International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

IJSR

Vol. (5), No. (8) August 2026 الإصدار (5)، العدد (8)

Encrypted Dynamic Control with Stability Tests and Application to Pantograph-Catenary Systems

Adel Ahmed Hassan Kubba
Associate Professor, Faculty of Education, Nile Valley University, Sudan
adelkubba60@gmail.com

Amna Hamid Mohammed Hamid
Mathematics Teacher at the Ministry of Education, Sultanate of Oman
amana,h080@moe.com, amanaoman579@gmail.com

Abstract

This paper addresses the challenges of implementing linear dynamic controllers on encrypted data using homomorphic encryption, focusing on the problem of scaling factor accumulation that leads to performance instability when operating systems with non-integer matrices over long time horizons. The paper demonstrates that integer matrices represent a fundamental solution to this problem, allowing signal scale to remain fixed throughout the operation without the need for re-encryption or resetting. The paper also presents two tests for analyzing the stability of nonlinear systems at equilibrium points: the first determines global stability based on the sign of determinants, while the second relies on Gershgorin criteria for local stability. The tests are applied to a dynamic system model of the pantograph-catenary system, identifying stability and instability regions in the parameter plane, and studying the influence of pantograph speed on system stability. Numerical results demonstrate the effectiveness of the proposed mathematical models in analyzing the behavior of complex physical systems.

Keywords: Homomorphic Encryption, Encrypted Control, Stability Tests, Pantograph-Catenary System, Integer State Matrix.

1. Introduction

Recent years have seen the development of networked control systems, and the threat of cyber-attacks has been a major problem. Against the intrusion of unauthorized access to computing devices in the network, the use of homomorphic encryption has been introduced, so as to protect all the data in the network by encryption while the control operation is directly performed on the encrypted data without decryption. As the significance of encrypted control is elimination of the decryption key from the network so that it decreases the vulnerability, it has been applied to various targets such as quadratic optimization, average consensus, cooperative control, model predictive control, and reset control. [11]

2. Additively Homomorphic Encryption over Integers

A. Homomorphic Encryption:

Let the set of plaintexts (unencrypted data) be given as, $Z_n := \left\{ i \in Z : -\frac{N}{2} \le i < \frac{N}{2} \right\}$, which is a set of integers, of cardinality $N \in N$. As all integers divided by N can have the remainder in Z_N, we define the modulo operation of $a \in Z$ by N, as $a \mod N := a - \left\lfloor \frac{a + \frac{N}{2}}{N} \right\rfloor N$, in which $\lfloor \cdot \rfloor$ is the floor function, so that $a \bmod N \in Z_N$ for all $a \in Z$. Then, the set Z_N is closed under modular addition and multiplication1. For the cryptosystem to be used, we consider the set C as the space of ciphertexts (encrypted data), and Enc: $Z_N \longrightarrow C$ and Dec: $C \longrightarrow Z_N$ as the encryption and decryption algorithms, respectively. As homomorphic encryption schemes allow operations over encrypted data in which the decryption of the operation result matches the result of modular arithmetic over plaintexts in Z_N, we suppose that the cryptosystem under consideration is at least additively homomorphic; with operations defined in C, it satisfies the following properties. [7]

H_1: There exists $\Delta_{Enc} \ge 0$ such that for every $m \in Z_N$, it satisfies

Dec (Enc (m)) = m + Δ mod N, with some $\Delta \in \mathbf{Z}$ such that $|\Delta| \le \Delta_{Enc}$.

H_2: There exists Add: $C \times C \longrightarrow C$ such that for every $c_1 \in C$ and $c_2 \in C$, it satisfies Dec (Add (c_1, c_2)) = Dec (c_1) + Dec (c_2) + Δ mod N, with some $\Delta \in \{-1, 0, 1\}$.

H3: There exists IntMult: $Z \times C \longrightarrow C$ such that for every $k \in Z$ and $c \in C$, it satisfies Dec (Int Mult (k, c)) = k· Dec(c) + Δ mod N, with some $\Delta \in Z$ such that $|\Delta| \le |k|$.

A remark is made about the presence of the error term Δ; it is to include recent homomorphic encryption schemes based on Learning with Errors (LWE) problem, which necessarily inject "errors" to every message being encrypted, for the sake of security. Otherwise, the use of Paillier encryption, a typical example of additively homomorphic cryptosystems, still can be considered, which satisfies H_1–H_3 with Δ = 0 for all cases.

Remark (2.1) [18] In H_1, the "injected error" Δ can be eliminated in practice. Indeed, if we use Enc_L: m Enc(m/L) and Dec_L: c $\lfloor L \cdot Dec(c) \rfloor$ instead of Enc and Dec, where $\lfloor c \rfloor$ is the rounding operation, and $1=L \in \mathbf{N}$ is such that $1/L > 2\Delta$ Enc, we obtain $Dec_L(Enc_L(m)) = \lfloor m + L\Delta \rfloor = m$. However, when it comes to H_2 and H_3, the error effect cannot be eliminated in general, especially when encrypted data are updated by the operations for unlimited number of times. Additively homomorphic

encryption schemes allow both addition and multiplication over encrypted data, but in H3, one may hope to conceal not only the information in c∈C but also the multiplier k ∈ **Z**. To this end, we consider multiplicatively homomorphic property as well, in which a separate algorithm may be used for encrypting the multipliers, in general. For example, the method presented can be employed, to make the use of the following property.

H_4: There exist Enc': $Z_N \longrightarrow C'$, Mult: $C' \times C \longrightarrow C$, and $\Delta_{Mult} \geq 0$ such that for every $k \in Z_N$ and $c \in C$, it satisfies Dec (Mult (Enc' (k), c)) = $k \cdot$ Dec (c) + Δ mod N, with some $\Delta \in Z$ such that $|\Delta| \leq \Delta_{Mult} + |k|$. Exploiting the properties H_2 and H_4, it is easily seen that matrix multiplication over encrypted messages can be done. Let us abuse notation and write c_1+c_2: = Add (c_1, c_2) and $c' \cdot c_1$:= Mult (c', c_1) for ciphertexts $c_1 \in C$, $c_2 \in C$, and $c' \in C'$, as usual, and use Enc: $Z_N^n \longrightarrow C_n$,

Enc': $\longrightarrow C'^{m\times n}$, Dec: $C_m \longrightarrow Z_N^m$, and +: $C^m \times C^m \longrightarrow C^m$ to apply the algorithms to each component of a matrix (or a vector). Then, multiplication of a vector $[c_j] \in C^n$ by a matrix $[c'_{ij}] \in C'^{m\times n}$ is defined as

$$\begin{bmatrix} c'_{11} & \cdots & c'_{1m} \\ \vdots & \ddots & \vdots \\ c'_{m1} & \cdots & c'_{mn} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} := \begin{bmatrix} c'_{11} \cdot c_1 \\ \vdots \\ c'_{m1} \cdot c_n \end{bmatrix} + \cdots + \begin{bmatrix} c'_{1n} \cdot c_1 \\ \vdots \\ c'_{mn} \cdot c_n \end{bmatrix}$$

So that for every $K \in \mathbf{Z}_N^{m\times n}$ and $c \in C^n$, it satisfies

$$\text{Dec (Enc'(K)} \cdot c) = K \cdot \text{Dec (c)} + \Delta \bmod N \qquad (1)$$

