ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المجلد التاسع – العدد الرابع والتسعون
تاريخ الإصدار: 2 – آب – 2026م

www.ajsp.net

"Encrypted Control of Linear Systems with Integer Matrices"

Researchers:

Adel Ahmed Hassan Kubba (1)

Amna Hamid Mohammed Hamid (2)

(1) Associate Professor - Nile Valley University - Faculty of Education

(2) Mathematics Teacher at the Ministry of Education, Sultanate of Oman

Received: 15/07/2026 | Revised: 16/07/2026 | Accepted: 23/08/2026 | Published: 02/08/2026

Abstract:

This paper addresses the topic of encrypted control in networked control systems, utilizing homomorphic encryption to protect control data from cyber-attacks. The research aims to perform control operations directly on encrypted signals and parameters without decryption, providing comprehensive data protection throughout the processing cycle. The paper proposes a methodology for converting linear time-invariant systems into linear time-varying systems with integer state matrices, enabling implementation on encrypted data over an infinite time horizon. The research also presents stability and performance tests using robust control theory, with lifting techniques applied to reduce conservatism in analysis. A numerical example is provided to demonstrate the effectiveness of the proposed method, showing improved results compared to traditional approaches.

Keywords: Encrypted Control - Homomorphic Encryption - Networked Control Systems – Stability - Linear Systems - Integer State Matrices - Robust Control - Dynamic Lifting

How to Cite This Article

Kubba, A. A. H., & Hamid, A. H. M. (2026). Encrypted control of linear systems with integer matrices. ***Arab Journal for Scientific Publishing (AJSP)*****, 9(94), (474-487).**

AJSP | Vol. 9 | Issue 94 | DOI: https://doi.org/10.36571/ajsp.94 **AJSP ORCID: https://orcid.org/0009-0005-8048-2082**

1. Introduction

As a countermeasure for the threat of cyber-attacks on networked control system, the notion of encrypted control has been introduced, to conceal and protect control data from third parties of malicious adversaries. It aims for control operation directly performed over encrypted signals and parameters via homomorphic encryption, which allows arithmetic operation over encrypted messages without decryption. By doing so, all control data can be protected by encryption thoroughly, while they are encrypted at sensors, processed at computing devices, and eventually transmitted and decrypted at actuators. Security problems are being regarded as more and more urgent in most applications that involve network communication, so the use of homomorphic encryption have been introduced for more and more methods and algorithms, for example, for model predictive control, optimization problems, average consensus or distributed aggregation, quantized control, reset control, and learning based control. The significance of stability in control systems, whether linear or nonlinear, is widely recognized. Consequently, researchers in the field of control systems have developed appropriate methods for analyzing system stability. Stability analysis is particularly important for cyber-physical systems (CPS), which are vulnerable to numerous attacks. Stability is a critical factor in various industrial systems, including breakwaters, structural reliability analysis, and inverter-based nonlinear power systems, and recent advances in this area should also be considered.

Encrypted control offers the ability to outsource the computations to evaluate the control law to external servers while maintaining the privacy of the involved data at the same time. This not only enhances flexibility and reduces the need for dedicated hardware for the controller, but also can be valuable for control and monitoring of distributed systems. [6]

2. System Model and Homomorphic Properties

Homomorphic Encryption (2.1)[2] Consider a cryptosystem denoted by ($\mathbf{Z}_q$, C, Enc; Dec), where Zq is the space of plaintexts (unencrypted data) with modulus q∈ **N**, C is the space of ciphertexts (encrypted data), and
Enc ⟶ $\mathbf{Z}_q$ ⟶ C and Dec: C ⟶ $\mathbf{Z}_q$ are the encryption and decryption algorithms, respectively. We abuse notation and let Enc: $\mathbf{Z}^n_q$⟶ C^n and Dec: C^n ⟶ $\mathbf{Z}^n_q$, n ∈ **N**, be regarded component-wise algorithms for vectors.
Throughout the paper, the cryptosystem is assumed to be additively homomorphic; i.e., to satisfy the followings:
H_1: For all m ∈ $\mathbf{Z}^n_q$ with n ∈ **N**, Dec(Enc(m)) = m holds.
H_2: There exists an operation Addn: $C^n \times C^n \longrightarrow C^n$ for each n ∈ N, such that Dec ($Add_n(c_1, c_2)$)= $Dec(c_1) + Dec(c_2)$ mod q, for all $c_1 \in C^n$ and $c_2 \in C^n$.

H_3: There exists Int Mult $_{m,n}$: $Z_q^{m\times n} \times C^n \longrightarrow C^m$ for each m ∈ N and n ∈ N, such that Dec (Int Mult $_{m,n}$ (K, c))=K. Dec(c) mod q, for all K∈ $Z_q^{m\times n}$ and c∈C^n.

