Journal of the Egyptian Mathematical Society (2014) **22**, 365–372

Egyptian Mathematical Society

**Journal of the Egyptian Mathematical Society**

www.etms-eg.org
www.elsevier.com/locate/joems

ORIGINAL ARTICLE

# Synchronization of chaotic systems using feedback controller: An application to Diffie–Hellman key exchange protocol and ElGamal public key cryptosystem

**P. Balasubramaniam** *, **P. Muthukumar**

*Department of Mathematics, Gandhigram Rural Institute - Deemed University, Gandhigram - 624 302, Tamilnadu, India*

Received 21 June 2013; revised 5 September 2013; accepted 3 October 2013
Available online 14 November 2013

**KEYWORDS**

Chaos;
Feedback control;
Synchronization;
Cryptography

**Abstract** In this paper, designing an appropriate linear and nonlinear feedback control, the two identical integer order chaotic systems are synchronized by analytically and numerically. It has been realizing that, synchronization using linear feedback control method is efficient than nonlinear feedback control method due to the less computational complexity and the synchronization error. ElGamal public key cryptosystem is described through the proposed Diffie–Hellman key exchange protocol based on the synchronized chaotic systems using linear feedback control and their security are analyzed. The numerical simulations are given to validate the correctness of the proposed synchronization of chaotic systems and the ElGamal cryptosystem.

**2010 MATHEMATICS SUBJECT CLASSIFICATION:** 34H10; 93B52; 34D06; 94A60



## 1. Introduction

In nonlinear science, chaos synchronization has grown intensively because of its potential and practical applications in many fields. The possibility of synchronizing two chaotic system has been introduced by Pecora and Carroll [1] and the synchronization of two identical chaotic systems with different initial conditions has been presented in [2]. Moreover, synchronization of two chaotic systems has been studied extensively in the last few years.

Most recently, the problem of controlling chaos for new dynamical system has been studied and the sufficient conditions for synchronization of chaotic systems have been derived in [3]. An efficient nonlinear control method has been applied to the synchronization of unified chaotic systems using the Lyapunov method in [4] and a nonlinear control scheme for the synchronization has been presented using the Lyapunov stability theory in [5]. The synchronization of an energy re-

* Corresponding author. Tel.: +91 451 2452371; fax: +91 451 2453071.
E-mail addresses: balugru@gmail.com (P. Balasubramaniam), muthukumardgl@gmail.com (P. Muthukumar).

Peer review under responsibility of Egyptian Mathematical Society.

ELSEVIER Production and hosting by Elsevier

1110-256X © 2013 Production and hosting by Elsevier B.V. on behalf of Egyptian Mathematical Society. Open access under CC BY-NC-ND license.
http://dx.doi.org/10.1016/j.joems.2013.10.003

source system has been investigated and three linear control schemes have been proposed to synchronize a energy resource system in [6]. The synchronization process of a four dimensional chaotic systems by using linear feedback controller, a single variable and an adaptive controller methods have been proposed and demonstrated in [7]. Synchronization of energy resource systems has been proposed when the parameters of the master system are unknown and different from the slave system using adaptive linear feedback control in [8].

Chaos synchronization has been tremendous worldwide interest in communication systems, which has applications in the encryption and decryption of information for secure communications. An adaptive scheme has been exhibited in [9] for chaos synchronization that solves the problem of security in the communications. The authors in [10] have been designed secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization and their security features have been analyzed. Two methods of encoding and decoding message for secure communication based on an adaptive chaos synchronization have been investigated by Xing and Huang [11]. In [12], a new technique has been suggested for synchronizing two chaotic systems and that technique has been applied into digital cryptography [13] for sending and receiving messages.

In this paper, linear and nonlinear feedback control methods to synchronize the chaotic systems are presented. The ultimate aim is to apply the synchronized chaotic systems with minimum synchronization error in secure communication. Synchronization using linear and nonlinear control methods are investigated and conclude that the linear feedback control method is an effective method for synchronizing chaotic systems based on synchronization cost and error. Here, these synchronized chaotic systems are used in ElGamal cryptosystem to improve the security level. Mathematically, the discrete logarithm problem is a difficult problem to find their solution and it is closely related to Diffie–Hellman key exchange in cryptography. So, the Diffie–Hellman key exchange protocol is introduced newly based on synchronized chaotic systems and ElGamal public key cryptosystem which is proposed via Diffie–Hellman key exchange with the help of Fibonacci $Q$ matrices. The encryption and decryption processes are demonstrated through a numerical example and the security of the proposed cryptosystem is investigated.

The remainder of this paper is organized as follows: Section 2, the method of synchronizing chaotic systems using feedback controllers and their numerical simulations are given. The applications of the synchronized chaotic systems are presented in Section 3. In addition, it has been shown that the numerical example supports well with the proposed public key cryptosystem. The efficiency and security of the proposed cryptosystem are analyzed in Section 4. The paper is concluded in Section 5.

