Sliding Mode Control for Multi-scale Synchronization of Multi-scroll Fractional Order Chaotic Systems and Its Applications

P. Muthukumar, *Member, IAENG,* and M. Nirmala Devi

***Abstract*—In this study, a fractional order dynamical system in four dimensions is constructed. It is found that the proposed system displays multi-scroll chaotic attractors without modifying the nonlinear functions and parameter values inside the system. Furthermore, the multi-scale synchronization between two identical multi-scroll fractional chaotic systems is achieved by applying sliding mode control theory. Inspired by the applications of fractional order dynamical systems, synchronized fractional multi-scroll chaotic systems are used to built a new key agreement protocol for all kinds of cryptosystems. The efficiency and security of the key agreement protocol are examined. Using numerical examples, the anticipated theoretical results are demonstrated.**

***Index Terms*—Fractional order system, Sliding mode control, Chaos, Multi-scale synchronization, Cryptography.**

I. Introduction

Fractional calculus is an effective mathematical tool that allows for integration and differentiation of non-integer order. Its history dates back 300 years, just like that of regular calculus. Recent years have seen a rise in interest in fractional order system dynamics because of its potential applications in engineering and science. In this way, many dynamical systems are modeled by fractional differential equations and expose productive fractional dynamical behaviours, for instance, see ([1], [2], [3], [4], [5], [6], [7]). Moreover, the control and synchronization of fractional order chaotic systems have received much research interest among researchers and various control techniques have been investigated for synchronization of fractional order dynamical systems in [8]-[9]. Among various types of control techniques, the sliding mode control is an effective robust method to control nonlinear and uncertain systems because it can switch the control law very quickly to drive the system states from any initial states onto a user-defined sliding surface, and to keep the system states on the surface for all subsequent time [10]. The system on the surface has desired performance, such as stability, disturbance rejection capability, and tracking ability. For instance, the global practical stabilization problem has been addressed for a class of non-holonomic mobile robots by using switching control in [11]. The stabilization of a class of linear uncertain fractional order dynamical system based on sliding mode control approaches has been investigated in [12]. An adaptive sliding mode controller [13] for a novel class of fractional order chaotic systems with uncertainty and external disturbance has been studied to realize chaos control. Consequently, the sliding mode control is widely used for synchronization of fractional order dynamical systems [14], [15], [16], [17], [18], [19], [20], [21], [22], [23].

In recent years, the chaotic system has been used in cryptography for secure communication as well as message encryption and decryption. A digital chaotic secure communication system has been proposed by introducing a concept magnifying glass to enlarge observed errors in [24]. Color image encryption scheme using one-time keys based on coupled chaotic systems has been demonstrated in [25]. A complete dislocated general hybrid projective synchronization method has been applied to secure communications in [26]. In [27], an advanced encryption standard algorithm has been developed for image encryption based on chaotic map. Further, the different types of secure communication schemes based on fractional order chaotic systems have been investigated in [28], [29], [30], [31], [32], [33]. The key agreement between the sender and the receiver is very important for every secure communication systems. The first public key construction and key agreement protocol based on the discrete logarithm problem in a finite field have been introduced by Diffie and Hellman [34]. The authors [35] are interested in chaos, the Diffie-Hellman key agreement protocol has been described based on synchronized chaotic systems. Key agreement protocol based on infinite non-commutative group presentation and representation levels have been handled in [36]. Also, the key agreement between the sender and receiver in a communication system have been constructed based on chaotic system and chaotic maps to improve the security of the key strength, for more details see [37]-[38].

A greater amount of attention has been paid in previous years to the study of multi-scroll integer order and fractional order chaotic systems because of their wide variety of dynamical behaviours [39], [40], [41], [42], [43]. In [39], [40], [41], [42], [43], the multi-scroll has been generated only by changing parameters of the system or functions involving that system. Therefore, multi-scrolls cannot be formed from a single chaotic system. It is a major drawback to generate multi-scrolls in a chaotic system. The main objective of this paper is to overcome these drawbacks by generating multi-scrolls in a dynamical system without changing any

Manuscript received January 5, 2024; revised September 12, 2024.

P. Muthukumar is a senior assistant professor in the PG and Research Department of Mathematics, Gobi Arts & Science College (Bharathiar University), Gobichettipalayam- 638 453, Erode, Tamil Nadu, India. (Corresponding author, e-mail: muthukumardgl@gmail.com).

M. Nirmala Devi is a research scholar in the PG and Research Department of Mathematics, Gobi Arts & Science College (Bharathiar University), Gobichettipalayam- 638 453, Erode, Tamil Nadu, India.(e-mail: nirmala1479@gmail.com).

parameter values and nonlinear functions of the system.

This paper introduces a novel 4-D fractional order dynamical system. The stability and chaotic behaviors of the system are investigated by theoretically and numerically. We show that, the proposed system generates 2-scroll, 3-scroll and 4-scroll chaotic attractors for fixed parameter values and nonlinear functions. Hence, the main objective of this paper is achieved. The multi-scale synchronization method is applied for synchronizing two identical fractional order multi-scroll chaotic systems. At the first time, synchronized fractional order multi-scroll chaotic systems are utilized to construct a key agreement protocol using conjugator search problem and discrete logarithm problem for cryptographic applications. The security level of the proposed system is stronger than an existing key agreement protocol based on conjugate search problem and discrete logarithm problem due to their hardness and the solutions of the fractional order multi-scroll chaotic systems.

This paper is organized as follows: In Section II, some basic definitions and theorems related to fractional order dynamics are presented. In Section III, a novel fractional order dynamical system is established and its dynamical behaviours are examined. Section IV causes the multi-scale synchronization method between two fractional order multi-scroll chaotic systems and their performances are examined. Section V introduces a new key agreement protocol for cryptosystem based on synchronized fractional order multi-scroll chaotic systems. Section VI analyzes the security of the proposed key agreement protocol. Conclusions are given in Section VII.

