a_4 x_1 + a_5 x_1^2 - y_1 + z_1 \\
\frac{d^\alpha z_1}{dt^\alpha} = a_6 y_1,
\]

(1)

where each parameter \(a_1, a_2, a_3, a_4, a_5\) and \(a_6\) corresponds to a function defined by the circuit parameters as given in [15]. The equation can be solved using basics of fractional-order calculus as described in detail in [26]. To solve the equation (1), Grünwald-Letnikov method can be deployed as given in [26]

\[
D_a^t = \lim_{h \to 0} \frac{1}{h^a} \sum_{j=0}^{\infty} (-1)^j \binom{a}{j} f(t - jh),
\]

(2)

where \(D\) corresponds to the fractional-order generalization. The details of the method can be found in [26]. Briefly, for calculation of binomial coefficients, the relation between Euler’s Gamma (\(\Gamma\)) function and factorial can be used as given in [26]

\[
\binom{a}{j} = \frac{a!}{j!(a-j)!} = \frac{\Gamma(a+1)}{\Gamma(j+1)\Gamma(a-j+1)}
\]

(3)

and \(\binom{a}{0} = 1\). Considering that \(n = \frac{a - x}{h}\), where \(a\) is a real constant, it is possible to define

\[
aD_a^t = \lim_{h \to 0} \frac{1}{h^a} \sum_{j=0}^{\lceil \frac{a-x}{h} \rceil} (-1)^j \binom{a}{j} f(t - jh)
\]

(4)

where \(\lceil x \rceil\) refers to the integer part of \(x\) and, \(a\) and \(t\) correspond to the operation limits for \(aD_a^t\). Following this method and using the Matlab script detailed in [26], it is possible to numerically solve the eq. (1). The initial conditions for chaotic state variables, parameters and the fractional orders are given in [15] as,

\[
x_{1,0} = 0.001, \ y_{1,0} = 0.001, \ z_{1,0} = 0.001 \\
a_1 = -1.638, \ a_2 = -0.936, \ a_3 = 4.5, \ a_4 = 0.7, \ a_5 = 0.4, \ a_6 = -1.75
\]

(5)

Substituting the initial conditions of \(x_1, y_1,\) and \(z_1\), chaos controlling parameters and fractional orders from (5), the set of equations given in (1) is numerically solved by applying the method described in [26]. Assuming a fixed step size \(h = 0.001\), the trajectories corresponding to the \(x_1, y_1,\) and \(z_1\) chaotic state variables are shown in Fig. 2 being exactly same to [15]. Therefore, in order to do the cryptanalysis, first the target RNG system is identically regenerated.
The maximum Lyapunov exponent of the fractional-order chaotic system specified by (1) for the parameters given in (5) is roughly 0.118 [15], showing that the system is chaotic. Based on the numerical solution of the chaotic state variables $x_1$, $y_1$, and $z_1$ with a fixed step size of $\Delta h$ and translation of the results to 32-bit binary integers, the bit generation method described in [15] is based on this. Then, by concatenating the 16 least significant bits of $x_1$, the 12 least significant bits of $y_1$, and the 16 least significant bits of $z_1$, random bit streams associated with each state variable are produced. By following this approach, bitstreams of 1 Mbits length are created for each chaotic state variable, and the NIST-800-22 randomness test suite is used to evaluate the bitstreams’ randomness. The step size for the numerical simulation $\Delta h$ is selected so that the NIST test is satisfied by the generated bit streams for each state variable.
chaotic state variable. According to the assertion made in [15], each RNG output that passes the randomness test suite is sufficiently random and thus the RNG can be employed in various cryptographic applications.