## 2. Synchronization of integer order chaotic systems

In this section, synchronization methods of two chaotic systems using nonlinear and linear feedback controllers and their numerical simulation results will be given.

### 2.1. Systems description

Consider a three dimensional autonomous chaotic dynamical system which can be expressed as in the following (see [14])

$$\begin{aligned} \dot{x} &= y(1-z) \\ \dot{y} &= y(1+z) - ax \\ \dot{z} &= a - xy - y^2 \end{aligned} \tag{1}$$

where $x$, $y$, $z$ are the state variables and $a$ is a parameter of the system (1). The strange attractors of the system (1) are different from Lorenz system in topological structure. The dynamical features of the system (1) have been analyzed in [14].

The system (1) exhibits chaos when $a = 2$. The chaotic attractor corresponding to the system (1) is shown in Fig. 1 and the different phase portraits are depicted in Fig. 2.

In the following subsections, the processes of synchronization of chaotic systems using nonlinear and linear feedback control methods are studied for the driving system (1).

### 2.2. Synchronization using nonlinear feedback control

Consider the following system as a response system, which is identical to system (1) as

$$\begin{aligned} \dot{x_1} &= y_1(1-z_1) + u_1 \\ \dot{y_1} &= y_1(1+z_1) - ax_1 + u_2 \\ \dot{z_1} &= a - x_1y_1 - y_1^2 + u_3 \end{aligned} \tag{2}$$

where $u_1$, $u_2$ and $u_3$ are feedback controllers.

Let $e_1 = x_1 - x$, $e_2 = y_1 - y$ and $e_3 = z_1 - z$ be the error variables.

Then the error system of (1) and (2) can be derived as follows:

$$\begin{aligned} \dot{e_1} &= e_2 - e_2e_3 - e_2z - e_3y + u_1 \\ \dot{e_2} &= -ae_1 + e_2(1+z) + e_2e_3 + ye_3 + u_2 \\ \dot{e_3} &= -e_1e_2 - e_1y - xe_2 - e_2^2 - 2e_2y + u_3 \end{aligned} \tag{3}$$

**Theorem 1.** *The systems (1) and (2) will approach global and exponential asymptotical synchronization with the following nonlinear control law:*

$$\begin{aligned} u_1 &= -k_1e_1 \\ u_2 &= -k_2e_2 \\ u_3 &= 2e_1(1+e_2) - k_3e_3 \end{aligned} \tag{4}$$

*where $k_1$, $k_2$ and $k_3$ are positive feedback gains which will be estimated in order to achieve synchronization.*