II. Preliminaries

Among various definitions for fractional derivatives, the definition of Caputo fractional derivative is most important than other fractional derivatives since it has the conventional initial conditions, which is described as follows:

Definition 2.1: [44] The α-order Caputo fractional derivative of function $f(t)$ with respect to t is defined by

$$D^{\alpha}f(t)=\frac{1}{\Gamma(n-\alpha)}\int_a^t (t-\tau)^{-\alpha+n-1}f^{(n)}(\tau)d\tau, \qquad (1)$$

where $n=[\alpha]+1$, $[\alpha]$ is the integer part of α, $\Gamma(\cdot)$ is the gamma function and D^{α} is called the α-order Caputo differential operator.

Theorem 2.2: [45] The autonomous system

$$D^{\alpha}x(t)=Ax(t),\ x(0)=x_0, \qquad (2)$$

where $0<\alpha\leq 1,\ x\in R^n$ is asymptotically stable if and only if

$$|\arg(eig(A))|>\frac{\alpha\pi}{2}. \qquad (3)$$

Also, this system is stable if and only if $|\arg(eig(A))|\geq\frac{\alpha\pi}{2}$ and those critical eigenvalues that satisfy $|\arg(eig(A))|=\frac{\alpha\pi}{2}$ have geometric multiplicity one.

Theorem 2.3: [46] A necessary condition for the fractional order system (2) to remain chaotic is keeping at least one eigenvalue λ in the unstable region. This means

$$\alpha>\frac{2}{\pi}\ \arctan\left(\frac{|Im(\lambda)|}{Re(\lambda)}\right). \qquad (4)$$

Definition 2.4: [46] An equilibrium point E of the system (2) is called a saddle point of index 1 (index 2) if the Jacobian matrix J at E has one (two) unstable eigenvalue(s).

III. Description of a new multi-scroll fractional order chaotic system

Consider the following four dimensional nonlinear integer order multi-scroll chaotic system, which is described in [40]

$$\begin{aligned}\dot{x}(t) &= a(y-h(x))\\ \dot{y}(t) &= x-y+z\\ \dot{z}(t) &= -b(y-w)\\ \dot{w}(t) &= -c(z+dw)\end{aligned} \qquad (5)$$

where $(x,y,z,w)\in R^4$, $h(x)=m_1\Big(\sum_{i=1}^{n-1}(-1)^i(|x+(4n-2-4i)|-|x-(4n-2-4i)|)+m_2x\Big)$ for every $n\geq 2$, $m_2=1.086$ and m_1 is the adjustable parameter.

The dynamical behaviors of the system (5) have been investigated in [40] for $a=10,b=15,c=0.05,d=27.333$. The authors in [40] have been found that, the system (5) exhibits three-scroll, four-scroll chaotic attractors at $m_1=0.381,0.385$ when $n=3,4$ respectively. Further, the system (5) exhibits five-scroll chaotic attractor for $m_1=0.41$ when $n=5$ with parameters $a=11,b=15,c=0.05$ and $d=27.333$.

Note that, an integer order system (5) has generated multi-scroll chaotic attractor for different values of nonlinear function $h(x)$ and a parameter a. Therefore, a unique chaotic system cannot generates the multi-scrolls. By motivation of the unique dynamical system to generates multi-scroll chaotic attractor, the fractional form of system (5) will be analyzed for fixed parameters a,b,c,d and fixed nonlinear function $h(x)$ as follows.

The fractional order of the system (5) is considered and the standard derivative is replaced by a fractional derivative as follows:

$$\begin{aligned}D^qx(t) &= a(y-h(x))\\ D^qy(t) &= x-y+z\\ D^qz(t) &= -b(y-w)\\ D^qw(t) &= -c(z+dw)\end{aligned} \qquad (6)$$

where $0<q<1,(x,y,z,w)\in R^4$ and a,b,c,d are the parameters of the system (6). Here D^q is the q-order differential operator in the sense of Caputo[44] and the nonlinear function $h(x)$ is fixed as $h(x)=m_1\left(\sum_{i=1}^{3}(-1)^i(|x+(14-4i)|-|x-(14-4i)|)+1.086x\right)$

Note that, parameters and nonlinear function $h(x)$ are fixed in the proposed fractional order dynamical system (6). The adjustable parameter m_1 is fixed as 0.431; the parameters a,b,c and d are also fixed as $a=12,b=15,c=0.05$ and $d=28$ respectively. The proposed system's stability and chaotic behaviors will be examined in detail in the following analysis.

A. Stability and existence of chaos

The commensurate fractional order system (6) has three equilibrium points which are found by

$$\begin{aligned} a(y-h(x)) &= 0 \\ x-y+z &= 0 \\ -b(y-w) &= 0 \\ -c(z+dw) &= 0 \end{aligned} \tag{7}$$

and they are represented as $E_0 = (0,0,0,0)$,
$E_+ = (11.9285, 0.4113, -11.5172, 0.4113)$ and
$E_- = (-11.9285, -0.4113, +11.5172, -0.4113)$.

The Jacobian matrix of the system (6) is

$$J(x,y,z,w) = \begin{pmatrix} -ah'(x) & a & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & -b & 0 & b \\ 0 & 0 & -c & -cd \end{pmatrix} \tag{8}$$

where $h'(x) = 0.431\big[-\frac{x+10}{|x+10|} + \frac{x-10}{|x-10|} + \frac{x+6}{|x+6|} - \frac{x-6}{|x-6|} - \frac{x+2}{|x+2|} + \frac{x-2}{|x-2|} + 1.086\big]$.

By linearizing the system (6) at E_0 yields the Jacobian matrix

$$J(0,0,0,0) = \begin{pmatrix} 4.7272 & 12 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & -15 & 0 & 15 \\ 0 & 0 & -0.05 & -1.4 \end{pmatrix}. \tag{9}$$

The characteristic equation of (9) is

$$\lambda^4 - 2.3272\lambda^3 - 6.1953\lambda^2 - 76.1215\lambda - 111.8166 = 0. \tag{10}$$

The eigenvalues of (10) are $\lambda_1 = 5.9962$, $\lambda_2 = -1.4845$ and $\lambda_{3,4} = -1.0923 \pm 3.3718i$.
If the Jacobian matrix (8) at E_0 has one eigenvalue with non-negative real part (unstable eigenvalue), then the equilibrium point E_0 is called a saddle point of index 1 and unstable since by Definition 2.4.