With some $\Delta \in \mathbf{Z}^n$ such that $\|\Delta\| \leq |K| + n\,\Delta_{Mult} + n - 1$, where $\|\cdot\|$ denotes the infinity norm of matrices or vectors. Utilizing the additively homomorphic properties H_2 and H_3 only, a property of matrix multiplication analogous to (1) is obtained, having either the multiplier or the multiplicand of the matrix multiplication as plaintext. For example, we define multiplication of a vector

$[c_j] \in C^n$ by a (plaintext) matrix $[k_{ij}] \in Z^{m\times n}$ as

$$\begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mn} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} := \begin{bmatrix} k_{11} \cdot c_1 \\ \vdots \\ k_{m1} \cdot c_n \end{bmatrix} + \cdots + \begin{bmatrix} k_{1n} \cdot c_1 \\ \vdots \\ k_{mn} \cdot c_n \end{bmatrix}$$

Where $k_{ij} \cdot c_j$: = IntMult (k_{ij}, c_j). Then, for every $K \in Z^{m\times n}$ and $c \in Cn$, it satisfies

$$\mathrm{Dec}(K \cdot c) = K \cdot \mathrm{Dec}(c) + \Delta \bmod N \qquad (2)$$

With some $\in Z^n$ such that $\|\Delta\| \leq \|K\| + n - 1$.

B. Problem Formulation:

Consider a continuous-time plant written by:

$$\dot{x}_p(t) = f(x_p(t) \cdot u_p(t)), \quad y_p(t) = h(x_p(t)), \quad t \geq 0, \qquad (3)$$

Where $x_p \in R^{np}$ is the state, $u_p \in R^m$ is the input, and $y_p \in R^p$ is the output of the plant, respectively. To control the plant (3), we suppose that a discrete-time linear time-invariant feedback controller has been designed as

$$x(t+1) = Fx(t) + Gy(t) + Pr(t) + e_x(t), \qquad (4)$$

$$u(t) = Hx(t) + Jy(t) + Qr(t) + e_u(t), \qquad (5)$$

$x(0) = x_0 + e_0, \quad t = 0, 1, 2, \ldots,$

Where $y(t) := y_p(t \cdot T_s) \in R^p$, $t = 0, 1, \ldots$, is the plant output discretized with the sampling time $T_s > 0$, $x(t) \in R^n$ is the state of the controller with the initial condition $x_0 \in R^n$, $r(t) \in R^q$ is the reference input, $u(t) \in R^m$ is the output of the controller, and $\{e_x(t), e_u(t), e_0\}$ are perturbations caused by, for example, quantization of signals. The discrete signal $u(t)$ is fed back to the continuous-time plant (3) as $u_p(t) = u(t)$, for $t \cdot T_s \leq t < (t+1) \cdot T_s$.

For the case when there is no perturbation, i.e., $e_x(t) \equiv 0$, $e_u(t) \equiv 0$, and $e_0 = 0$, the states and outputs of (3) and (4) are written as $x'_p(t)$, $y'_p(t)$, $x'(t)$, and $u'(t)$, respectively. The design of the controller (4) is supposed to (locally) stabilize the closed-loop system. From this rationale, we make two assumptions as follows, the first of which is for the stability of closed-loop system with respect to perturbations.

- Given $\varepsilon > 0$, there exists $\eta(\varepsilon) > 0$ such that $\sup_t(\|e_x(t)\|) \leq \eta(\varepsilon)$, $\sup_t(\|e_u(t)\|) \leq \eta(\varepsilon)$, and $\|e_0\| \leq \eta(\varepsilon)$ implies

$$\|x_p(t) - x'_p(t)\| \leq \varepsilon, \quad \|y_p(t) - y'_p(t)\| \leq \varepsilon, \qquad (6)$$

$$\|x(t) - x'(t)\| \leq \varepsilon, \quad \|u(t) - u'(t)\| \leq \varepsilon, \qquad (7)$$

For all $t \geq 0$ and $t \in N \cup \{0\}$, respectively.

In addition, the input, the state, and the output of the controller are assumed to be bounded, as follows, which is necessary because of the finiteness of the plaintext space Z^N.

- There exist compact sets $Y \subset R^p$, $R \subset R^q$, $X \subset R^n$, and $U \subset R^m$, which are known, such that $y'(t) \in Y$, $r(t) \in R$, $x'(t) \in X$, and $u'(t) \in U$, for all $t \in N \cup \{0\}$.

3. Encryption of Dynamic Systems

We show how to utilize the properties H_1–H_4 of the cryptosystem to perform the operation of the given controller (4) over encrypted data. In terms of the dynamic operation for infinite time horizon, the benefit of systems having integer state matrix is addressed. First, we deal with encryption and operation methods for real-valued signals and parameters, where the limitation on recursive multiplication by fractional numbers is to be seen. [9]

Operation over Encrypted Non-integer Real Numbers (3.1) [15] Let us begin with encryption of the input of the controller (4). Since the components of signals y(t) and r(t) are not integers in general, they are converted to elements of the plaintext space ZN, with quantization; let $\{r_{y,i}\}_{i=1}^{p}$ and $\{r_{r,i}\}_{i=1}^{q}$ of positive real numbers be step sizes for each component of $y(t) = \{y_i\}_{i=1}^{p}$ and $r(t) = \{r_i\}_{i=1}^{q}$, respectively, so that the i-th components $y_i(t)$ and $r_i(t)$ are quantized as

$$y_i(t) \mapsto \left[\frac{y_i(t)}{r_{y,i}}\right], \qquad r_i(t) \mapsto \left[\frac{r_i(t)}{r_{r,i}}\right],$$

Respectively. Then, a parameter $1 / L \geq \max(\{1 / r_{y,i}\}_{i=1}^{p} \cup \{1 / r_{r,i}\}_{i=1}^{q})$ is chosen so that they are scaled as

$$\bar{y}(t) := col\left\{\left[\frac{r_{y,i}}{L}\left[\frac{y_i(t)}{r_{y,i}}\right]\right]\right\}_{i=1}^{p} \in Z^p,$$
$$\bar{r}(t) := col\left\{\left[\frac{r_{r,i}}{L}\left[\frac{r_i(t)}{r_{r,i}}\right]\right]\right\}_{i=1}^{p} \in Z^q, \qquad (8)$$

Where col $\{\cdot\}$ is the stacking operation for column vectors. The encrypted signals $y(t) \in C^p$ and $r(t) \in C_q$ are defined as

$$y(t) := Enc(\bar{y}(t) \mod N),\ r(t) := Enc(\bar{r}(t) \mod N). \qquad (9)$$

The precision of the messages in y(t) and r(t) depends on the parameter 1/L as well as the quantizers. For example, the message in the i-th component $y_i(t) \in C$ of y(t) recovered by decryption will be obtained as

$$L \cdot Dec(y_i(t)) = L\left[\frac{r_{y,i}}{L}\left[\frac{y_i(t)}{r_{y,i}}\right]\right] + L\Delta =: r_{y,i}\left[\frac{y_i(t)}{r_{y,i}}\right] + \delta_L + L\Delta \qquad (10)$$

$$=: y_i(t) + \delta_{r,i} + \delta_L + L\Delta,$$

Where $|\delta_L| \le L/2$ and $|\delta_{r,i}| \le r_{y,i} = 2$ so that the recovered result can be made arbitrarily close6 to $y_i(t)$, by increasing the parameters $1/r_{y,i}$ and $1/L$. Thus, encrypted signals y(t) and r(t) can be understood to have the "scaled" values of y(t)/=L and r(t)/L, respectively. The computation algorithms over encrypted messages are basically performed with integers, as well, but homomorphic operations such as multiplication by real matrices are also rendered possible using additional "scaling factors". For example, with the help of homomorphic operations defined, the first output u(0) of (4) can be computed over encrypted data as

$$u(0) = \left[\frac{H}{s}\right] x(0) + \left[\frac{J}{s}\right] y(0) + \left[\frac{Q}{s}\right] r(0), \tag{11}$$