**Proof.** Consider the Lyapunov candidate function as

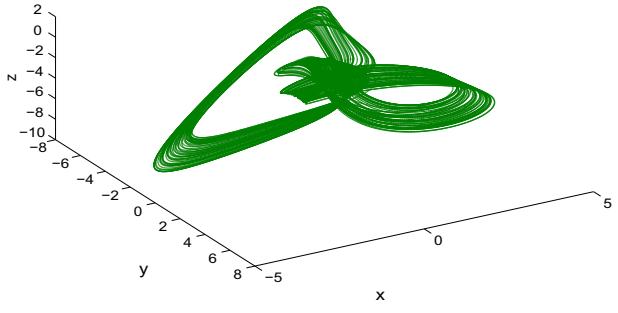


**Fig. 1** Chaotic attractor corresponding to the system (1) in 3D view.

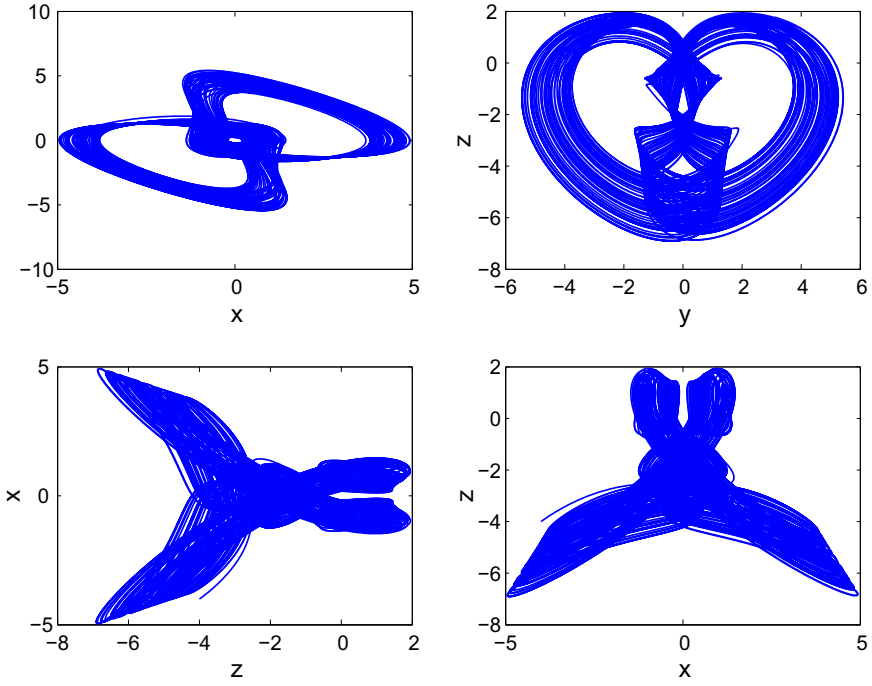


**Fig. 2** Different phase portraits of the system (1) in 2D view.

$$V = \frac{1}{2}\left(e_1^2 + e_2^2 + e_3^2\right) \tag{5}$$

Then the time derivative of $V$ can be written as

$$\begin{aligned}\dot{V} &= e_1\dot{e_1} + e_2\dot{e_2} + e_3\dot{e_3}\\ &= e_1(e_2 - e_2e_3 - e_2z - e_3y + u_1) + e_2(-ae_1 + e_2(1+z)\\ &\quad + e_2e_3 + ye_3 + u_2) + e_3(-e_1e_2 - e_1y - e_2x - e_2^2 - 2e_2y\\ &\quad + u_3)\\ &= (e_1e_2 - e_1e_2e_3 - e_1e_2z - e_1e_3y + e_1u_1)\\ &\quad + \left(-ae_1e_2 + e_2^2(1+z) + e_2^2e_3 + e_2e_3y + e_2u_2\right)\\ &\quad + \left(-e_1e_2e_3 - e_1e_3y - e_2e_3x - e_2^2e_3 - 2e_2e_3y + e_3u_3\right)\end{aligned}$$

$$\begin{aligned}\dot{V} \leqslant\ & -2|e_1e_2e_3| - (a+L-1)|e_1e_2| - 2L|e_2e_3| - 2L|e_1e_3|\\ & + (1+L)e_2^2 + |e_2|u_2 + |e_1|u_1 + |e_3|u_3\end{aligned} \tag{6}$$

where $L$ is the boundary satisfying $|x|, |y|, |z| \leqslant L$ and $|x_1|, |y_1|, |z_1| \leqslant L$.

Substitute (4) in (6),

$$\begin{aligned}\dot{V} \leqslant\ & -\left[k_1e_1^2 + (a+L-1)|e_1e_2| + 2L|e_2e_3| + (k_2 - 1 - L)e_2^2\right.\\ & \left. + k_3e_3^2\right] = -|e^T|P|e|\end{aligned}$$

where $|e| = (|e_1|, |e_2|, |e_3|)^T$ and

$$P = \begin{pmatrix} k_1 & \frac{1}{2}(a+L-1) & 0\\ \frac{1}{2}(a+L-1) & k_2 - 1 - L & L\\ 0 & L & k_3\end{pmatrix} \tag{7}$$

Then the error system (3) is asymptotically stable if the matrix $P$ should be positive definite.

The necessary and sufficient conditions for a matrix $P$ to be positive definite are

1. The diagonal elements of $P$ must be all positive.
2. The determinants of all the upper left-hand corners of $P$ are positive.

If above conditions are satisfied, then the matrix $P$ is positive definite. Hence $P$ is positive definite, then $\dot{V}$ is negative definite, which implies the error system (3) is asymptotically stable. Based on Lyapunov's stability theory, $\lim_{t\to\infty}\|e(t)\| = 0$. Therefore the systems (1) and (2) are synchronized successfully. □

### 2.3. Synchronization process using linear feedback control

Consider the following response system with the linear feedback controller as described by

$$\begin{aligned}\dot{x_1} &= y_1(1 - z_1) - g_1(x_1 - x)\\ \dot{y_1} &= y_1(1 + z_1) - ax_1 - g_2(y_1 - y)\\ \dot{z_1} &= a - x_1y_1 - y_1^2 - g_3(z_1 - z)\end{aligned} \tag{8}$$

where $g_1$, $g_2$ and $g_3$ are positive feedback gains.

Then the error dynamical system of (1) and (8) can be derived as follows:

$$\begin{aligned}\dot{e_1} &= e_2 - (y_1z_1 - yz) - g_1e_1\\ \dot{e_2} &= -ae_1 + (y_1z_1 - yz) + e_2 - g_2e_2\\ \dot{e_3} &= -(x_1y_1 - xy) - y_1^2 + y^2 - g_3e_3\end{aligned} \tag{9}$$

where $e_1 = x_1 - x$, $e_2 = y_1 - y$ and $e_3 = z_1 - z$.