By linearizing the system (6) at $E_\pm$ yields the Jacobian matrix

$$J(x,y,z,w) = \begin{pmatrix} -5.6168 & 12 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & -15 & 0 & 15 \\ 0 & 0 & -0.05 & -1.4 \end{pmatrix} \tag{11}$$

The characteristic equation of (11) is

$$\begin{aligned} \lambda^4 + 8.0168\lambda^3 + 18.6303\lambda^2 + 101.2781\lambda \\ +113.1654 = 0 \end{aligned} \tag{12}$$

The eigenvalues of (12) are $\lambda_1 = -7.0866, \lambda_2 = -1.2791$ and $\lambda_{3,4} = 0.1744 \pm 3.5290i$.
If the Jacobian matrix (8) at $E_\pm$ has two unstable eigenvalues, then the equilibrium points $E_\pm$ are called saddle points of index 2 and unstable since by Definition 2.4.

Note that, the saddle points with index 1 is not responsible for generating scrolls around on it and the scrolls are generated only around the saddle points with index 2. Therefore the equilibrium points $E_\pm$ are responsible for generating the scrolls and E_0 is responsible for connecting the scrolls. For these equilibrium points, the system (6) is stable for every fractional order $q \leq 0.9686$ since by Theorem 2.2 and it is shown in Fig. 1.

According to the Theorem 2.3, the proposed fractional

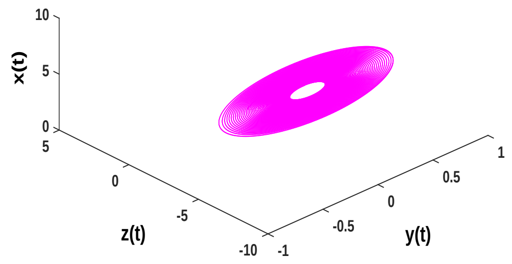

Fig. 1. 3D view of system (6) when $q = 0.96$

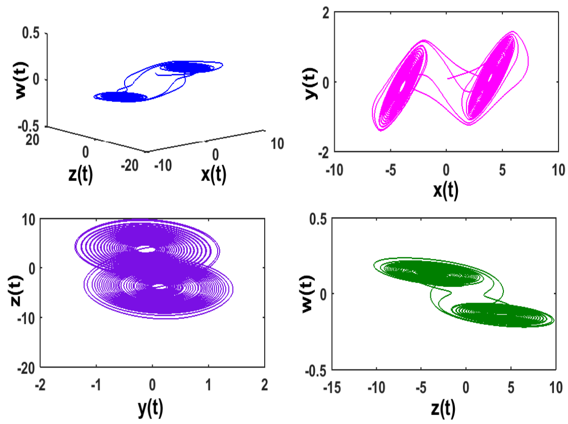

Fig. 2. Different phase portraits of the chaotic attractor of the system (6) when $q = 0.97$

order system (6) exhibits chaos when $q > 0.9686$.
That is,

$$\begin{aligned} q &> \frac{2}{\pi}\, arctan\Big(\frac{|Im(\lambda)|}{Re(\lambda)}\Big) = \frac{2}{\pi}\, arctan\Big(\frac{3.5290}{0.1744}\Big) \\ &> 0.9686 \end{aligned} \tag{13}$$

The chaotic attractors of the proposed system when $q = 0.97, q = 0.98$ and $q = 0.99$ are visualized in Figs. 2-4 respectively.

Result 3.1: 1. The proposed fractional order system (6) exhibits chaos when the fractional order $q > 0.9686$. The minimum effective dimension is 3.88.
2. If $q = 0.97, 0.98, 0.99$, then the system (6) have a two-scroll, three-scroll and four-scroll chaotic attractors by Figs. 2-4 respectively.
3. The proposed system (6) exhibits multi-scroll chaotic attractor for different fractional order q without affect the parameters and nonlinear function $h(x)$, which is completely different from surviving fractional order multi-scroll chaotic systems in [41], [42], [43].

Remark 3.2: In general, multi-scrolls have been generated only by changing parameters or nonlinear functions of the chaotic system. If the chaotic system has any one of these types of changes, then dynamical behaviors of the modified chaotic system have been entirely different from the original

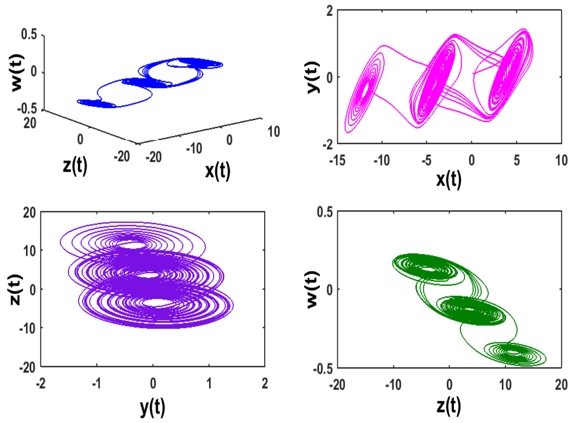

Fig. 3. Different phase portraits of the chaotic attractor of the system (6) when $q = 0.98$

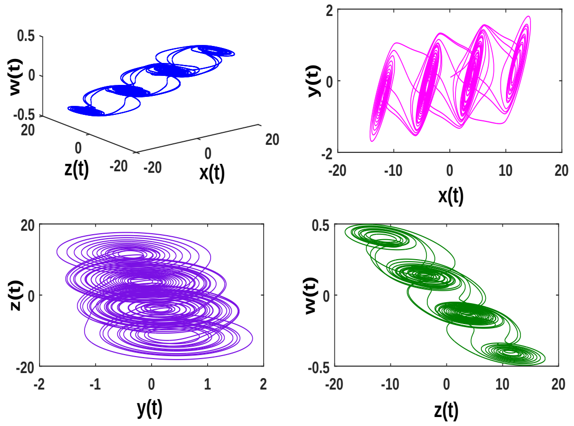

Fig. 4. Different phase portraits of the chaotic attractor of the system (6) when $q = 0.99$

chaotic system. Therefore, a single chaotic system cannot be generated multi-scrolls. As per Result 3.1, the proposed fractional order chaotic system (6) generates multi-scrolls without changing the parameters or nonlinear functions of the system. To the best of authors knowledge, there is no multi-scroll chaotic system suggested or investigated previously without changing the parameters or nonlinear functions of the system.