Where $1/s \ge 1$ is the scaling factor to convert the matrices to integers, and we suppose $x(0)=[0,\ldots,0]^T \in Z^n$ so that x(0)=Enc(x(0)), for simplicity. Then, according to the homomorphic properties, it satisfies

$$\begin{aligned} Dec(u(0)) = \left[\frac{H}{s}\right] Dec(x(0)) + \left[\frac{J}{s}\right] Dec(y(0)) \\ + \left[\frac{Q}{s}\right] Dec(r(0)) + \Delta \mod N \end{aligned}$$

With some $\Delta \in \mathbf{Z}$, and as in (10), the message u(0) can be recovered with sufficiently large 1/L and 1/s, as

$$\begin{aligned} Ls \cdot Dec(u(0)) &\approx s\left[\frac{J}{s}\right] y(0) + s\left[\frac{Q}{s}\right] r(0) + Ls\Delta \\ &\approx u(0). \end{aligned} \tag{12}$$

As long as the norm of the term Ls Δ can be made sufficiently small8, and the size N of plaintext space is given sufficiently large. Here, the outcome u(0) can be understood to have the message of u(0)/(Ls). Now, for the dynamic operation of (4) over encrypted data, let us try to compute $x(t) \in C^n$ and $u(t) \in C^m$, t = 1, 2,…, recursively, which are supposed to have messages of x(t) and u(t) at each time t, respectively. As a first attempt, we make the use of matrices in (3.1.4) converted to integers simply by scaling and rounding, just as in (3.1.9). For the first iteration of (4), the state x(1) can be

updated as, $x(0)=\left[\frac{F}{s}\right]x(0)+\left[\frac{G}{s}\right]y(0)+\left[\frac{P}{s}\right]r(0),$

With the factor 1=s, so that x(1) has the message of x(1)/(Ls). But from the second iteration, the state x(t), which already have been multiplied with the scaling factor 1/s, is again multiplied by the scaled matrix [F/s] for the next update.

As a result, it can be checked, by induction, that the state x(t) at time t should be of the scale $1/(Ls^t)$, i.e., x(t) should have the message of $x(t)/(Ls^t)$; if it is true at time t, and if x(t) is to be multiplied by the scaled matrix [F/s] again, the term [F/s]x(t) will have the message of the scale $1=(Ls^{t+1})$. Then, the next state x(t + 1) should be computed

$$x(t+1)=\left[\frac{F}{s}\right]x(t)+\left[\frac{G}{s^{t+1}}\right]y(t)+\left[\frac{P}{s^{t+1}}\right]r(t), \qquad (13)$$

And the message of x(t + 1) becomes of the scale $1=(Ls^{t+1})$.

Similarly, the output u(t) of the system, which is to be decrypted, is computed as

$$u(t)=\left[\frac{H}{s}\right]x(t)+\left[\frac{J}{s^{t+1}}\right]y(t)+\left[\frac{Q}{s^{t+1}}\right]r(t), \qquad (14)$$

Which it is supposed to have the message of $u(t)=(Ls^{t+1})$.

Finally, let us consider the correctness of (13). One may expect that decryption of u(t) yields the correct result as

$$Ls^{t+1} \cdot Dec(u(t)) \approx u(t) \qquad (15)$$

At each time t, and it might be correct for the first several time steps, just as in (12). However, it is hopeless as the time goes by, when the matrices in (4) are not integers so that 1/ s > 1. To see why, let us look at the left-hand-side of (14). Since the length of the range of Dec(.) is N, the length of the range that each component of the left-hand-side can cover is not more than NLs^{t+1} at each time t, which tends to zero as t tends to infinity. Hence, no matter how large the parameter N may be chosen, it is impossible to cover the range set of u(t) for the whole time.

An attempt might be made to divide the state x(t) by the accumulated factor 1/st, from time to time, in order to reset the scale of x(t) and u(t).

Systems having Integer State Matrix (3.2) [11] to describe the encryption method for controllers having integer state matrix, in this subsection, we temporarily assume that the state matrix of (4) consists of integers, i.e., $F \in \mathbf{Z}^{n\times n}$. In terms of encryption, the benefit of systems having integer state matrix is that they can be converted to systems over integers by scaling, in which the scale of the state

is fixed. To see the detail, let us convert the controller (4) to a system over integers, before the encryption. As the plant output y(t) and the reference output r(t) have already been converted to integers as (6), we choose a scaling factor $1/s_1 \geq 1$ for the matrices G and P in (4) so that the part (5) of the controller is converted to operate over integers as

$$\bar{x}(t+1) = F\bar{x}(t) + \left[\frac{G}{s_1}\right]\bar{y}(t) + \left[\frac{P}{s_1}\right]\bar{r}(t) =: F\bar{x}(t) + \bar{G}\bar{y}(t) + \bar{P}\bar{r}(t) \qquad (16)$$

$\bar{x}(0) = \left[\frac{x_0}{Ls_1}\right]$. Thanks to the state matrix F consisting of integers, it is seen that the construction is noticeably better than (13); as there is no recursive multiplication by a scaling factor as in (13), the state x(t) has the value of $x(t)=(Ls_1)$ for all t. Indeed, let the errors due to the truncation in (16) be denoted as, $\delta_x(t) := \left[\frac{G}{s_1}\right]\cdot\bar{y}(t) - \frac{Gy(t)}{Ls_1} + \left[\frac{P}{s_1}\right]\cdot\bar{r}(t) - \frac{Pr(t)}{Ls_1}$, $\delta_0 := \left[\frac{x_0}{Ls_1}\right] - \frac{x_0}{Ls_1}$, and suppose $e_x(t)$ and e_0 in (3.1.4) be given by $e_x(t)=Ls_1\delta_x(t)$ and $e_0= Ls_1\delta_0$. Then, it satisfies $x(t) = x(t)=(Ls_1)$ for all t. The conversion for the output (5) is also straightforward; with an additional factor $1/s_2 \geq 1$, it is converted as

$$\bar{u}(t) = \left[\frac{H}{s_2}\right]\bar{x}(t) + \left[\frac{J}{s_1 s_2}\right]\bar{y}(t) + \left[\frac{Q}{s_1 s_2}\right]\bar{r}(t) =: \bar{H}\bar{x}(t) + \bar{J}\bar{y}(t) + \bar{Q}\bar{r}(t) \qquad (17)$$