3. ATTACK SYSTEM

A chaotic system being either integer-order or fractional-order, generates irregular noise-like signals with wide-band frequency spectrum which make chaotic systems attractive to be used in RNGs. The time evolution of the signal trajectories from a fractional-order chaotic system depends on its initial conditions, parameter values or fractional orders in an extremely sensitive manner. This means that two identical systems which start from slightly different initial conditions, parameter values or orders, will separate exponentially in time depending on the Lyapunov exponents. However, synchronization of chaotic systems also needs to be taken into account especially when a RNG is designed based on a chaotic system. The predictability of chaos raises concerns related to the security of RNG [27, 28]. There are various methods for cryptanalysis of chaos based RNGs such as return-map attacks [29], prediction approaches [30], synchronization based attacks [31], and parameter revealing methods [32] have been presented in literature dealing with the security of chaotic systems. Despite being relatively less compared to the integer order chaotic systems, there are also studies related to the synchronization of fractional-order chaotic systems [33–37].

In this study, the preferred attack method stands on the pioneering study on the synchronization of chaotic systems by Pecora and Carroll [24, 38] as it is a relatively simpler method to implement both numerically and experimentally as a circuit. The purpose in this method is to achieve convergence between the target and attack RNGs by applying linear continuous feedback in drive-response configuration. For each observable chaotic state variable $x_1$, $y_1$ or $z_1$, three response systems are presented for numerical cryptanalysis of the drive RNG. The response system can be forced to operate synchronized to the drive system simply by tuning the magnitude of the feedback coupling coefficient in order to make the largest conditional Lyapunov exponent (CLE) of the difference system less than zero. The fractional-order memcapacitor based chaotic RNG represented by the eq. (1) is targeted by three response systems while the architecture and the bit generation method of the RNG is open to public as it is already published, and one of the chaotic state variables is observable for a limited period of time. In this study, the chaos controlling parameters $a_1$, $a_2$, $a_3$, $a_4$, $a_5$, $a_6$ and the fractional order $q$ of the target RNG are considered as public information which is completely fair assumption because, the RNG output should be unpredictable even if all the details about the target RNG is publicly known according to the Kerckhoff’s principle. Even if an attacker has access to all knowl-
edge about the RNG under attack, it must still remain impossible to regenerate the
RNG output. Additionally, in literature there are mathematical approaches to derive
the value of these parameters [32] which is outside of the scope of this study.

3.1. RESPONSE SYSTEM FOR OBSERVABLE $x_1$

With identical parameters and fractional orders, the response system is con-
structed as a copy of the driving system. It is assumed that the chaotic state variable
$x_1$ can be monitored for a time interval. Based on linear continuous feedback, the
equation set defining the response system for the drive RNG’s cryptanalysis can be
written as:

$$
\begin{align*}
\frac{d^\alpha x_2}{dt^\alpha} &= a_1 x_2 + a_2 x_2^2 + a_3 y_2 + k(x_1 - x_2) \\
\frac{d^\alpha y_2}{dt^\alpha} &= a_4 x_2 + a_5 x_2^2 - y_2 + z_2 \\
\frac{d^\alpha z_2}{dt^\alpha} &= a_6 y_2,
\end{align*}
$$

(6)

where $k$ refers to the linear continuous coupling strength between the drive and res-
ponse RNGs.

The convergence error functions are given as $e_x = x_1 - x_2$, $e_y = y_1 - y_2$, $e_z = z_1 - z_2$. To meet the requirement $|e_x(t)|, |e_y(t)|, |e_z(t)| \to 0$ as $t \to \infty$, the proper
range of coupling strength values $k$ must be identified. The Lyapunov exponents
of the fractional-order difference system must be determined using the difference
system’s Jacobian matrix, as detailed in [39], in order to stabilize the synchronization
between the drive and response systems. By subtracting the equation set (6) from (1),
it is possible to determine the defining equation set for the difference system, which
may be written as follows:

$$
\begin{align*}
\frac{d^\alpha e_x}{dt^\alpha} &= \frac{d^\alpha x_1}{dt^\alpha} - \frac{d^\alpha x_2}{dt^\alpha} = a_1(x_1 - x_2) - a_2(x_1^2 - x_2^2) + a_3(y_1 - y_2) - k(x_1 - x_2) \\
\frac{d^\alpha e_y}{dt^\alpha} &= \frac{d^\alpha y_1}{dt^\alpha} - \frac{d^\alpha y_2}{dt^\alpha} = a_4(x_1 - x_2) + a_5(x_1^2 - x_2^2) - (y_1 - y_2) + (z_1 - z_2) \\
\frac{d^\alpha e_z}{dt^\alpha} &= \frac{d^\alpha z_1}{dt^\alpha} - \frac{d^\alpha z_2}{dt^\alpha} = a_6(y_1 - y_2).
\end{align*}
$$