Remark 3.3: A special feature of the proposed multi-scroll fractional order chaotic system is that generates multi-scrolls with fixed parameters and nonlinear system functions. The proposed system has been named the '**PM chaotic system**'.

IV. Sliding Mode Control Design and Multi-Scale Synchronization

In this section, the sliding mode control theory is applied to achieve the multi-scale synchronization between two identical fractional order multi-scroll chaotic systems.

The master system is described by

$$\begin{aligned} D^q x_m(t) &= a(y_m - h(x_m)) \\ D^q y_m(t) &= x_m - y_m + z_m \\ D^q z_m(t) &= -b(y_m - w_m) \\ D^q w_m(t) &= -c(z_m + dw_m) \end{aligned} \tag{14}$$

and the slave system is described by

$$\begin{aligned} D^q x_s(t) &= a(y_s - h(x_s)) + u_1 \\ D^q y_s(t) &= x_s - y_s + z_s + u_2 \\ D^q z_s(t) &= -b(y_s - w_s) + u_3 \\ D^q w_s(t) &= -c(z_s + dw_s) + u_4 \end{aligned} \tag{15}$$

where $u = (u_1, u_2, u_3, u_4)^T$ is the controller to be determined later.

Define the error states $e_1 = x_s - \beta_1 x_m, e_2 = y_s - \beta_2 y_m, e_3 = z_s - \beta_3 z_m$ and $e_4 = w_s - \beta_4 w_m$ where $\beta_i \neq 0$, $i = 1, 2, 3, 4$ are the multi-scale factors. The ultimate aim is to find the suitable controller u such that $\lim_{t\to\infty} \|e_i(t)\| = 0$ for every i.

Then the fractional order error dynamical system is written as

$$\begin{aligned} D^q e_1(t) &= ae_2 - a(h(x_s) - \beta_1 h(x_m)) + u_1 \\ D^q e_2(t) &= e_1 - e_2 + e_3 + u_2 \\ D^q e_3(t) &= -b(e_2 - e_4) + u_3 \\ D^q e_4(t) &= -c(e_3 + de_4) + u_4 \end{aligned} \tag{16}$$

For every $\eta_i > 0$, the sliding surface is defined in the space of the synchronization errors as

$$s_i(t) = e_i(t) + \eta_i D^{-q} e_i(t), \;\; i = 1, 2, 3, 4. \tag{17}$$

When the fractional order system operates in the sliding mode, it satisfies the following conditions

$$s_i(t) = 0 \text{ and } \dot{s}_i(t) = 0, \;\; i = 1, 2, 3, 4.$$

Consider

$$\dot{s}_i(t) = D^{1-q}(D^q(s_i(t))) = 0 \rightarrow D^q(s_i(t)) = 0. \tag{18}$$

Substitute (17) into (18), we have

$$\begin{aligned} D^q(s_i(t)) &= D^q\left(e_i(t) + \eta_i D^{-q} e_i(t)\right) \\ &= D^q e_i(t) + \eta_i e_i(t). \end{aligned} \tag{19}$$

Since $\dot{s}_i(t) = 0$, we have the following sliding mode dynamics

$$D^q e_i(t) = -\eta_i e_i(t). \tag{20}$$

According to the Theorem 2.2, the fractional order system (20) is asymptotically stable. According to the sliding mode control theory, the equivalent control laws u_i^e and the discontinuous reaching laws u_i^d are selected as follows:

$$\begin{aligned} u_1^e &= a(h(x_s) - \beta_1 h(x_m)) - ae_2 - \eta_1 e_1 \\ u_2^e &= -e_1 - e_3 + (1 - \eta_2)e_2 \\ u_3^e &= b(e_2 - e_4) - \eta_3 e_3 \\ u_4^e &= c(e_3 + de_4) - \eta_4 e_4 \end{aligned} \tag{21}$$

and

$$u_i^d = \rho.sign(s_i), i = 1, 2, 3, 4, \tag{22}$$

where ρ is a positive feedback gain of the controller and

$$sign(s_i) = \begin{cases} +1, & s_i > 0 \\ 0, & s_i = 0 \\ -1, & s_i < 0. \end{cases}$$

Finally, the total control input u is selected as the summation of the equivalent control laws and the discontinuous reaching laws. It is described by

$$u_i = u_i^e + u_i^d,\ i = 1, 2, 3, 4. \tag{23}$$

Remark 4.1: The controller shown in (23) suffers from the high frequency switching near the sliding surface and chattering occurs due to $sign(\cdot)$ function. If the $sign(\cdot)$ function can be replaced by saturation function, then we avoid the chattering in the controller.

Theorem 4.2: If the controller u is selected as given in (23) for the fractional order error dynamical system (16) then their state trajectories are converge to the sliding surface $s_i = 0$, $i = 1, 2, 3, 4$. That is, the multi-scale synchronization between the fractional order chaotic systems (14) and (15) is achieved.