The property H_2 means that the cryptosystem can perform addition directly over encrypted messages, and H_3 means the ability of performing constant multiplication over ciphertexts, where the multiplier is unencrypted. We abuse notation and use $c_1 + c_2 := Add_n(c_1, c_2)$ for $c_1 \in C^n$ and $c_2 \in C^n$, and K.

c := Int Mult $_{m,n}$ (K, c) for K ∈ $Z_q^{m\times n}$ and c ∈ C^n. As typical examples of additively homomorphic encryption, Paillier cryptosystem or cryptosystems based on the Learning with Errors (LWE) problem, such as can be considered. Regarding the latter, the case of using LWE-based cryptosystems, the presence of "injected errors" should be considered in practice, as they satisfy H_1–H_3 with small. We omit the argument of error effect, for simplicity.

Problem Formulation (2.2) [2] Consider a linear time-invariant system, given as

$$x(t+1) = Fx(t) + Gy(t) + ex(t), \quad x(0) = x_0 + e_{x,}0,$$
$$u(t) = Hx(t) + Jy(t) + e_u(t), \qquad t = 0, 1, 2, \ldots, \qquad (1)$$

where x(t) ∈ $\mathbf{R}^n$ is the state, y(t)∈**R**p is the input, and u(t)∈$\mathbf{R}^m$ is the output of the system, respectively, and $x_0 \in \mathbf{R}^n$ is the initial state, and $e_x(t) \in \mathbf{R}^n$, $e_u(t) \in \mathbf{R}^m$, and $e_{x,0} \in \mathbf{R}^n$ denote perturbations. For the ideal case, i.e., the case that $e_x(t) \equiv 0$, $e_u(t) \equiv 0$, and $e_{x,0} = 0$, the input, state, and output are denoted as {y'(t), x'(t), u'(t)}, respectively. Assuming that the system (1) is a part of stable closed-loop system, we make two mild assumptions, as follows:
A_1: The input, state, and output of (1) for the ideal case are bounded; there exists M>0, which is known, such that, ||[y'(t); x'(t); u'(t)]||≤M, for all t∈ N_0. Especially for the output u'(t) =: col $\{u'_i(t)\}_{i=1}^m$, we let

$$u_i^{min} \le u'_i(t) \le u_i^{max}, \quad \forall t \in N_0, \ \forall i = 1,\ldots m, \qquad (2)$$

with some real numbers $\{u'^{min}_i(t)\}_{i=1}^m$ and $\{u'^{max}_i(t)\}_{i=1}^m$.

A_2: The trajectories {y'(t), x'(t), u'(t)} of(1) are stable with respect to the perturbations $\{e_{x,0}, e_x(t), e_u(t)\}$, for any □>0, there exists a constant □x>0 such that if $sup_t(|||[e,(t), e_u(t), e_{x,0}||) \le$ □x, then ||y(t)− y'(t)|| ≤ □, ||x(t)−x'(t)||≤ □, and ||u(t)−u'(t))|| ≤ □, ∀t ∈ $\mathbf{N}_0$.
Given the system (1) with the real matrices {F, G, H, J} and $x_0 \in \mathbf{R}^n$, the objective is to implement (1) with a digital computer, to operate over encrypted data. Regarding quantization for digital implementation, let the input y(t)∈$\mathbf{R}^p$ of(1) be quantized and encoded as

$$\bar{y}(t) := \left[\frac{y(t)}{r}\right] \bmod q, \qquad (3)$$

where r > 0 is the step size for the quantization, and q ∈ **N** is the size of plaintext space, so that it consists of elements of the set $\mathbf{Z}_q$, i.e., y(t) ∈ $\mathbf{Z}^p_q$. Then, it can be encrypted as

$$y(t) := Enc(y(t)) \in C^p. \qquad (4)$$

Then, the problem is to construct a dynamic system defined over the space C which satisfies the followings:
- It receives the signal y(t) ∈ C^p as input, and computes its next state and its output u(t)∈ C^m, using only the operations Add_n and $IntMult_{m,n}$ of H_2 and H_3.
- The performance of the constructed system is equivalent to that of (1), for any □ > 0, the parameters of the system can be chosen so that it guarantees ||g(Dec(u(t))) – u'(t)|| ≤□ for all t ∈ $\mathbf{N}_0$, with some function g : $Z^m_q \longrightarrow \mathbf{R}^m$ for the decrypted output.

The constructed system can perform the operation for an infinite time horizon, without decrypting, resetting, or re-encrypting any portion of encrypted data.

3. The Method

A quantitative descriptive method was adopted for the investigation. The quantitative technique is a research approach based on positivism or scientific philosophy with concrete and practical scientific principles.