(7)

To find the Jacobian matrix, the derivatives of $\dot{e}_x$ with respect to $e_x$, $e_y$ and $e_z$
can be given as

$$
\frac{\partial \dot{e}_x}{\partial e_x} = a_1 + 2a_2 x_1 - k, \quad \frac{\partial \dot{e}_x}{\partial e_y} = a_3, \quad \frac{\partial \dot{e}_x}{\partial e_z} = 0.
$$

(8)
While calculating $\frac{\partial \dot{e}_x}{\partial e_x}$, $(x_1^2 - x_2^2) = (x_1 - x_2)(x_1 + x_2)$ and $x_1 = x_2$ is considered as in [40].

Similarly, the derivatives of $\dot{e}_y$ with respect to $e_x, e_y$ and $e_z$ can be written as

$$\frac{\partial \dot{e}_y}{\partial e_x} = a_4 + 2a_5x_1, \quad \frac{\partial \dot{e}_y}{\partial e_y} = -1, \quad \frac{\partial \dot{e}_y}{\partial e_z} = 1. \quad (9)$$

Finally, the derivatives of $\dot{e}_z$ with respect to $e_x, e_y$ and $e_z$ can be defined as

$$\frac{\partial \dot{e}_z}{\partial e_x} = 0, \quad \frac{\partial \dot{e}_z}{\partial e_y} = a_6, \quad \frac{\partial \dot{e}_z}{\partial e_z} = 0. \quad (10)$$

Using the derivative functions, the Jacobian matrix associated with the difference system given in (7) can be defined as

$$J = \begin{bmatrix}
\frac{\partial \dot{e}_x}{\partial e_x} & \frac{\partial \dot{e}_x}{\partial e_y} & \frac{\partial \dot{e}_x}{\partial e_z} \\
\frac{\partial \dot{e}_y}{\partial e_x} & \frac{\partial \dot{e}_y}{\partial e_y} & \frac{\partial \dot{e}_y}{\partial e_z} \\
\frac{\partial \dot{e}_z}{\partial e_x} & \frac{\partial \dot{e}_z}{\partial e_y} & \frac{\partial \dot{e}_z}{\partial e_z}
\end{bmatrix} = \begin{bmatrix}
a_1 + 2a_5x_1 & a_3 & 0 \\
a_4 + 2a_5x_1 & -1 & 1 \\
0 & a_6 & -k
\end{bmatrix} \quad (11)$$

Using this Jacobian matrix given in (11) and using the variational equations based method and the provided Matlab script detailed in [39], the Lyapunov exponents of the difference system given in (7) can be calculated.

The conditional Lyapunov exponents (CLEs) correspond to the Lyapunov exponents of the fractional-order difference system given by equation (7). There are 3 CLE values since there are 3 dimensions. If the largest CLE in the CLE spectrum has a negative value, steady synchronization may be possible, as explained in detail in [24]. The relationship between the greatest CLE value and the coupling strength $k$ is seen in Fig. 3(a). It can be seen that the largest CLE value, which denotes the path to synchronization, is negative for coupling strengths $k \geq 0.6$. The driving and response RNGs can thus synchronize with one another if the time series $x_1$ is observable and the condition $k \geq 0.6$ is met.