Proof: Consider the Lyapunov candidate function as

$$V = s_1^2 + s_2^2 + s_3^2 + s_4^2. \tag{24}$$

Then,

$$\begin{aligned}
\dot{V} &= 2\left(s_1\dot{s}_1 + s_2\dot{s}_2 + s_3\dot{s}_3 + s_4\dot{s}_4\right)\\
&= 2\left[s_1\left(D^q e_1(t) + \eta_1 e_1(t)\right) + s_2\left(D^q e_2(t) + \eta_2 e_2(t)\right)\right.\\
&\quad \left. + s_3\left(D^q e_3(t) + \eta_3 e_3(t)\right) + s_4\left(D^q e_4(t) + \eta_4 e_4(t)\right)\right]\\
&= 2\left[s_1\left(ae_2 - a(h(x_s) - \beta_1 h(x_m)) + \eta_1 e_1(t) + u_1\right)\right.\\
&\quad + s_2\left(e_1 - e_2 + e_3 + \eta_2 e_2(t) + u_2\right)\\
&\quad + s_3\left(-b(e_2 - e_4) + \eta_3 e_3(t) + u_3\right)\\
&\quad \left. + s_4\left(-c(e_3 + de_4) + \eta_4 e_4(t) + u_4\right)\right]\\
&= 2\left[s_1(-\rho sign(s_1)) + s_2(-\rho sign(s_2))\right.\\
&\quad \left. + s_3(-\rho sign(s_3)) + s_4(-\rho sign(s_4))\right]\\
&= -2\rho\left(|s_1| + |s_2| + |s_3| + |s_4|\right) < 0.
\end{aligned} \tag{25}$$

Integrating (25) from zero to t, one can obtain that

$$\int_0^t 2\rho\left(|s_1| + |s_2| + |s_3| + |s_4|\right) \leq V(0) - V(t),$$

which implies that

$$\lim_{t\to\infty} s_i(t) = 0.$$

Thus, the Lyapunov candidate function satisfies the Lyapunov stability theory. Thus, the state trajectories of the fractional order error system (16) is globally asymptotically stable since the state trajectories of the sliding surface are converges to zero as $t \to \infty$. Hence, the master system (14) and the slave system (15) are synchronized successfully. ■

A. Numerical simulation

In the numerical simulations, the initial values of the master and slave systems are taken as $(x_m(0), y_m(0), z_m(0), w_m(0)) = (0.1, 0.1, 0.1, 0.1)$ and $(x_s(0), y_s(0), z_s(0), w_s(0)) = (-0.5, 0.5, 0.5, -0.5)$ and the fractional order q is fixed as 0.99. For every i, we assume that $\rho = 0.02, \eta_i = 7$ and $\beta_i = 2$. Then, the 3D phase projection between the master system (14) and the slave system (15) are depicted in Fig. 5(a) and their corresponding time responses of the error states are depicted in Fig. 5(b). Thus, the error states are tend to zero after a time $t \geq 200$ and hence the multi-scale synchronization between the systems (14) and (15) are achieved.

V. Application to key agreement protocol

In this section, the synchronized fractional order multi-scroll chaotic systems are applied to construct a novel key agreement protocol (KAP) for cryptosystem with the help of conjugator search problem (CSP) and discrete logarithm problem (DLP). KAP is a protocol whereby a shared secret becomes available to two or more souls for promote the cryptosystems and cryptographic applications. It has important role in cryptography and it is a major component of data security in any system.

A. Proposed key agreement protocol

Consider two cryptographic entities: Alice (sender) and Bob (receiver), as well as a master system (14) for the sender and a slave system (15) for the receiver. Alice and Bob agree on three elements $q \geq 0.97$, a large prime number p and a time $t \geq t_0$ where t_0 is the time when the synchronization errors between systems (14) and (15) are tend to zero onwards.

1. Alice chooses a secret 2×2 circulant matrix A randomly and solve a system (14) at t, then she calculates $S = AXA^{-1}$ (mod p) where $X = \begin{pmatrix} \lfloor 5x_m(t)q \rfloor & \lfloor 5y_m(t)q \rfloor \\ \lfloor 5z_m(t)q \rfloor & \lfloor 5w_m(t)q \rfloor \end{pmatrix}$.
2. Alice picks an integer $s \in N$ and computes $\gamma = S^s = (AXA^{-1})^s = AX^sA^{-1}$ (mod p). She sends γ to Bob.
3. Bob chooses a secret 2×2 circulant matrix B randomly and solve a system (15)) at t, then she calculates $R = BYB^{-1}$ (mod p) where $Y = \begin{pmatrix} \lfloor 5x_s(t)q \rfloor & \lfloor 5y_s(t)q \rfloor \\ \lfloor 5z_s(t)q \rfloor & \lfloor 5w_s(t)q \rfloor \end{pmatrix}$.
4. Bob picks an integer $r \in N$ and computes $\delta = R^r = (BYB^{-1})^r = BY^rB^{-1}$ (mod p). He sends δ to Alice.
5. Alice calculates a private key
$$\begin{aligned} K_A &= A\delta^s A^{-1} = A(BY^rB^{-1})^s A^{-1}\\ &= ABY^{rs}B^{-1}A^{-1} \pmod{p}. \end{aligned}$$
6. Bob calculates a private key
$$\begin{aligned} K_B &= B\gamma^r B^{-1} = B(AX^sA^{-1})^r B^{-1}\\ &= BAX^{sr}A^{-1}B^{-1} \pmod{p}. \end{aligned}$$
7. Their common secret key is $K = K_A = K_B$ since $AB = BA$ and $Y^{rs} = X^{sr}$.

In the following subsection, the proposed key agreement protocol based on synchronized fractional order multi-scroll chaotic systems will be demonstrated numerically.

B. Numerical example

Assume that $q = 0.99, t = 220, p = 37, s = 5, r = 3$, $A = \begin{pmatrix} 3 & 5 \\ 5 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 5 & 11 \\ 11 & 5 \end{pmatrix}$. Further, assume that Alice and Bob solves the systems (14) and (15) respectively at time t for given q.