**Theorem 2.** *The systems (1) and (8) will approach global and exponential asymptotical synchronization with the following linear control law:*

$$\begin{aligned}v_1 &= -g_1e_1\\ v_2 &= -g_2e_2\\ v_3 &= -g_3e_3\end{aligned} \tag{10}$$

*where $g_1$, $g_2$ and $g_3$ are positive feedback gains which will be estimated in order to achieve synchronization.*

**Proof.** Consider the Lyapunov candidate function as

$$V_1 = \frac{1}{2}\left(e_1^2 + e_2^2 + e_3^2\right) \tag{11}$$

Then the time derivative of $V_1$ can be written as

$$\begin{aligned}\dot{V}_1 &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3\\ &= e_1(e_2 - (y_1z_1 - yz) + v_1) + e_2(-ae_1 + (y_1z_1 - yz) + e_2\\ &\quad + v_2) + e_3\left(-(x_1y_1 - xy) - y_1^2 + y^2 + v_3\right)\\ &= (e_1e_2 - (y_1z_1 - yz)e_1 + e_1v_1)\\ &\quad + \left(-ae_1e_2 + e_2^2 + (y_1z_1 - yz)e_2 + e_2v_2\right)\\ &\quad + \left(-(x_1y_1 - xy)e_3 - \left(y_1^2 - y^2\right)e_3 + e_3v_3\right)\end{aligned}$$

$$\begin{aligned}\dot{V}_1 &\leqslant |e_1e_2| - \left(L_1^2 - L_1^2\right)|e_1| + v_1e_1 - a|e_1e_2| + e_2^2\\ &\quad + \left(L_1^2 - L_1^2\right)|e_2| + v_2e_2 - \left(L_1^2 - L_1^2\right)|e_3|\\ &\quad - \left(L_1^2 - L_1^2\right)|e_3| + v_3e_3\end{aligned} \tag{12}$$

where $L_1$ is the boundary satisfying $|x|, |y|, |z| \leqslant L_1$ and $|x_1|, |y_1|, |z_1| \leqslant L_1$. Substitute (10) in (12),

$$\begin{aligned}\dot{V}_1 &\leqslant -\left[-(a+1)|e_1e_2| + g_1e_1^2 + (g_2+1)e_2^2 + g_3e_3^2\right]\\ &= -|e^T|P_1|e|\end{aligned}$$

where $|e| = (|e_1|, |e_2|, |e_3|)^T$ and

$$P_1 = \begin{pmatrix} g_1 & -\frac{1}{2}(a+1) & 0\\ -\frac{1}{2}(a+1) & g_2+1 & 0\\ 0 & 0 & g_3\end{pmatrix} \tag{13}$$

Then the error system (9) is asymptotically stable if the matrix $P_1$ is be positive definite.

The necessary and sufficient conditions for a matrix $P_1$ to be positive definite are given in Theorem 1. Based on Lyapunov's stability theory, $\lim_{t\to\infty}\|e(t)\| = 0$. Thus, the synchronization of systems (1) and (8) is achieved successfully. □

### 2.4. Numerical simulations

Choose the value $L = L_1 = 10$, $k_1 = g_1 = 25$ and $k_3 = g_3 = 20$.

Here the value of $L = 10$, then $k_2 > 11$. So, we choose $k_2 = g_2 = 13$.

Then the nonlinear controller (4) becomes

$$\begin{aligned}u_1 &= -25e_1\\ u_2 &= -13e_2\\ u_3 &= 2e_1(1+e_2) - 20e_3\end{aligned} \tag{14}$$

Then the error system (3) can be written as

$$\begin{aligned}\dot{e}_1 &= e_2e_3 - 9e_2 - 10e_3 - 25e_1\\ \dot{e}_2 &= -ae_1 - 2e_2 + e_2e_3 + 10e_3\\ \dot{e}_3 &= -8e_1 - e_2^2 - 30e_2 + e_1e_2 - 20e_3\end{aligned} \tag{15}$$

The time variation of the error system (15) using nonlinear feedback controller can be depicted in Fig. 3. Let $r(t)$ be the synchronization error of the system (1) and (2) and it can be described as $r(t) = \sqrt{e_1^2 + e_2^2 + e_3^2}$. The evolution of the synchronization error $r(t)$ using nonlinear feedback controller with various time $t$ is depicted in Fig. 4.

For the above values, the linear controller (10) becomes

$$\begin{aligned}v_1 &= -25e_1\\ v_2 &= -13e_2\\ v_3 &= -20e_3\end{aligned} \tag{16}$$

Then the error system (9) can be written as

$$\begin{aligned}\dot{e}_1 &= e_2 - 25e_1\\ \dot{e}_2 &= -ae_1 - 12e_2\\ \dot{e}_3 &= -20e_3\end{aligned} \tag{17}$$

The time variation of the error system (17) using linear feedback controller can be depicted in Fig. 5. The evolution of the synchronization error $r(t)$ using linear feedback controller with various time $t$ is depicted in Fig. 6.