3.2. RESPONSE SYSTEM FOR OBSERVABLE $y_1$

Similarly, if the chaotic state variable $y_1$ is observable, then the corresponding response system to attack the drive RNG is given as

$$\frac{d^q x_2}{dt^q} = a_1x_2 + a_2x_2^2 + a_3y_2$$
$$\frac{d^q y_2}{dt^q} = a_4x_2 + a_5x_2^2 - y_2 + z_2 + k(y_1 - y_2)$$
$$\frac{d^q z_2}{dt^q} = a_6y_2. \quad (12)$$
The corresponding difference system can be given as,

\[
\begin{align*}
\frac{d^4 e_x}{dt^4} &= \frac{d^4 x_1}{dt^4} - \frac{d^4 x_2}{dt^4} = a_1(x_1 - x_2) - a_2(x_1^2 - x_2^2) + a_3(y_1 - y_2) \\
\frac{d^4 e_y}{dt^4} &= \frac{d^4 y_1}{dt^4} - \frac{d^4 y_2}{dt^4} = a_4(x_1 - x_2) + a_5(x_1^2 - x_2^2) - (y_1 - y_2) + (z_1 - z_2) - k(y_1 - y_2) \\
\frac{d^4 e_z}{dt^4} &= \frac{d^4 z_1}{dt^4} - \frac{d^4 z_2}{dt^4} = a_6(y_1 - y_2).
\end{align*}
\]

(13)

Using the same method, the Jacobian matrix associated with the error system defined by equation (13) is then given as

\[
J = \begin{bmatrix}
a_1 + 2a_2x_1 & a_3 & 0 \\
a_4 + 2a_5x_1 & -1 - k & 1 \\
0 & a_6 & 0
\end{bmatrix}
\]

(14)
CLE values can be again obtained by calculating the Lyapunov exponents of the fractional-order system given by eq. (13), using the Jacobian matrix given in (14) and following the methodology explained in [39].

Figure 3(b) shows the change of the largest CLE value with the feedback coupling strength $k$ when $y_1$ time series is probed. By observing the Fig. 3(b), it is possible to claim that for $k \geq 0.5$, the largest CLE is less than zero, therefore stable synchronization between drive and response RNGs is achievable as explained in [24].

### 3.3. RESPONSE SYSTEM FOR OBSERVABLE $z_1$

Finally, in case that $z_1$ is observable, the response system used for the cryptanalysis of the target fractional-order chaotic system by linear continuous feedback is defined as

$$\frac{d^q x_2}{dt^q} = a_1 x_2 + a_2 x_2^2 + a_3 y_2$$
$$\frac{d^q y_2}{dt^q} = a_4 x_2 + a_5 x_2^2 - y_2 + z_2$$
$$\frac{d^q z_2}{dt^q} = a_6 y_2 + k(z_1 - z_2).$$

Then similarly, the difference system can be given as,

$$\frac{d^q e_x}{dt^q} = \frac{d^q x_1}{dt^q} - \frac{d^q x_2}{dt^q} = a_1(x_1 - x_2) - a_2(x_1^2 - x_2^2) + a_3(y_1 - y_2)$$
$$\frac{d^q e_y}{dt^q} = \frac{d^q y_1}{dt^q} - \frac{d^q y_2}{dt^q} = a_4(x_1 - x_2) + a_5(x_1^2 - x_2^2) - (y_1 - y_2) + (z_1 - z_2)$$
$$\frac{d^q e_z}{dt^q} = \frac{d^q z_1}{dt^q} - \frac{d^q z_2}{dt^q} = a_6(y_1 - y_2) - k(z_1 - z_2).$$

Then similarly, the Jacobian matrix of the difference system given in (16) is found as

$$J = \begin{bmatrix}
a_1 + 2a_2 x_1 & a_3 & 0 \\
a_4 + 2a_5 x_1 & -1 & 1 \\
0 & a_6 & -k.
\end{bmatrix}$$

Using (17) and the method from [39], Lyapunov exponents of the difference system given in equation (16) can be calculated. Figure 3(c) gives the change of the largest CLE with respect to the coupling strength $k$ when $z_1$ is observable. Based on Figure 3(c), it is seen that the for coupling strength values in the range $0.3 \geq k \geq 1.7$, the largest CLE is less than zero. Hence stable synchronization between drive and response RNGs is also achievable by probing only $z_1$ variable for a certain amount of time and applying appropriate coupling strength $k$. 