So that the output $\bar{u}(t)$ is of the (fixed) scale $1/(Ls_1s_2)$. Thus, the plant input u(t) can be obtained as $u(t) = Ls_1s_2\,\bar{u}(t)$, but more specifically, it is obtained as

$$u(t) = S^u(\bar{u}(t)) := \mathrm{col}\left\{ r_{u,i}\left[\frac{Ls_1s_2\cdot\bar{u}_i(t)}{r_{u,i}}\right]\right\}_{i=1}^{m}, \qquad (18)$$

Where $\bar{u}_i(t)$ is the i-th component of $\bar{u}(t)\in Z^m$, and $\{r_{u,i}\}_{i=1}^{m}$ of positive numbers are the step sizes of the quantizers for the plant inputs. As a result, we can regard the result (18) as the same as the output u(t) of (6), with the term $e_u(t)$ in (18) given as $e_u(t) = Ls_1s_2\delta_u(t) + (S^u(\bar{u}(t)) - Ls_1s_2\,\bar{u}(t)$, where

$$\delta_u(t) := \left(\left[\frac{H}{s_1}\right] - \frac{H}{s_1}\right)\bar{x}(t) + \left[\frac{J}{s_1 s_2}\right]\bar{y}(t) - \frac{Jy(t)}{Ls_1 s_2} + \left[\frac{Q}{s_1 s_2}\right]\bar{r}(t) - \frac{Qr(t)}{Ls_1 s_2}$$

Is the error caused by truncation in (16).

4. First Test of Stability

We establish a test for the asymptotic stability of the equilibrium when D is an open subset of, R_+^n = $\{(x_1,..., x_n) \in R^n : x_i \geq 0$ for i = 1,…, n$\}$.

The following proposition relates the equilibrium stability with the sign of certain determinants.

Proposition (4.1) [11] Let D be an open subset of R_+^n containing $\bar{x} = (\bar{x}_1,\ldots,\bar{x}_n\, x_n)$. Suppose that the function f: D ⟶ $\mathbf{R}^n$ defined satisfies f∈ C_1 (D) and f($\bar{x}$) = 0. Let Δ_j ($\bar{x}$) be the determinants defined by

$$\Delta_j(\bar{x}) = (-1)^j \left| \frac{a_j}{\bar{x}_j}\frac{\partial f_j(\bar{x})}{\partial x_i} + \frac{a_i}{\bar{x}_i}\frac{\partial f_i(\bar{x})}{\partial x_j} \right|_{i=1,\ldots,j}, \quad j = 1,..., n \qquad (19)$$

Where a_j is a positive constant.

i. If $\Delta_j(\bar{x})$ for j = 1,…, n are positive, then $\bar{x}$ is globally asymptotically stable.

ii. If $\Delta_j(\bar{x})$ for j = 1,…, n has alternate signs starting with a negative value, then $\bar{x}$ is unstable.

5. Second Test of Stability

The following result focus on determining conditions that allow us to establish the sign of the eigenvalues of Df$(\bar{x})$ through the Gershgorin circles.

Proposition (5.1) [20] Let $\bar{x}$ an equilibrium point of,

$$Df(\bar{x}) = \begin{pmatrix} J_{11} & J_{12} & \cdots & J_{1n} \\ J_{21} & J_{22} & \cdots & J_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ J_{n1} & J_{n2} & \cdots & J_{nn} \end{pmatrix}, \qquad (20)$$

The Jacobian matrix evaluated in $\bar{x}$ and

$$R_i = \sum_{j=1, j\neq i}^{n} |J_{ij}|, \qquad (21)$$

For i = 1,…, n. If $J_{ii} < 0$ and $R_i < |J_{ii}|$ for i = 1,…, n then $\bar{x}$ is locally asymptotically stable.

Corollary (5.2) [20] Let $\bar{x}$ an equilibrium point, $Df(\bar{x})$ defined in (19), and

$$R_j = \sum_{i=1, i\neq j}^{n} |J_{ij}|, \qquad (22)$$

For j = 1, …, n. If $J_{jj} < 0$ and $R_j < |J_{jj}|$ for j = 1, …, n then $\bar{x}$ is locally asymptotically stable.

6. Application of Stability Tests

We apply the two tests formulated to analyze the stability of the following system of ordinary differential equation:

$$\frac{dx_j}{dt} = \alpha_j x_j (1 - x_j) - \sigma_j \prod_{i=1}^{n} x_j, \qquad j = 1,2,..., n, \qquad (23)$$

Where $0 < \alpha_j < 1$ and $0 < \alpha_j < 1$ for j = 1, 2, …, n.

Stability analysis by test 1 (6.1) [22]

$$\text{Let, } D_1 = \{x \in R^n: 0 < x_j < 1, j = 1, 2,\ldots, n\}. \qquad (24)$$

The following lemma ensures that all solutions of (23) starting in the closure of D_1 denoted by D_1, remain there for all $t \geq 0$.

Proposition (6.2) [22] the system (23) has at least 2^n+1 equilibrium solution in D_1.

To proof the following proposition, we use the first test of stability.

Proposition (6.3) [22] suppose that the system (23) has an interior steady state

$$\bar{x} \in D_2 \subset D_1 \text{ where, } D_2 = \{x \in R^n: 0 < x_i < 1, 0 < x_i + x_j < 1 \text{ I}, j = 1, \ldots, n\}.$$

Then this steady state is globally asymptotically stable on the interior set of D_1.

Proof. From (23) we conclude that: $f_j = \alpha_j x_j (1 - x_j) - \sigma_j \prod_{i=1}^{n} x_k, \qquad j = 1,2,..., n,$

Which implies that

International Journal for Scientific Research, London Vol (5), No (8), 2026
https://doi.org/10.59992/IJSR.2026.v5n8p6 E-ISSN 2755-3418

$$\frac{\partial f_j(\bar{x})}{\partial \bar{x}_j} = \alpha_j\left(1-\bar{x}_j\right) - \alpha_j \bar{x}_j - \sigma_j \prod_{k=1,k\neq j}^{n} \bar{x}_k, \qquad j = 1,2,\ldots, n, \tag{25}$$

From equilibrium equations we have:

$$\alpha_j\left(1-\bar{x}_j\right) - \sigma_j \prod_{k=1,k\neq j}^{n} \bar{x}_k, \qquad j = 1,2,\ldots, n, \tag{26}$$

Therefore, substituting (25) in (26) we verify the first hypothesis of Proposition (6.3), that is, $\frac{\partial f_j(\bar{x})}{\partial \bar{x}_j} = -\alpha_j \bar{x}_j, \qquad j = 1,2,\ldots, n.$ On the other hand,

$$l_{i,j}(\bar{x}) = \left(\frac{\partial f_i(\bar{x})}{\partial \bar{x}_i}\right)^{-1} \frac{\partial f_i(\bar{x})}{\partial \bar{x}_j} + \left(\frac{\partial f_j(\bar{x})}{\partial \bar{x}_j}\right)^{-1} \frac{\partial f_j(\bar{x})}{\partial \bar{x}_i}$$

$$= \left(-\alpha_i \bar{x}_i\right)^{-1}\left(-\sigma_j \prod_{k=1,k\neq j}^{n} \bar{x}_k\right) + \left(-\alpha_j \bar{x}_j\right)^{-1}\left(-\sigma_j \prod_{k=1,k\neq j}^{n} \bar{x}_k\right)$$

$$= \left(\frac{\sigma_i}{\alpha_i} + \frac{\sigma_j}{\alpha_j}\right) \prod_{k=1,k\neq i,k\neq j}^{n} \bar{x}_k \tag{27}$$