**Remark 2.3.** From Fig. 3, the errors $e_1$, $e_2$ and $e_3$ are tend to zero when $t \geqslant 1.3$ and the trajectory of $r(t)$ tends to zero when $t \geqslant 1.4$, see Fig. 4.

**Remark 2.4.** From Fig. 5, the errors $e_1$, $e_2$ and $e_3$ are tend to zero when $t \geqslant 0.3$ and the trajectory of $r(t)$ tends to zero when $t \geqslant 0.4$ by Fig. 6.

**Result 2.5.** From the above remarks, one can easily realize that the error of the synchronization of chaotic systems (1) and (8) using linear feedback control is 10 times less than the synchronization of chaotic systems (1) and (2) using nonlinear feedback control for the same feedback gains.

**Result 2.6.** As the synchronization cost and error are reduced by using linear feedback control for synchronizing the systems (1) and (8), it is very useful to apply linear feedback controllers in real life applications for secure communications are concerned. Hence the synchronized chaotic systems (1) and (8) are applied into ElGamal cryptosystem to improve the security level which will be presented in the next section.

## 3. Application of the proposed synchronized chaotic systems

In this section, the proposed integer order synchronized chaotic systems are applied into the famous ElGamal [15] cryptosystem with the help of the Fibonacci $Q$ matrix. It has so many applications in recent technologies including PGP, GNU and, etc.

Some basic assumptions are needed to describe the ElGamal cryptosystem via Diffie–Hellman key exchange and they can be given as follows.

Consider the Fibonacci $Q$ matrix as in [16] given by

$$Q = \begin{pmatrix} 1 & 1\\ 1 & 0\end{pmatrix} \tag{18}$$

Then for any integer $n \geqslant 1$ the $n$th power of $Q$ matrix has the form

$$Q^n = \begin{pmatrix} F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix} \tag{19}$$