---

**Figure 3(b)** shows the change of the largest CLE value with the feedback coupling strength $k$ when $y_1$ time series is probed. By observing the Fig. 3(b), it is possible to claim that for $k \geq 0.5$, the largest CLE is less than zero, therefore stable synchronization between drive and response RNGs is achievable as explained in [24].
4. NUMERICAL RESULTS

In this section, based on the drive-response synchronization attack method, numerical simulations are conducted for response systems defined by (6), (12) and (15), and the values of coupling strength $k$ are adjusted using Fig. 3(a), Fig. 3(b) and Fig. 3(c) while the observable chaotic state variables are $x_1$, $y_1$ and $z_1$ respectively. As the largest CLE can be made negative by choosing the magnitude of coupling $k$ while any one of the state variable $x_1$, $y_1$ and $z_1$ is observable, convergence of drive and response RNGs should be achievable. The initial conditions of the drive RNG is $x_{1,0} = 0.001$, $y_{1,0} = 0.001$, $z_{1,0} = 0.001$ as in [15] where as the initial conditions of each response system is chosen as $x_{2,0} = 0.2$, $y_{2,0} = 0.2$, $z_{2,0} = 0.2$.

![Fig. 4 - (Color online). a) $x_1$-$x_2$ showing the unsynchronized (blue) and synchronized (red) behaviors of drive and response systems for observable $x_1$ and coupling strength $k=0.6$. b) Time evolution of $\log|e_x|$ observable $x_1$ and coupling strength $k = 1, 2$ and 5.](image)

Figure 4(a) demonstrates the transition from asynchronous to synchronous behavior for $x_1$ and $x_2$ while the available chaotic state variable is $x_1$ and the strength of coupling is adjusted $k = 0.6$ where the CLE is negative as shown in Figure 3(a). Figure 4(b) shows the time evolution of error function $\log_{10}|e_x|$ for varying coupling strength values. As can be seen on Figure 4(b), the values of $\log_{10}|e_x|$ approach to zero because the CLE is less than zero for these three coupling strength values. Furthermore, it is seen that the time it takes to reach complete synchronization of drive and response systems is minimum for the highest coupling strength ($k = 5$) as the absolute value of largest CLE is also higher for ($k = 5$) as shown in Fig. 3(a).

On the other hand, when $y_1$ is available for probing, based on Fig. 3(b), the largest CLE is negative for $k = 0.5$, thus synchronization between $x_1$ and $x_2$ is possible and stable. Figure 5(a) illustrates that despite starting from different initial conditions, the trajectory $x_1$-$x_2$ becomes a line with a slope $m = 1$ indicating that
synchronization is achieved between chaotic state variables $x_1$ and $x_2$. Similarly, Fig. 5(b) shows the time evolution of the error function $\log_{10}|e_x|$ with respect to the value of the coupling strength. It is seen that the time needed to reach synchronized behavior of the response and drive systems is smaller when $k = 4$ compared to the cases where $k = 1$ and $k = 15$. It is because as seen on Fig. 3(b), the magnitude of the largest CLE is higher when $k = 4$. 

Finally, when $z_1$ is probed and the feedback coupling coefficient is $k = 0.3$,
as shown in Fig. 3(c), the largest CLE is negative for the fractional-order difference system (16), making synchronization achievable and stable. Figure 6(a) shows how, through linear feedback coupling, $x_1$ and $x_2$ go from asynchronous behavior (blue line) to synchronized behavior (red line), respectively. Similar to Fig. 6(a), Fig. 6(b) depicts the time development of error function $\log_{10}|e_x|$ for varied coupling strength values. Due to the comparatively bigger magnitude of the biggest CLE, as shown on Fig. 3(c), it is noted that the time to convergence of the drive and response RNGs is shorter for $k = 1.2$ compared to $k = 0.4$ and $k = 1.6$.