Definition (3.1) [29] The system satisfies quadratic performance specified by P_p if it is asymptotically stable for $w_p = 0$ and there exists $\square > 0$ such that

$$\sum_{t=0}^{\infty}\begin{pmatrix} w_p(t) \\ w_p(t) \end{pmatrix}^T P_p \begin{pmatrix} w_p(t) \\ w_p(t) \end{pmatrix} \le -\varepsilon \sum_{t=0}^{\infty} w_p(t)^T w_p(t) \qquad (5)$$

for $\square(0) = 0$ and all $w_p \in \ell^2$.

This includes the ℓ_2-gain, among other common performance specifications.

Dynamic Control with Bootstrapping (3.2) [29] We first show how we can test performance using the system and bootstrapping description. Then, we use a lifting approach to reduce the conservatism of our analysis.

A. Stability and performance analysis As described, we consider the bootstrapping error as a time-varying, unknown, static uncertainty described by the sector condition (5). Clearly, the zero-element resembling no error, i.e., no bootstrapping, is also contained in the uncertainty description $\square$. Then, by applying robust control theory, we can obtain the following theorem.

Theorem (3.3) [29] The encrypted closed-loop with the bootstrapping uncertainty(5) satisfies robust quadratic performance with performance index

$P_p = \begin{pmatrix} Q_p & S_p \\ S_p^T & R_p \end{pmatrix}$ with $R_p \le 0$, if there exist $X > 0$ and $t > 0$ such that

$$(*)^T \begin{pmatrix} -X & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} I & 0 & 0 \\ A & B_p & B_u \end{pmatrix} \qquad (6)$$

$$+ (*)^T P_p \begin{pmatrix} 0 & I & 0 \\ C_p & D_{pp} & D_{pu} \end{pmatrix} \qquad (7)$$

$$+ (*)^T \tau P_p \begin{pmatrix} 0 & 0 & 0 \\ C_u & D_{up} & D_{uu} \end{pmatrix} < 0. \qquad (8)$$

Proof. The proof follows directly from our uncertainty description for bootstrapping (5), which suits the robust stability and performance test.

B. Lifted dynamics The stability and performance test in Theorem (3.3) is conservative for the actual encrypted system in the sense that it remains valid even if the bootstrapping error is introduced in every time step. In reality, however, we know that we need to perform bootstrapping only every $T_{BS} \in N$ time steps. This number results from the fact that the cryptosystem supports several multiplications, i.e., control updates until the modulus has to be raised again. Inspired by the success of lifting, we adapt the lifting idea to obtain a z of the lifted system. We lift the involved signals as

$$\tilde{z}_u = z_u(kT_{BS}), \quad \tilde{w}_u(k) = \tilde{w}_u(kT_{BS}), \quad \tilde{\xi}(k) = \xi(kT_{BS})$$

$$\tilde{z}(k) = \begin{pmatrix} z_p(kT_{BS}) \\ \vdots \\ z_p(kT_{BS} + (T_{BS} - 1)) \end{pmatrix}, \ \tilde{w}(k) = \begin{pmatrix} w_p(kT_{BS}) \\ \vdots \\ w_p(kT_{BS} + (T_{BS} - 1)) \end{pmatrix},$$

$$\begin{pmatrix} \tilde{\xi}(k+1) \\ \hline \tilde{z}_p(k) \\ \hline \tilde{z}_u(k) \end{pmatrix} = \left(\begin{array}{c|c|c} \tilde{\mathcal{A}} & \tilde{\mathcal{B}}_p & \tilde{\mathcal{B}}_u \\ \hline \tilde{\mathcal{C}}_p & \tilde{\mathcal{D}}_{pp} & \tilde{\mathcal{D}}_{pu} \\ \hline \mathcal{C}_u & \tilde{\mathcal{D}}_{up} & \mathcal{D}_{uu} \end{array}\right) \begin{pmatrix} \tilde{\xi}(k) \\ \hline \tilde{w}_p(k) \\ \hline \tilde{w}_u(k) \end{pmatrix} \tag{9}$$

with

$$\tilde{A} = A^{T_{BS}}, \quad \tilde{B}_u = A^{T_{BS}-1}B_u, \quad \tilde{B}_p = \begin{pmatrix} A^{T_{BS}-1}B_p \cdots B_p \end{pmatrix},$$

$$\tilde{C}_p = \begin{pmatrix} C_p \\ \vdots \\ C_p A^{T_{BS}-1} \end{pmatrix}, \tilde{D}_p \begin{pmatrix} 0 \\ C_p B_u \\ \vdots \\ C_p A^{T_{BS}-2} B_u \end{pmatrix}, \tilde{D}_{pp} = \begin{pmatrix} D_{pp} & 0 & \cdots & 0 \\ C_p B_p & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ C_p A^{T_{BS}-2} B_p & \cdots & C_p B_p & D_{pp} \end{pmatrix},$$

$$\tilde{D}_{up} = \begin{pmatrix} D_{up} & 0 & \cdots & 0 \end{pmatrix}.$$

With this equivalent system description, we can proceed with an improved stability and performance analysis.