From (26) we have:

$$\frac{\sigma_j}{\alpha_j} = \frac{1-\bar{x}_i}{\prod_{k=1,k\neq j}^{n} \bar{x}_k}, \quad j = 1,\ldots, n. \tag{28}$$

Substituting (28) in (27) we obtain: $l_{ij}(\bar{x}) = \frac{1-\bar{x}_i}{\bar{x}_j} + \frac{1-\bar{x}_j}{\bar{x}_i}, \qquad \text{for} \quad i \neq j.$

From hypothesis $\bar{x} \in D_2$, results that $0 < \bar{x}_i + \bar{x}_j < 1$ which implies

$(\bar{x}_i + \bar{x}_j)^2 < \bar{x}_i + \bar{x}_j$, or equivalently $(1-\bar{x}_i)\bar{x}_i + (1-\bar{x}_j)\bar{x}_j > 2\bar{x}_i \bar{x}_j$. The above implies that the second hypothesis is satisfied. That is $l_{ij} > 2$. Therefore $\bar{x}$ is globally asymptotically stable on interior set of D_1.

International Journal for Scientific Research, London
https://doi.org/10.59992/IJSR.2026.v5n8p6
Vol (5), No (8), 2026
E-ISSN 2755-3418

7. Mathematical Model of Pantograph

The physical model presented in fig.7.1 is described with the following equations of motion:

$$M_s\ddot{y}_3 + c_s(\dot{y}_3 - \dot{y}_2) + k_s(y_3 - y_2) + k_L y_3 + c_L\dot{y}_3 = 0$$

$$M_u\ddot{y}_2 + c_s(\dot{y}_2 - \dot{y}_3) + k_s(y_2 - y3) + k_p(y_2 - y_1) = 0 \qquad (29)$$

$$EI\frac{\partial^4 y}{\partial x^4} - T\frac{\partial^2 y}{\partial x^2} + \beta\frac{\partial^2 y}{\partial x^2} + m\frac{\partial^2 y}{\partial x^2} = f(t)w(x,t)$$

The system of equations (29) can be substituted by the equivalent system as below:

$$M_s\ddot{y}_3 + c_s(\dot{y}_3 - \dot{y}_2) + k_s(y_3 - y_2) + k_L y_3 + c_L\dot{y}_3 = 0$$

$$M_u\ddot{y}_2 + M_s\ddot{y}_3 + k_L + k_L\dot{y}_3 + k_p(y_2 - y_1) = 0 \qquad (30)$$

$$EI\frac{\partial^4 y}{\partial x^4} - T\frac{\partial^2 y}{\partial x^2} + \beta\frac{\partial^2 y}{\partial x^2} + m\frac{\partial^2 y}{\partial x^2} = f(t)w(x,t)$$

Where y_1, y_2, y_3 are respectively, the deflections of the wire compressed by the oscillating system, the deflections of the centroid of the masses M_u and M_s from the equilibrium position, y(x, t) is the deflection of the wire, EI is the bending stiffness of the wire, T is horizontal tension in the wire, β is viscous damping of the wire, m is the mass per unit length of the wire, c_s and c_L are damping coefficients, k_s, k_L and k_p are stiffness elements of the system, $y_0 = y(x, 0)$ is the micro-irregularity in x, d is the length of the contact zone between pantograph and contact wire, L is the length of the span for the wire, g is gravity acceleration, t is the time and, $f(t) = (M_s + M_u)g - (F + M_u\ddot{y}_2 + M_s\ddot{y}_3 + k_L y_3 + cL\dot{y}_3)$

$$w(x,t) = \begin{cases} \frac{1}{d} & \text{for } vt - \frac{d}{2} \le x \le vt + \frac{d}{2} \\ 0 & \text{in the rest.} \end{cases}$$

$$y_1(t) = \int_0^L [y_0(x) + y(x,t)]w(x,t)dx = \frac{1}{d}\int_{vt+\frac{d}{2}}^{vt+\frac{d}{2}} [y_0(x) + y(x,t)]dx$$

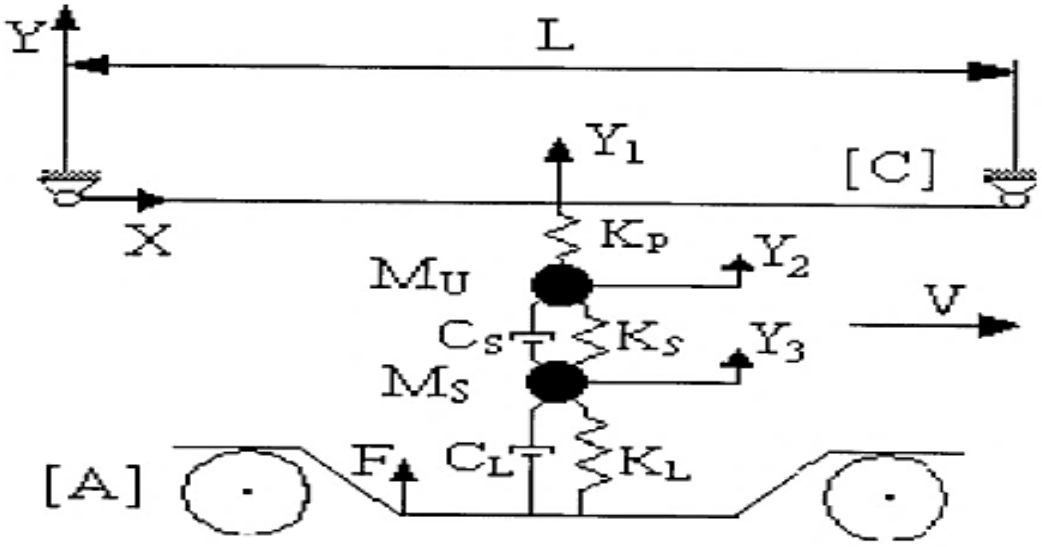

Fig. (7.1): Physical model

We introduce dimensionless variables and parameters (where the fundamental natural frequency of the wire span is ω_1, the maximum displacement of a simply supported wire when a unit load is applied in its midpoint is y_{st}), as follows:

$$\xi = \frac{\pi x}{L},\ \tau = \frac{\pi v t}{L},\ \tilde{v} = \sqrt{\frac{m}{T}}v = \tilde{v}_T,\ \tilde{M} = \frac{M_s + M_u}{mL},\ \tilde{g} = \frac{48}{\pi^4 \tilde{M}\tilde{v}^2}$$

$$y_{st} = \frac{gL^3}{48EI},\ \tilde{y} = \frac{y}{y_{st}},\ \mu = \frac{M_u}{M_s + M_u},\ \tilde{\omega}_{ns} = \frac{L}{\pi v}\sqrt{\frac{k_s}{M_s + M_u}}, \qquad (31)$$

$$\tilde{\omega}_{nL} = \frac{L}{\pi v}\sqrt{\frac{k_L}{M_s + M_u}},\ \ \tilde{\Omega}_n = \frac{L}{\pi v}\sqrt{\frac{k_p}{M_s + M_u}},\ \tilde{v}_\beta = \frac{m\pi}{\beta L}v,$$

$$\zeta_s = \frac{c_s}{2\sqrt{k_s(M_s + M_u)}},\ \zeta_L = \frac{c_L}{2\sqrt{k_L(M_s + M_u)}},$$

$$\Delta = \frac{\pi d}{L},\ \ \tilde{v}_{EI}\frac{L}{\pi}\sqrt{\frac{m}{EI}}v$$

Equations (30) have now the following form, using (31):