Alice calculates

$$\begin{aligned} S = AXA^{-1} &= A\begin{pmatrix} 20 & 2 \\ -14 & 37 \end{pmatrix}A^{-1}\\ &= \begin{pmatrix} 13 & 5 \\ 20 & 7 \end{pmatrix} \pmod{37}. \end{aligned}$$

$$\gamma = S^s = (AXA^{-1})^s = \begin{pmatrix} 29 & 1 \\ 4 & 13 \end{pmatrix} \pmod{37}.$$

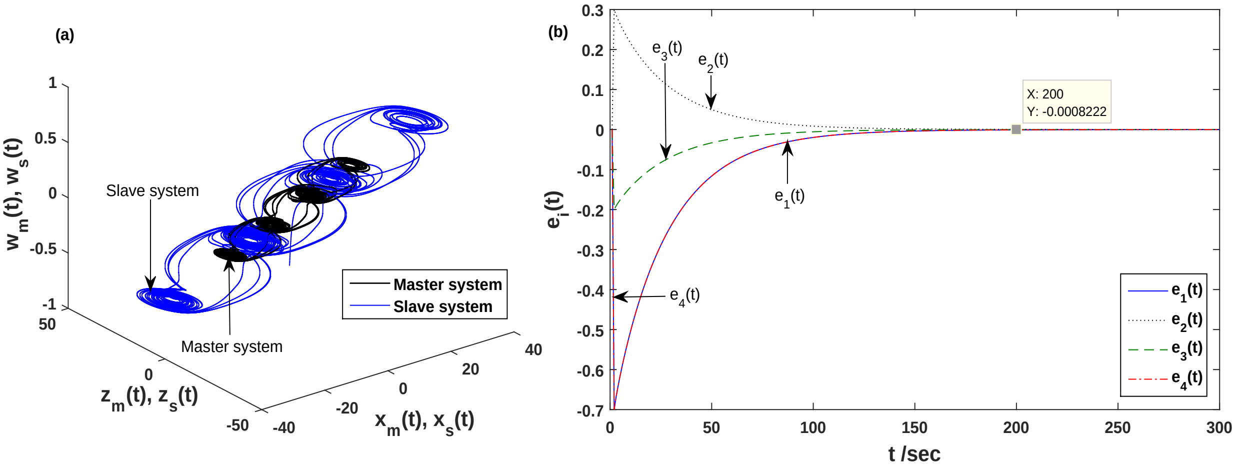

Fig. 5. Synchronization of master and slave systems: (a) Projection for state trajectories and (b) Time responses for error states

She sends γ to Bob. He calculates

$$R = BYB^{-1} = B\begin{pmatrix} 20 & 2 \\ -14 & 37 \end{pmatrix}B^{-1} = \begin{pmatrix} 24 & 1 \\ 24 & 33 \end{pmatrix} \pmod{37}.$$

$$\delta = R^r = (BYB^{-1})^r = \begin{pmatrix} 6 & 2 \\ 11 & 24 \end{pmatrix} \pmod{37}.$$

He sends δ to Alice.

Alice computes her private key

$K_A = A\delta^s A^{-1} = \begin{pmatrix} 2 & 7 \\ 29 & 4 \end{pmatrix} \pmod{37}.$

Bob computes his private key

$K_B = B\gamma^r B^{-1} = \begin{pmatrix} 2 & 7 \\ 29 & 4 \end{pmatrix} \pmod{37}.$

Finally, their common secret key $K = K_A = K_B$.

VI. Security of the Proposed KAP

The proposed KAP consists of two major problems with the supports of the solutions of fractional order multi-scroll chaotic systems, one is a matrix CSP and another one is a matrix DLP.

Consider the matrix CSP:

For given X and S find the conjugator matrix A such that

$$S = AXA^{-1}.$$

The unknown matrix A can be found by solving the homogenous matrix equation

$$SA - AX = 0.$$

It is very difficult to find the matrix A for satisfying the above homogenous matrix equation. Consider the matrix DLP:

For given G and X find the value s such that

$$G = X^s.$$

It is very difficult to find the value of s for satisfying the above DLP because the computation of the higher power of X is impossible and X is calculated from the fractional order chaotic system (14) at t.

Consider the cryptanalysis of the proposed key agreement protocol:

Assume that, the following matrix relation and the X, S values are given.

$$S = AX^sA^{-1}.$$

Suppose an Adversary (ADV) trying to obtain the secret key either K_A or K_B as mentioned in the proposed KAP.

Here X^s is unknown since s is unknown. So ADV choose the arbitrary natural number k and calculate the matrix

$$H = X^k$$

Then making the relation with known matrices S and H such that

$$S = A_1HA_1^{-1}.$$

The matrix A_1 can be determined by solving matrix CSP and obtain a matrix A_1 instead of A.

Finally ADV can try to obtain the secret key for an arbitrary natural number l such that

$$K_{A_1} = A_1H^lA_1^{-1} = A_1(BX^kB^{-1})^lA_1^{-1} = A_1BX^{kl}B^{-1}A_1^{-1}.$$

Hence the cryptanalysis fails since $K_{A_1} \neq K_A$.

Hence ADV would fail to recover a secret key by solving the CSP.

ADV again trying to solve the matrix DLP by guessing some conjugator A_2 and find s from the relation

$$A_2^{-1}SA_2 = X^s.$$

It is very difficult to find the value of s from the above relation because of the hardness of matrix DLP, matrix CSP and the hardness of finding the solutions of the fractional order multi-scroll chaotic systems at a time t when secret order q.

Suppose any one could be found the value of s, then computes

$$K_{A_2} = A_2G^lA_2^{-1} = A_2(BX^sB^{-1})^lA_2^{-1} = A_2BX^{sl}B^{-1}A_2^{-1}.$$

Hence the cryptanalysis fails $K_{A_2} \neq K_A$ and $X^{sl} \neq X^{rs}$.

Hence neither A_1 nor A_2 provide a valid key determination if they are not equal to the actual matrix A. Analogously the ADV must find the exact value of s instead of arbitrary value k, which is impossible.

Finally ADV would fails to recover a secret key by solving both matrix CSP and DLP without the knowledge of the solutions of the fractional order multi-scroll chaotic system for exact t and q.

The above discussions are same for $R = BYB^{-1}, Y^r$ and K_B.

Remark 6.1: The proposed key agreement protocol is more secure than arbitrary key agreement protocol contains DLP and CSP due to the additional security of the solutions of the synchronized fractional order chaotic systems apart from the hardness of matrix DLP and CSP.

VII. Conclusions

A four dimensional fractional order dynamical system with an order as low as 3.88 is developed and chaos is observed in the new fractional system. It is discovered that the proposed system exhibits chaotic attractors with many scrolls without requiring modifications to the nonlinear functions. Using the sliding mode control technique, two commensurate fractional order multi-scroll chaotic systems have been effectively multi-scale synchronized. Furthermore, the necessary condition for guaranteeing the stability of the fractional order error dynamical system has been derived. A secure key agreement procedure has been presented based on the solutions of synchronized fractional order multi-scroll chaotic systems. The efficiency of the proposed protocol has been ascertained through security analysis. Numerical simulations have been used to verify the efficiency of the proposed protocol, which is shown to be more secure than the existing key agreement approach that involves the conjugator search problem and the discrete logarithm problem.