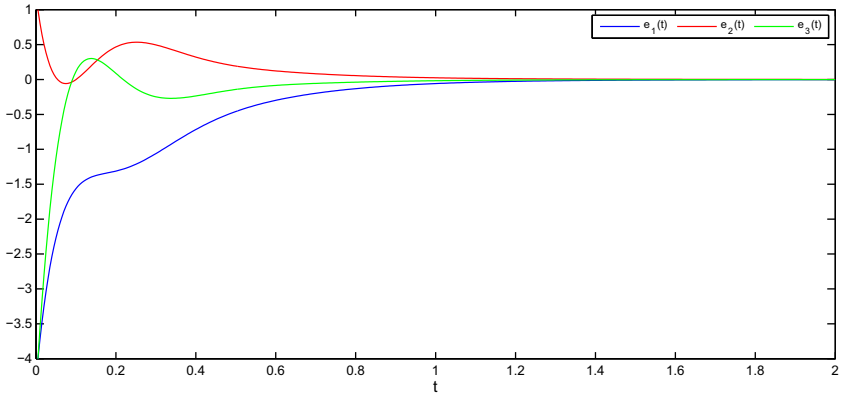


**Fig. 3** Time variation of the error system using nonlinear feedback control.

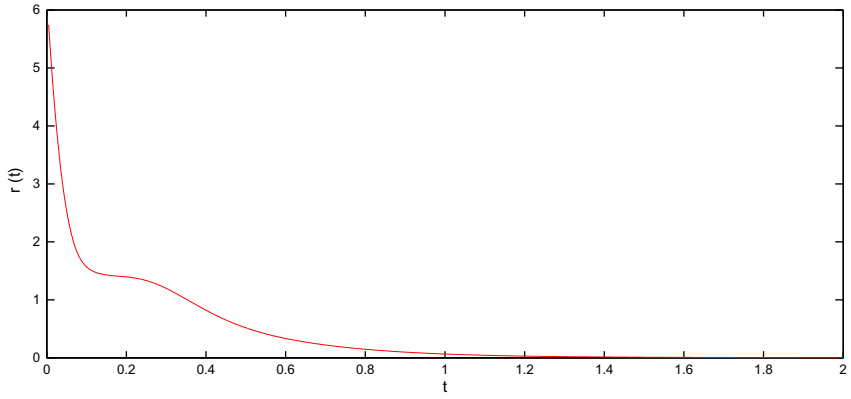


**Fig. 4** The evolution of the synchronization error $r(t)$ using nonlinear feedbaack control.

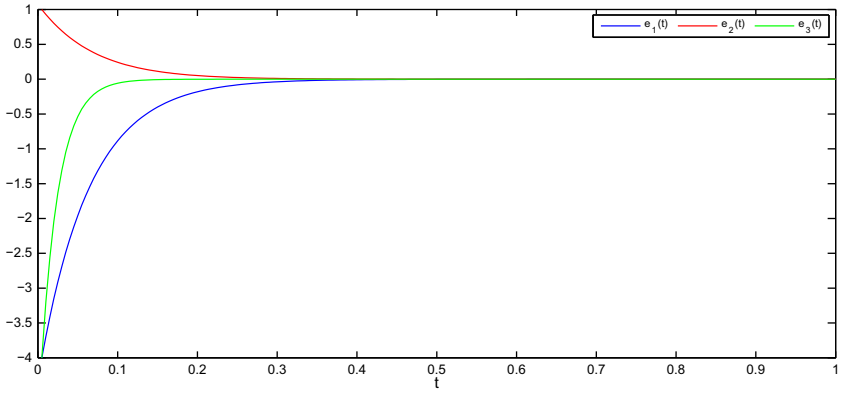


**Fig. 5** Time variation of the error system using linear feedback control.

The plaintext ($p$) can be divided into message units. Consider the assignment of numbers for unit messages as given in Table 1.

The plain text can be arranged into sequence of integers $p_1$, $p_2$, $p_3$, $p_4$, ..., $p_n$ using Table 1. Divide the sequence $p_1$, $p_2$, $p_3$, $p_4$, ..., $p_n$ into blocks of four terms. Consider the first four terms $p_1$, $p_2$, $p_3$, $p_4$ as a first block and let it be $M_1$, $p_5$, $p_6$, $p_7$, $p_8$ as a second block and let it be $M_2$, and so on. If the total term of plaintext sequence is not a multiple of 4, then include the necessary blank spaces at the end of the sequence to complete the sequence as a multiple of 4. Choose the first block and form a $2\times 2$ square matrix $M_1 = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$. Do the same for another blocks.

Consider two cryptographic entities Alice and Bob and let Alice be a sender and Bob be a receiver. Consider the driving system (1) as a sender system and the response system (8) as a receiver system. The synchronization error $r(t)$ of the system (1) and (8) tends to zero after time $t \geqslant 0.4$ and hence $x_1 = x$, $y_1 = y$, $z_1 = z$ after $t_0 = 0.4$.

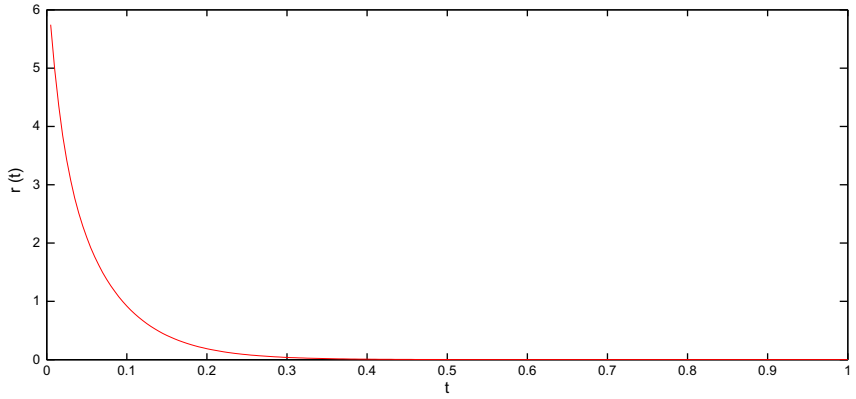


**Fig. 6** The evolution of the synchronization error $r(t)$ using linear feedback control.

### *3.1. Diffie–Hellman key exchange based on synchronized chaotic systems*

The security of many cryptographic techniques depends on the intractability of the discrete logarithm problem. The concept of a public key construction based on discrete logarithm problem was introduced by Diffie–Hellman [17] in 1976. It was a brilliant insight of Diffie and Hellman that the difficulty of the discrete logarithm problem and finding their solution. Here, we describe the Diffie–Hellman key exchange problem based on synchronized chaotic systems as follows.

Alice and Bob agree on a public element $Q$ and $n = 38$.

1. Alice to pick a secret number $t_1 > t_0$ and compute $x$ at $t_1$ from (1) that she keeps secret. She calculates $s = [t_1 * \mid x \mid] \pmod{38}$ where $[a]$ is the integer part of $a$ and $\mid b \mid$ is the modulus value of $b$.
2. Alice computes $A = Q^s \pmod{38}$ and sends to Bob.
3. Bob to pick a secret number $t_2 > t_0$ and compute $x_1$ at $t_2$ from (8) that he keeps secret. He calculates $r = [t_2 * \mid x_1 \mid] \pmod{38}$.
4. Bob computes $B = Q^r \pmod{38}$ and sends to Alice.
5. Alice generates key $K_A = B^s = (Q^r)^s \pmod{38}$.
6. Bob generates key $K_B = A^r = (Q^s)^r \pmod{38}$.

Their common secret key $K = K_A = K_B$, since $(Q^r)^s = Q^{rs} = (Q^s)^r$.