International Journal for Scientific Research, London
https://doi.org/10.59992/IJSR.2026.v5n8p6
Vol (5), No (8), 2026
E-ISSN 2755-3418

$$(1-\mu)\ddot{\tilde{y}}_3 + 2\square_s\,\tilde{\omega}_{sn}^2(\dot{\tilde{y}}_3 - \dot{\tilde{y}}_2) + (\dot{\tilde{y}}_3 - \dot{\tilde{y}}_2) + \tilde{\omega}_{nL}^2\,\tilde{y}_3 + 2\square_L\tilde{\omega}_{nL}\,\dot{\tilde{y}}_3 = 0$$

$$\mu\ddot{\tilde{y}}_2 + (1-\mu)\,\ddot{\tilde{y}}_3 + \tilde{\Omega}_n^2(\tilde{y}_2 - \tilde{y}_1 + \tilde{\Omega}_{nL}^2\,\tilde{y}_3 + 2\square_L\tilde{\omega}_{nL}\,\dot{\tilde{y}}_3 = 0$$

$$\frac{1\cdot}{\tilde{v}_{EI}^2}\frac{\partial^4\tilde{y}}{\partial\zeta^4} - \frac{1\cdot}{\tilde{v}_T^2}\frac{\partial^2\tilde{y}}{\partial\zeta^2} + \frac{1\cdot}{\tilde{v}_\beta^2}\frac{\partial^4\tilde{y}}{\partial\tau} + \frac{\partial^2\tilde{y}}{\partial\tau^2} = \tilde{f}(\tau)\tilde{\omega}(\zeta,\tau) \qquad (32)$$

The following notations are used in equation (32):

$$\tilde{f}(\tau) + \tilde{M}\pi\left(\tilde{g} - \mu\ddot{\tilde{y}}_2 - (1-\mu)\ddot{\tilde{y}}_3 - \tilde{\omega}_{nL}^2\tilde{y}_3 - 2\zeta_L\tilde{\omega}_{nL}\dot{\tilde{y}}_3\right)$$

$$\tilde{w}(\zeta,t) = \begin{cases} \dfrac{1\cdot}{\Delta} & \text{for } \tau - \dfrac{\Delta}{2} \le \zeta \le \tau + \dfrac{\Delta}{2} \\ 0 & \text{in the rest} \end{cases} \qquad (33)$$

$\tilde{y}_1 = \dfrac{1}{\Delta}\int_{\tau-\frac{\Delta}{2}}^{\tau+\frac{\Delta}{2}}[\tilde{y}(\zeta,\tau) + \tilde{y}_0(\zeta)]\,d\zeta$. We study the third equation of (32), where is neglected the constant force of the right hand for analysis the motion stability of the system, as follows:

$$\frac{1\cdot}{\tilde{v}_{EI}^2}\frac{\partial^4\tilde{y}}{\partial\zeta^4} - \frac{1\cdot}{\tilde{v}_T^2}\frac{\partial^2\tilde{y}}{\partial\zeta^2} + \frac{1\cdot}{\tilde{v}_\beta^2}\frac{\partial^4\tilde{y}}{\partial\tau} + \frac{\partial^2\tilde{y}}{\partial\tau^2}$$

$$= -M\pi\left(\mu\ddot{\tilde{y}}_2 + (1-\mu)\ddot{\tilde{y}}_3 + \tilde{\omega}_{nL}^2\tilde{y}_3 - 2\zeta_L\tilde{\omega}_{nL}\dot{\tilde{y}}_3\right)\tilde{w}(\zeta,\tau) \qquad (34)$$

The solution of the equation (34) is expanded after its natural modes

$\sin j\,\zeta$, $j = 1, 2, \ldots$ (corresponding to a simply supported wire) and after the same system of functions is developed the function $\tilde{w}(\zeta,\tau)$. Thus, we have the following expression of them:

$$\tilde{y}(\zeta,\tau) = \sum_{j=1}^{\infty} T_j \sin j\zeta$$

$$\tilde{w}(\zeta,\tau) = \frac{2\cdot}{\pi}\sum_{j=1}^{\infty}\frac{\sin j\Delta}{j\Delta}\sin j\zeta\, j\tau \qquad (35)$$

The functions $T_j(\tau)$ are defined by the following differential equations:

$$\frac{d^2T_j}{d\tau^2}+\frac{1}{\tilde{v}_\beta}\cdot\frac{dT_j}{d\tau}+\left(\frac{j^4}{\tilde{v}_{EI}^2}+\frac{j^2}{\tilde{v}_T^2}\right)$$

$$=-\tilde{M}\pi\left(\mu\ddot{\tilde{y}}_2+(1-\mu)\ddot{\tilde{y}}_3+\tilde{\omega}_{nL}^2\tilde{y}_3-2\zeta_L\tilde{\omega}_{nL}\dot{\tilde{y}}_3\right)\frac{2}{\pi}\cdot\frac{\sin j\Delta}{j\Delta}\sin j\tau \qquad (36)$$

The displacement $\tilde{y}_1(\tau)$ has the expression:

$$\tilde{y}_1=\sum_{j=1}^{\infty}T_j\sin j\tau \qquad (37)$$

In equation (37) we consider an approximation with five terms. Finally, the dimensionless system of equations that specifies the state problem for the dynamic system, described by fig.7.1, is:

$$(1-\mu)\ddot{\tilde{y}}_3+2\square_s\,\tilde{\omega}_{sn}^2(\dot{\tilde{y}}_3-\dot{\tilde{y}}_2)+(\dot{\tilde{y}}_3-\dot{\tilde{y}}_2)+\tilde{\omega}_{nL}^2\,\tilde{y}_3+2\square_L\tilde{\omega}_{nL}\,\dot{\tilde{y}}_3=0$$

$$\mu\ddot{\tilde{y}}_2+(1-\mu)\ddot{\tilde{y}}_2+\tilde{\Omega}_n^2\left(\tilde{y}_2-\sum_{j=1}^{\infty}\left[T_j(\tau)+w_j\right]\frac{\sin j\Delta}{j\Delta}\sin j\tau\right) \qquad (38)$$

$$+\tilde{\omega}_{nL}^2\tilde{y}_3-2\zeta_L\tilde{\omega}_{nL}\dot{\tilde{y}}_3=0,\frac{d^2T_j}{d\tau^2}+\frac{1}{\tilde{v}_\beta}\cdot\frac{dT_j}{d\tau}+\left(\frac{j^4}{\tilde{v}_{EI}^2}+\frac{j^2}{\tilde{v}_T^2}\right)T_j$$

$$=-2\tilde{M}\left(\mu\ddot{\tilde{y}}_2+(1-\mu)\ddot{\tilde{y}}_3+\tilde{\omega}_{nL}^2\tilde{y}_3-2\zeta_L\tilde{\omega}_{nL}\dot{\tilde{y}}_3\right)\sin j\tau.\quad j=1,2,....$$