References

[1] D. Kusnezov, A. Bulgac, and G. Do Dang, "Quantum levy processes and fractional kinetics," *Physical review letters*, vol. 82, no. 6, p. 1136, 1999.

[2] N. Laskin, "Fractional market dynamics," *Physica A: Statistical Mechanics and its Applications*, vol. 287, no. 3, pp. 482–492, 2000.

[3] A. M. El-Sayed, "Fractional-order diffusion-wave equation," *International Journal of Theoretical Physics*, vol. 35, no. 2, pp. 311–322, 1996.

[4] R. L. Bagley and R. Calico, "Fractional order state equations for the control of viscoelasticallydamped structures," *Journal of Guidance, Control, and Dynamics*, vol. 14, no. 2, pp. 304–311, 1991.

[5] Z. U. A. Zafar, M. T. Hussain, M. Inc, D. Baleanu, B. Almohsen, A. S. Oke, and S. Javeed, "Fractional-order dynamics of human papillomavirus," *Results in Physics*, vol. 34, p. 105281, 2022.

[6] A. M. Tusset, D. Inacio, M. E. Fuziki, P. M. Costa, and G. G. Lenzi, "Dynamic analysis and control for a bioreactor in fractional order," *Symmetry*, vol. 14, no. 8, p. 1609, 2022.

[7] P. Muthukumar, N. R. Babu, and P. Balasubramaniam, "Detecting critical point of fractional-order chemical system with synchronization and application to image enhancement technique," *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, vol. 91, no. 4, pp. 661–674, 2021.

[8] S. Agrawal and S. Das, "Function projective synchronization between four dimensional chaotic systems with uncertain parameters using modified adaptive control method," *Journal of Process Control*, vol. 24, no. 5, pp. 517–530, 2014.

[9] I. N'Doye, H. Voos, and M. Darouach, "Observer-based approach for fractional-order chaotic synchronization and secure communication," *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 3, no. 3, pp. 442–450, 2013.

[10] I. U. VADIM, "Survey paper variable structure systems with sliding modes," *IEEE Transactions on Automatic control*, vol. 22, no. 2, pp. 212–222, 1977.

[11] H. Chen, J. Zhang, B. Chen, and B. Li, "Global practical stabilization for non-holonomic mobile robots with uncalibrated visual parameters by using a switching controller," *IMA Journal of Mathematical Control and Information*, pp. 543–557, 2013.

[12] A. Pisano, M. Rapaić, Z. Jeličić, and E. Usai, "Sliding mode control approaches to the robust regulation of linear multivariable fractional-order dynamics," *International Journal of Robust and Nonlinear Control*, vol. 20, no. 18, pp. 2045–2056, 2010.

[13] C. Yin, S. Dadras, S.-m. Zhong, and Y. Chen, "Control of a novel class of fractional-order chaotic systems via adaptive sliding mode control approach," *Applied Mathematical Modelling*, vol. 37, no. 4, pp. 2469–2483, 2013.

[14] H. Chen, W. Chen, and B. Chen, "Robust synchronization of incommensurate fractional-order chaotic systems via second-order sliding mode technique," in *Proceedings of the 32nd Chinese Control Conference*, pp. 3147–3151, IEEE, 2013.

[15] T.-C. Lin and T.-Y. Lee, "Chaos synchronization of uncertain fractional-order chaotic systems with time delay based on adaptive fuzzy sliding mode control," *Fuzzy Systems, IEEE Transactions on*, vol. 19, no. 4, pp. 623–635, 2011.

[16] P. Balasubramaniam, P. Muthukumar, and K. Ratnavelu, "Theoretical and practical applications of fuzzy fractional integral sliding mode control for fractional-order dynamical system," *Nonlinear Dynamics*, vol. 80, no. 1-2, pp. 249–267, 2015.

[17] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "Sliding mode control design for synchronization of fractional order chaotic systems and its application to a new cryptosystem," *International Journal of Dynamics and Control*, vol. 5, pp. 115–123, 2015.

[18] S. Kuntanapreeda, "Tensor product model transformation based control and synchronization of a class of fractional-order chaotic systems," *Asian Journal of Control*, vol. 17, no. 2, pp. 371–380, 2015.

[19] H. Delavari, "A novel fractional adaptive active sliding mode controller for synchronization of non-identical chaotic systems with disturbance and uncertainty," *International Journal of Dynamics and Control*, vol. 5, pp. 102–114, 2015.

[20] A. Gokyildirim, H. Calgan, and M. Demirtas, "Fractional-order sliding mode control of a 4d memristive chaotic system," *Journal of Vibration and Control*, vol. 30, no. 7-8, pp. 1604–1620, 2024.

[21] F. Yu, Q. Zhu, and Y. Chen, "Adaptive fractional-order fast-terminal-type sliding mode control for underwater vehicle-manipulator systems," *Journal of Mechanisms and Robotics*, vol. 15, no. 6, p. 064501, 2023.

[22] X. Tian, G. Zhao, Z. Yang, J. Ge, and H. Xie, "Backstepping-based sliding mode adaptive control for fractional-order system considering saturation phenomenon," *IAENG International Journal of Applied Mathematics*, vol. 52, no. 1, pp. 246–253, 2022.

[23] B. Subartini, S. Vaidyanathan, A. Sambas, S. Zhang, *et al.*, "Multistability in the finance chaotic system, its bifurcation analysis and global chaos synchronization via integral sliding mode control.," *IAENG International Journal of Applied Mathematics*, vol. 51, no. 4, pp. 995–1002, 2021.

[24] Z. Li, K. Li, C. Wen, and Y. C. Soh, "A new chaotic secure communication system," *Communications, IEEE Transactions on*, vol. 51, no. 8, pp. 1306–1312, 2003.

[25] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 628–640, 2014.