Previous numerical simulations show that robust synchronization between the drive and response RNGs is possible. Even though the drive and response RNGs start out with different initial conditions, they will eventually synchronize if the largest CLE value is kept negative by using a coupling strength $k$ that corresponds to a chaotic state variable $x_1$, $y_1$ or $z_1$ that can be observed for a period of time. It is demonstrated that the response RNG can be watched to predict the next bit of the drive RNG proposed in [15] through the drive-response linear feedback arrangement. Thus, by converting the $x_2$, $y_2$ and $z_2$ values to 32 bit binary integers and concatenating particular parts of least significant bits as stated in [15] as the bit generation method, it is possible to regenerate the same output bit sequence of the target RNG. As a result, it is demonstrated that synchronization attacks can be used against RNGs based on fractional-order chaotic systems just as easily as those based on integer-order chaotic systems. The output of the RNG proposed in [15] is predictable because it only uses the numerical solutions of a deterministic fractional-order chaotic memcapacitor oscillator, which violates the first and second secrecy criteria for RNGs despite the target RNG’s output satisfying the NIST randomness test suite.

A cryptographic system also includes a key generation method and an encryption algorithm despite the fact that it is possible to use a synchronization attack to get the output bitstream of the target RNG proposed in [15]. It can be assumed that the information encrypted by the key values generated by the target RNG should therefore still be challenging to decipher. However, Kerckhoffs’s principle [41] is a cornerstone of cryptography. According to this rule, for a cryptosystem to be regarded as secure, everything about it should be assumed to be public information, with the exception of the cryptographic key [41]. Therefore, even if an attacker has complete knowledge of a cryptosystem design, he or she shouldn’t be able to decrypt the data unless they have access to the key. In other words, if the keys become predictable, a cryptographic system is not secure. The mechanisms used for key generation and encryption are both totally deterministic and can be assumed known. Even if a cryptosystem uses a highly complex key generation or encryption technique, Kerckhoff’s principle states that it cannot be claimed to be safe if it is possible to predict the RNG result. As a result, as this cryptanalysis investigation demonstrates that the target RNG suggested in [15] can have all of its output bits predicted, it cannot be regarded
as cryptographically secure and should not be used in a cryptographic system.

5. CONCLUSIONS

This study presented the first cryptanalysis study applied on a random number generator (RNG) based on a fractional-order chaotic system to reveal the associated security vulnerabilities. In this paper, the cryptanalysis of a RNG based on a fractional-order chaotic memcapacitor oscillator is presented. As chaos is deterministic either when it is integer order or fractional-order, it is wrong to consider it as the sole source of randomness in a RNG. Rather, the non-deterministic fluctuations in initial conditions of circuit components, fractional orders or chaos controlling parameters due to various noise sources is the actual randomness source where as the chaotic system boosts the deviation of trajectories starting from slightly different initial conditions. Although the proposed attack method is applicable to any chaos based RNGs, to demonstrate the security vulnerabilities, a fractional-order chaos based RNG using a memcapacitor is targeted. As the target RNG wrongly uses numerical solutions of fractional-order deterministic chaos as an entropy source to generate random output bits, the accurate prediction of RNG output is possible through synchronization of chaotic systems. An attack method based on drive-response technique with linear coupling is proposed to highlight the security vulnerabilities associated with fractional-order chaos based RNGs. Applying linear continuous feedback in drive-response configuration and adjusting the coupling strength, the largest conditional Lyapunov exponents of the difference system is brought down to negative values. Thus, stable synchronization between drive and response RNGs is numerically demonstrated. It is shown that if the details of the target RNG is known and a chaotic state variable of the target system is observable for a limited amount of time, then the output of drive and response RNGs become synchronized to each other by adjusting the magnitude of coupling strength.

REFERENCES