In equation system (38) we use the notations:

$$\tilde{v}_{EI}^2=\frac{mL^2}{EI\pi^2}v^2,\qquad \tilde{v}_T^2=\frac{m}{T}v^2,\quad \tilde{v}_\beta=\frac{m\pi}{\beta L}v.$$

The initial conditions for the system of equations (38), considered known, that assure the uniqueness of the solution, are:

$$\tilde{y}_3(0)=\tilde{y}_{03},\quad \dot{\tilde{y}}_3(0)=\tilde{y}_{\dot{0}3},\quad \tilde{y}_2(0)=\tilde{y}_{02},$$
$$\dot{\tilde{y}}_2(0)=\tilde{y}_{\dot{0}2},\quad T_i(0)=T_{0i},\quad \dot{T}_i(0)=\dot{T}_{0i},\quad i=1,2,...$$

8. Numerical Tests

The above theoretical exposure is analyzed in this paragraph for concrete physical model described by fig.8.1. The values of the contact wire parameters, used here for all the tests, are defined by the span length L = 60[m], by the mass of the wire per unit length m = 0.63[kg/m] and by viscous damping β = 0.1[Ns/m]. The values of the pantograph dynamical system parameters, used here for all the tests, are defined by the concentrated masses M_u = 2.2[kg], Ms = 19.8[kg], the value of the rapport

$\mu = M_u/(M_s + M_u) = 0.1$ and ³s = 0.3, $\zeta_L = 0.3$. The physical model of pantograph chosen here is obtained by decomposition of pantograph mass in two concentrated masses with hypothetical values of the parameters and with a hypothetical design. The stiffness k_p = 2250M/m is also used in the mathematical model calculation.

Identification of the stability and instability zones (8.1) [6] we consider also the following fixed dimensionless values of the parameters:

$$\tilde{\Omega}_n + 3.185, \quad \tilde{v}_\beta = 19.8, \qquad \tilde{\omega}_{nL} = 0.48, \quad \tilde{v}_{EI} = 90.96. \qquad (39)$$

The corresponding real values of the parameters are:

$$v = \frac{L}{\pi\tilde{\Omega}_n}\sqrt{\frac{k_p}{M_s + M_u}} = 60.64[m/s], \quad \beta = \frac{m\pi}{\tilde{v}_\beta L}v = 0.1[Ns/m],$$

$$\sqrt{k_L} = \frac{\pi v\tilde{\omega}_{nL}}{L}\sqrt{M_s + M_u} = 7.148[N/m],$$

$$\sqrt{EI} = \frac{L}{\pi v\tilde{\omega}_{nL}}\sqrt{m} = 10.1[Nm^2], \; EI = 102[Nm^2].$$

The free parameters in the plane of parameters are in these case dimensionless variables $\tilde{\omega}_{ns}$ and $\tilde{v}$ T for which correspond, respectively, stiffness element k_s of the system and horizontal tension in the wire T, real parameters of the dynamical system. We analyze the stability of motion for the dimensionless displacement $\tilde{y}_2$ of the concentrated mass M_u in the free vibration of the system. In fig.8.1 is plotted with continuous line the domain of periodic solutions of $\tilde{y}_2$ in the two chosen parameters plane defined by the variables $\tilde{\omega}_{ns}$ and $\tilde{v}$ T, in the case of free vibrations of the system.

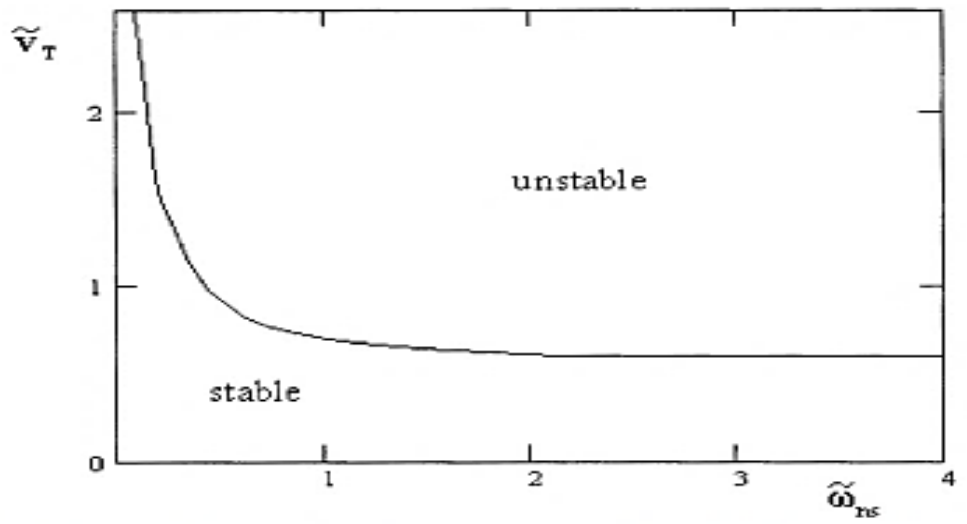

Fig. (8.1): Stable and unstable zones in the plane of parameters

On the figure are specified the stable and unstable zones of the displacement $\tilde{y}_2$. The algorithm, has been applied for perform the stability regions from fig.8.2.

Influence of pantograph speed on the system stability (8.2) [6] We study influence of the pantograph speed on the stability of the dynamical system described by equations (3.3.10), where j = 1, 2, …, 5. Evolution of the displacement $\tilde{y}_2$, of the concentrated mass Mu, is used for analyze the motion stability of the physical model from fig.8.1.

The last real values of the parameters, that define the mathematical model of dynamical system tested here, are k_s = 40N/m, T = 1500N and v = 25m/s, 30m/s, 35m/s. In fig .8.2 are plotted evolutions of the displacement $\tilde{y}_2$ versus dimensionless variable τ that correspond to real variable of time. For fixed values of the parameters of the dynamical system, with exception of the speed v, we have identified existence of the critical value of the speed v of the dynamical system, looking the curves drown in fig.8.2. By choosing of other free parameter of the system, as tension T in the wire, we can identify other critical values of the dynamical system described by physical model from fig.8.1.

The values of the free parameter, chosen in the neighborhood of the critical value, permit us to find influence of the all-other parameters of the dynamical system pantograph – contact wire on its evolution.