[26] L.-f. Zhang, X.-l. An, and J.-g. Zhang, "A new chaos synchronization scheme and its application to secure communications," *Nonlinear Dynamics*, vol. 73, no. 1-2, pp. 705–722, 2013.

[27] J. Li and H. Liu, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," *Information Security, IET*, vol. 7, no. 4, pp. 265–270, 2013.

[28] X. Wu, H. Wang, and H. Lu, "Modified generalized projective synchronization of a new fractional-order hyperchaotic system and its application to secure communication," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 3, pp. 1441–1450, 2012.

[29] I. N'Doye, H. Voos, and M. Darouach, "Observer-based approach for fractional-order chaotic synchronization and secure communication," *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 3, no. 3, pp. 442–450, 2013.

[30] J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721–1729, 2015.

[31] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "Fast projective synchronization of fractional order chaotic and reverse chaotic systems with its application to an affine cipher using date of birth (dob)," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1883–1897, 2014.

[32] N. Khan and P. Muthukumar, "Transient chaos, synchronization and digital image enhancement technique based on a novel 5d fractional-

order hyperchaotic memristive system," *Circuits, Systems, and Signal Processing*, vol. 41, no. 4, pp. 2266–2289, 2022.
[33] P. Muthukumar and N. Khan, "The large key space image encryption algorithm based on modulus synchronization between real and complex fractional-order dynamical systems," *Multimedia Tools and Applications*, vol. 82, no. 12, pp. 17801–17825, 2023.
[34] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.
[35] P. Balasubramaniam and P. Muthukumar, "Synchronization of chaotic systems using feedback controller: An application to diffie–hellman key exchange protocol and elgamal public key cryptosystem," *Journal of the Egyptian Mathematical Society*, vol. 22, no. 3, pp. 365–372, 2014.
[36] E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis, "Key agreement protocol (kap) using conjugacy and discrete logarithm problems in group representation level.," *Informatica, Lith. Acad. Sci.*, vol. 18, no. 1, pp. 115–124, 2007.
[37] X. Wang and J. Zhao, "An improved key agreement protocol based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 4052–4057, 2010.
[38] P. Gong, P. Li, and W. Shi, "A secure chaotic maps-based key agreement protocol without using smart cards," *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2401–2406, 2012.
[39] L. Wang, "3-scroll and 4-scroll chaotic attractors generated from a new 3-d quadratic autonomous system," *Nonlinear dynamics*, vol. 56, no. 4, pp. 453–462, 2009.
[40] D. Chen, Z. Sun, X. Ma, and L. Chen, "Circuit implementation and model of a new multi-scroll chaotic system," *International Journal of Circuit Theory and Applications*, vol. 42, no. 4, pp. 407–424, 2014.
[41] F. Chen, L. Xia, D. Guo, and Y. Liu, "A fractional-order multi-scroll chaotic system," *Journal of Information & Computational Science*, vol. 10, no. 4, pp. 1203–1211, 2013.
[42] C. Zhang and S. Yu, "Generation of multi-wing chaotic attractor in fractional order system," *Chaos, Solitons & Fractals*, vol. 44, no. 10, pp. 845–850, 2011.
[43] W. M. Ahmad, "Generation and control of multi-scroll chaotic attractors in fractional order systems," *Chaos, Solitons & Fractals*, vol. 25, no. 3, pp. 727–735, 2005.
[44] M. Caputo, "Linear models of dissipation whose q is almost frequency independent—ii," *Geophysical Journal International*, vol. 13, no. 5, pp. 529–539, 1967.
[45] D. Matignon, "Stability results for fractional differential equations with applications to control processing," in *Computational engineering in systems applications*, vol. 2, pp. 963–968, Lille France, 1996.
[46] M. S. Tavazoei and M. Haeri, "A necessary condition for double scroll attractor existence in fractional-order systems," *Physics Letters A*, vol. 367, no. 1, pp. 102–113, 2007.

Dr. P. Muthukumar holds the position of Assistant Professor (Senior Grade) in the PG & Research Department of Mathematics at Gobi Arts & Science College (Affiliated to Bharathiar University), Gobichettipalayam, Tamil Nadu, India since 2017. He received his M.Sc. in Mathematics from Madurai Kamaraj University, India in 2006, and his M.Phil. degree in Mathematics from Gandhigram Rural Institute-Deemed University, India in 2007. Subsequently, he worked for four years as a lecturer in Mathematics . In 2015, The Gandhigram Rural Institute-Deemed University, Gandhigram, India awarded him a Ph.D. in Mathematics. He worked as a Postdoctoral Fellow (PDF) at the Institute of Mathematical Sciences, University of Malaya, Malaysia from 2015 to 2016. He is actively involved in the academic community, being a member of prestigious organizations such as the International Association of Engineers (IAENG) in Hong Kong, Cryptology Research Society of India (CRSI) in Kolkata, International Institute of Organized Research (I2OR) in India, American Mathematical Society (AMS) in USA and Zentralblatt MATH (zbMATH) in Germany. His expertise is recognized in various scholarly circles, as evidenced by his role on the editorial boards of several SCI-indexed journals. His research spans a broad spectrum of Mathematics, including stability analysis, dynamical systems, fractional calculus, chaos theory, synchronization, number theory and cryptography. He has contributed significantly to the field with numerous publications in high-impact journals indexed by Scopus, SCI, and Web of Science.

M. Nirmala Devi was born on 14th October 1979 in Madurai, Tamil Nadu, India. She completed her under graduation in the field of Mathematics (B.Sc) in Madurai Kamaraj University, Madurai in 1999. She received her M.Sc. in Mathematics at Mannar Thirumalai Naicker College, Pasumalai , Madurai, in 2001 which is affiliated to Madurai Kamaraj University. In pursuit of her passion for mathematics she pursued her Mater of Philosophy in 2014 at Madurai Kamaraj University. Building upon her rich academic and passion for mathematical inquiry she now sets her sights on a new frontier the pursuit of a Doctor of Philosophy (Ph.D) degree in Mathematics at Gobi Arts & Science College, Gobichettipalayam, in the year 2022 in the study on different synchronization techniques of chaotic systems and its applications.