**Remark 3.1.** In the general Diffie–Hellman algorithm, the sender and receiver should pick an integer for computing the discrete logarithm. The proposed Diffie–Hellman algorithm is developed to relax the restriction of choosing integer so that it is valid for all numbers.

### *3.2. ElGamal cryptosystem*

It is a public key cryptosystem which is based on the Diffie–Hellman key exchange. ElGamal encryption is probabilistic. Consider the assumptions of the proposed Diffie–Hellman key exchange and the completed encryption and decryption process of the ElGamal cryptosystem based on synchronized chaotic systems as described by

1. Alice picks a random secret number $t_1 > t_0$ and compute $x$ at $t_1$ from (1). Then set $s = [t_1 * \mid x \mid] \pmod{38}$, she calculates and publishes $C = Q^s \pmod{38}$.
2. Bob wants to send a message $M \in M_2(\mathbb{R})$ to Alice.
3. Bob picks a random secret number $t_2 > t_0$ and compute $x_1$ at $t_2$ from (8). Then set $r = [t_2 * \mid x_1 \mid] \pmod{38}$, he computes $D = Q^r \pmod{38}$.
4. Bob sends two elements $D$ and $E_i = M_i(C^r) \pmod{38}$ to Alice where $i = 1, 2, \ldots, m$.
5. Alice recovers a message $M_i = E_i(D^s)^{-1} \pmod{38}$.

The ElGamal cryptosystem should be applied to communication systems where both parities are not able to interact in reasonable time due to delays in transmission. The numerical illustration of the proposed ElGamal cryptosystem will be given in the next section.

### *3.3. Numerical example*

Alice picks a random number $t_1 = 4.985$, then get $x = -0.2637$ by solving the system (1) at $t_1$ and calculates $s = [t_1 * \mid x \mid] = 1 \pmod{38}$. She computes $C = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \pmod{38}$ and sends $A$ to Bob.

Bob wants to send a message $M =$ **MEET AT SPA**. $M$ has 11 characters, which is not a multiple of 4. So, insert a one black space at the end of the message. Then Bob split a message into 3 blocks let it be $M_1$,$M_2$ and $M_3$.

Bob picks a random number $t_2 = 10.10$, then get $x_1 = 0.7058$ by solving the system (8) at $t_1$ and calculates $r = [t_2 * \mid x_1 \mid] = 7 \pmod{38}$.

Bob takes a first block, $M_1 = \begin{pmatrix} M & E \\ E & T \end{pmatrix} = \begin{pmatrix} 24 & 16 \\ 16 & 31 \end{pmatrix} \pmod{38}$ since by Table 1.

**Table 1** Assignment of numbers with unit messages.

| Number assigned | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | ... | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unit message | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | – | . | A | B | ... | Z |

He computes $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^s = \begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix}$ and $E_1 = M_1 * C^r = \begin{pmatrix} 28 & 22 \\ 17 & 38 \end{pmatrix} \pmod{38}$.

Then he sends $D$ and $E_1$ values to Alice.

Alice recovered a message $M_1$,

$$M_1 = E_1(D^s)^{-1} = \begin{pmatrix} 28 & 22 \\ 17 & 38 \end{pmatrix}\begin{pmatrix} 21 & 13 \\ 13 & 8 \end{pmatrix}^{-1} = \begin{pmatrix} 24 & 16 \\ 16 & 31 \end{pmatrix} \pmod{38} = \begin{pmatrix} M & E \\ E & T \end{pmatrix}.$$

Continue the procedure for $M_2$ and $M_3$.

Finally, Alice recover a original message $M$ = **MEET AT SPA** from $M_1$, $M_2$ and $M_3$.

In every cryptosystem, the security is very important. It will be analyzed in the next section for proposed ElGamal cryptosystem.

## 4. Security analysis

The security of proposed ElGamal public key cryptosystem depends on the perception and consensus of experts as to the difficulty of problems such as integer factorization (IFP) and discrete logarithm (DLP).

### 4.1. DLP attack

Suppose an Adversary (ADV) recovers the private key by solving the DLP. Then compute the value of $Q^{rs} \pmod{n}$ and tries to recover a message $M$. But it is not sufficient to recover $M$ because the decryption $M = E * (D^s)^{-1} \pmod{n}$ involves inverse problem and IFP.

To recover a message $M$, ADV needs to solve the inverse problem modulo $n$. The process finding the solution of the inverse congruence is computationally infeasible since ADV does not known the factorization of $n$ and difficult to find the value of $E$. So ADV faced many difficulties and problems to recover the information or a message $M$. Hence ADV would fail to recover a message $M$ by using DLP attack.

### 4.2. IFP attack

Suppose ADV successfully factoring an integer $n$ into primes $p$ and $q$. Then ADV computes the value of $C$, $D$, $E \pmod{n}$ by solving congruence modulo $p$ and modulo $q$ and using Chinese Remainder Theorem.