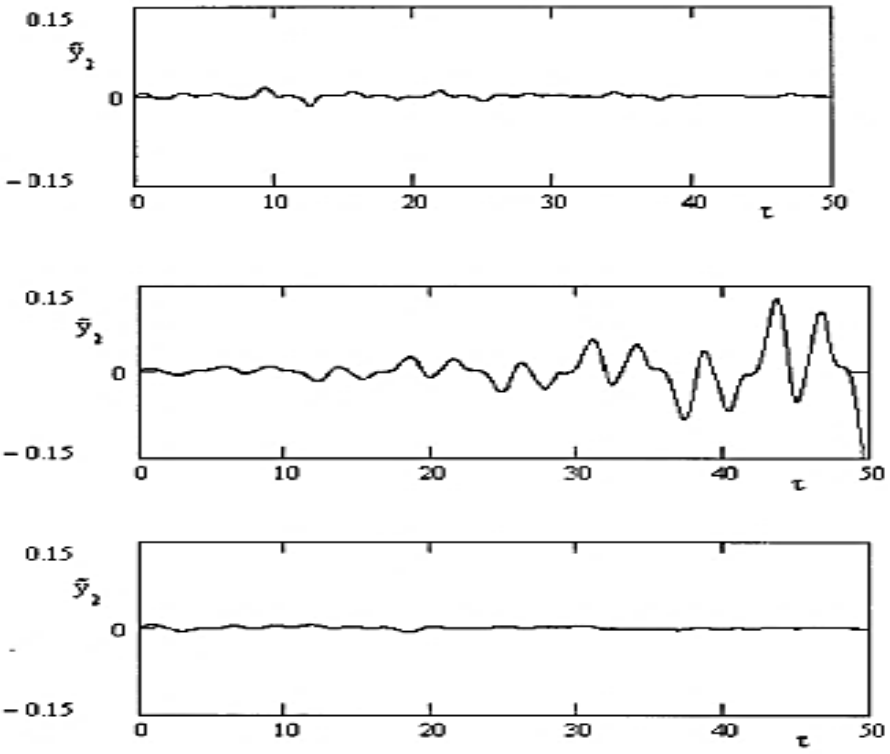

Fig. (8.2): Influence of speed v = 25m/s, 30m/s, 35m/s, on mass Mu evolution

The results underline possibility to study evolution of our concrete dynamical system by the mathematical model attached to physical model.

9. Result

For a system having an integer state matrix $F \in \mathbb{Z}^{n\times n}$, the encrypted controller (4)–(5) can be implemented over encrypted data without scale drift, ensuring that decrypted states and outputs retain fixed precision $1/(Ls_1)$ and $1/(Ls_1s_2)$ for all time, provided quantization errors remain bounded.

10. Summary

The paper integrates homomorphic encryption with dynamic control systems, proposing methods to avoid precision decay by restricting to integer state matrices. It derives two stability criteria (determinant-based and Gershgorin-based) and applies them to a pantograph-catenary model. Numerical experiments reveal stability regions and critical speeds, validating the theoretical frameworks for secure and stable control under encryption.

References

1. J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," arXiv preprint arXiv:1912.07362, 2019.
2. P. Parlier, "Public-key cryptosystems based on composite degree residuality classes," in Advances in Cryptology – EUROCRYPT 1999, Prague, Czech Republic, Springer, 1999, pp. 223–238.
3. O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in Proc. 37th Annual ACM Symp. Theory of Computing (STOC), Baltimore, MD, USA, 2005, pp. 84–93.
4. Z. Brake ski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in Proc. IEEE 52nd Annu. Symp. Found. Compute. Sci. (FOCS), Palm Springs, CA, USA, 2011, pp. 97–106.
5. C. Gentry, A Fully Homomorphic Encryption Scheme, Ph.D. thesis, Stanford University, 2009.
6. J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in Advances in Cryptology – ASIACRYPT 2017, Hong Kong, China, Springer Cham, 2017, pp. 409–437.
7. K. Kagiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in Proc. 54th IEEE Conf. Decision and Control (CDC), Osaka, Japan, 2015, pp. 7256–7263.
8. C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semi homomorphic encryption," IEEE Trans. Autom. Control, vol. 65, no. 9, pp. 3950–3957, 2020.
9. N. Schlüter, P. Binfet, and M. Schulze Darup, "A brief survey on encrypted control: From the first to the second generation and beyond," Annu. Rev. Control, vol. 56, p. 100913, 2023.
10. M. Schulze Darup, "Encrypted model predictive control in the cloud," in Privacy in Dynamical Systems, Singapore, Springer, 2019, pp. 231–265.
11. J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, "Need for controllers having integer coefficients in homomorphically encrypted dynamic system," in Proc. 57th IEEE Conf. Decision and Control (CDC), Miami, FL, USA, 2018, pp. 5020–5025.
12. J. Kim, H. Shim, H. Sandberg, and K. H. Johansson, "Method for running dynamic systems over encrypted data for infinite time horizon without bootstrapping and re-encryption," in Proc. 60th IEEE Conf. Decision and Control (CDC), Austin, TX, USA, 2021, pp. 6528–6534.

13. J. Lee, D. Lee, and J. Kim, "Stabilization by controllers having integer coefficients," 2025. Preprint: https://arxiv.org/abs/2505.00481.
14. J. Lee, D. Lee, S. Lee, J. Kim, and H. Shim, "Conversion of controllers to have integer state matrix for encrypted control: Non-minimal order approach," in Proc. 62nd IEEE Conf. Decision and Control (CDC), Singapore, 2023, pp. 5091–5096.
15. N. Schlüter, M. Neuhaus, and M. Schulze Darup, "Encrypted dynamic control with unlimited operating time via FIR filters," in Proc. 2021 European Control Conf. (ECC), Rotterdam, Netherlands, 2021, pp. 952–957.
16. J. Adamek, N. Schlüter, and M. Schulze Darup, "On the design of stabilizing FIR controllers," in Proc. 10th Int. Conf. Control, Decision and Information Technologies (CoDIT), Valletta, Malta, 2024, pp. 2037–2042.
17. S. Schor and F. Allgaier, "Bootstrapping guarantees: Stability and performance analysis for dynamic encrypted control," IEEE Control Syst. Lett., vol. 8, pp. 2235–2240, 2024.
18. A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Towards private data-driven control," in Proc. 59th IEEE Conf. Decision and Control (CDC), Jeju, South Korea, 2020, pp. 5449–5456.
19. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.
20. N. Schlüter, M. Neuhaus, and M. Schulze Darup, "Encrypted extremum seeking for privacy-preserving PID tuning as-a-service," in Proc. 2022 European Control Conf. (ECC), London, UK, 2022.
21. J. Kim et al., "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," IFAC-Papers Online, vol. 49, no. 22, pp. 175–180, 2016.
22. S. Lang, M. Seidel, and F. Allgaier, "Robust performance for switched systems with constrained switching and its application to weakly hard real-time control systems," in Cyber-physical Networking, Springer, 2024. Preprint: https://arxiv.org/abs/2411.08436v1.
23. C. Scherer and S. Weiland, Linear Matrix Inequalities in Control, vol. 3, Delft, The Netherlands, Lecture Notes, Dutch Institute for Systems and Control, 2000.
24. M. Green and D. J. N. Lime beer, Linear Robust Control, Englewood Cliffs, NJ, Prentice-Hall, 1995.
25. J. Lomberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in Proc. CACSD Conf., Taipei, Taiwan, 2004.
26. MOSEK Apes, MOSEK Optimization Toolbox for MATLAB 10.2.17, 2024.

27. A. Al Badawi and Y. Polyakov, "Demystifying bootstrapping in fully homomorphic encryption," Cryptal. Print Arch., Paper 2023/149, 2023.

28. C. Marcella, V. Sacasas, M. Manzano, R. Assoil, F. H. P. Fitzek, and N. Aara, "Survey on fully homomorphic encryption, theory, and applications," Proc. IEEE, vol. 110, no. 10, pp. 1572–1609, 2022.