To recover a message $M$, ADV needs to find the values $r$ and $s$. But $r$ and $s$ are exponent of $Q$ but $Q$ is only shared by Alice and Bob. So ADV compulsorily to solve two DLP along with primes $p$ and $q$ for finding the values of $r$ and $s$. Hence ADV would fail to recover the values $r$ and $s$ since it is very difficult to solve the DLP of modulo primes $p$ and $q$. Moreover, $s$ and $r$ are computed from the chaotic systems (1) and (8) respectively and solving these chaotic systems is very difficult. So, ADV would fail to recover a message $M$ by using IFP attack.

Finally ADV would fails to recover a message $M$ by solving both matrix DLP and IFP.

**Remark 4.1.** From the security analysis of the proposed cryptosystem, we conclude that the proposed cryptosystem is stronger than the usual ElGamal cryptosystem due to additional hardness of choosing $r$ and $s$ because finding the value of $x$ and $x_1$ from synchronized chaotic systems is very hard from (1) and (8) at time $t_1$ and $t_2$ respectively.

## 5. Conclusions

Linear and nonlinear feedback controllers are designed to realize drive-response synchronization of an existing chaotic system. It has shown that synchronization using linear feedback control method is suitable and efficient than nonlinear control method due to less synchronization cost and synchronization error. The novel Diffie–Hellman key exchange protocol is presented based on synchronized chaotic systems using linear control with the support of Fibonacci $Q$ matrix and that protocol is generalized to pick a number to computing discrete logarithm instead of an integer. ElGamal cryptosystem based on novel Diffie–Hellman key exchange protocol has been proposed and the numerical example has been fully exhibited. Further, we have shown that the security of the proposed cryptosystem is stronger than the usual ElGamal cryptosystem due to the hardness of DLP and IFP and the additional securities.

## Acknowledgements

This work is supported by the University Grants Commission-Basic Science Research (UGC-BSR), Government of India, New Delhi. The authors are very thankful to the editors and anonymous reviewers for their careful reading, constructive comments and fruitful suggestions to improve this manuscript. The comments of the anonymous reviewer are more useful to improve the paper by using the linear feedback control method for synchronizing chaotic systems with less cost and error than the nonlinear feedback control method.

## References

[1] L.M. Pecora, T.L. Carroll, Synchronication in chaotic systems, Phys. Rev. Lett. 64 (1990) 821–824.
[2] T.L. Carroll, L.M. Pecora, Synchronizing chaotic circuits, IEEE Trans. Circ. Syst. I Fundam. Theory Appl. 38 (1991) 453–456.
[3] M.T. Yassen, Controlling chaos and synchronization for new chaotic system using linear feedback control, Chaos Solitons Fract. 26 (2005) 913–920.
[4] Ju.H. Park, On synchronization of unified chaotic systems via nonlinear control, Chaos Solitons Fract. 25 (2005) 699–704.
[5] Ju.H. Park, Adaptive modified projective synchronization of a unified chaotic system with an uncertain parameter, Chaos Solitons Fract. 34 (2007) 1552–1559.
[6] Z. Wang, Chaos synchronization of an energy resource system based on linear control, Nonlinear Anal.: Real World Appl. 11 (2010) 3336–3343.
[7] X. Wang, Y. Wang, Adaptive control for synchronization of a four-dimentional chaotic system via a single variable, Nonliner Dyn. 65 (2011) 311–316.
[8] X. Shi, Z. Wang, Adaptive synchronization of the energy resource systems with mismatched parameters via linear feedback control, Nonlinear Dyn. 69 (2012) 993–997.
[9] S. Boccaletti, A. Farini, F.T. Arecchi, Adaptive synchronization of chaos for secure communication, Phys. Rev. E 55 (1997) 4979–4981.

[10] T-I. Chien, T-L. Liao, Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization, Chaos Solitons Fract. 24 (2005) 241–255.
[11] G-j. Xing, D-b. Huang, Encoding–decoding message for secure communication based on adaptive chaos synchronization, J. Shanghai Univ. (Engl. Ed.) 12 (2008) 400–404.
[12] S. Banerjee, A.R. Chowdhury, Lyapunov function, parameter estimation, synchronization and chaotic cryptography, Commun. Nonlinear Sci. Numer. Simulat. 14 (2009) 2248–2254.
[13] M. Mitra, S. Banerjee, Digital cryptography and feedback synchronization of chaotic systems, Int. J. Mod. Phys. B 25 (2011) 521–529.
[14] I. Pehlivan, Z. Wei, Analysis, nonlinear control, and chaos generator circuit of another strange chaotic system, Turk. J. Elec. Eng. Comp. Sci. 20 (2012) 1229–1239.
[15] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory IT 31 (1985) 469–473.
[16] J.R. Silvester, Fibonacci properties by matrix methods, Math. Gaz. 63 (1979) 188–191.
[17] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (1976) 644–654.