Lemma (3.4) [29] The original system satisfies quadratic performance specified by

$$P_p = \begin{pmatrix} Q_p & S_p \\ S_p & R_p \end{pmatrix}, \tag{10}$$

if and only if the lifted system (9) satisfies quadratic performance specified by

$$\tilde{P}_p = \begin{pmatrix} I_{T_{BS}} \otimes Q_p & I_{T_{BS}} \otimes S_p \\ I_{T_{BS}} \otimes S_p^T & I_{T_{BS}} \otimes R_p \end{pmatrix}. \tag{11}$$

Proof: Similar results were derived (stability), (ℓ_2-performance), (the general case). The proof follows from

$$\sum_{t=0}^{\infty} \begin{pmatrix} w_p(t) \\ z_p(t) \end{pmatrix}^T P_p \begin{pmatrix} w_p(t) \\ z_p(t) \end{pmatrix} = \sum_{k=0}^{\infty} \begin{pmatrix} \tilde{w}_p(k) \\ \tilde{z}_p(k) \end{pmatrix}^T \tilde{P}_p \begin{pmatrix} \tilde{w}_p(k) \\ \tilde{z}_p(k) \end{pmatrix} \tag{12}$$

and

$$\sum_{t=0}^{\infty} w_p(t)^T w_p(t) = \tilde{w}_p(k)^T \tilde{w}_p(k). \tag{13}$$

This performance equivalence can be used for our second theorem.

Theorem (3.5) [29] The encrypted closed-loop system (4.3.9) with the bootstrapping uncertainty (5) satisfies robust quadratic performance with performance index $P_p = \begin{pmatrix} Q_p & S_p \\ S_p & R_p \end{pmatrix}$, with $R_p \geq 0$, if there exist $X > 0$ and $\square > 0$ such that

$$(*)^T \begin{pmatrix} -X & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} I & 0 & 0 \\ \tilde{A} & \tilde{B}_p & \tilde{B}_u \end{pmatrix} \tag{14}$$

$$+ (*)^T P_p \begin{pmatrix} 0 & I & 0 \\ \tilde{C}_p & \tilde{D}_{pp} & \tilde{D}_{pu} \end{pmatrix} \tag{15}$$

$$+(*)^{T}\tau P_u\begin{pmatrix}0 & 0 & 0\\ C_u & D_{up} & D_{uu}\end{pmatrix}<0. \qquad (16)$$

with

$$\tilde{P}_p=\begin{pmatrix}I_{T_{BS}}\otimes Q_p & I_{T_{BS}}\otimes S_p\\ I_{T_{BS}}\otimes S_p^T & I_{T_{BS}}\otimes R_p\end{pmatrix}. \qquad (17)$$

Proof. The proof follows from Theorem (3.3) and Lemma (3.4).

Theorem (3.6) [28] yields a less conservative test than Theorem (3.3) since its lifted system description (9) captures the fact that the bootstrapping errors only occur every TBS time steps.

4. Numerical example

For the numerical evaluation we use the system with

$$A=\begin{pmatrix}-0.5 & 0.1\\ 0 & -0.2\end{pmatrix},\quad B=\begin{pmatrix}0\\1\end{pmatrix},\quad B_1=\begin{pmatrix}1\\1\end{pmatrix},\quad E=\begin{pmatrix}1\\1\end{pmatrix},$$

$C = (1 \quad 0)$, $F_1 = 0$, $C_1 = I$, $D_1 = 0$,

$$A_c=\begin{pmatrix}0.13 & 0.1\\ -1.27 & 0.15\end{pmatrix},\quad B_c=\begin{pmatrix}0.63\\ -0.27\end{pmatrix},\quad B_2=I,$$

$C_c = (-1 \quad 0.35)$, $D_c = 0$, $F_2 = 0$.

Using the polynomial with $T_{BS} = 10$, an upper bound on the ℓ_2-gain is found with $Q_p=-\gamma_{\ell_2}^2 I$, $S_p=0$, and $R_p=I$. Theorem (3.3) yields $\gamma_{\ell_2}=5.13$, and the less conservative Theorem (3.5) returns $\gamma_{\ell_2} = 3.97$. A simulation over 10.000-time steps yields an empirical lower bound of $\gamma_{\ell_2} = 1.88$.

Analysis of Rest and FIR Controllers (4.1) [7] It is interesting to note that if the sector slope is chosen as $\gamma = 1$ in the uncertainty description (9), then also reset controllers can be analyzed using Theorem (3.3) This is because this sector includes minus identity as part of its error description, and this is precisely the error introduced by resetting the entire controller state to zero. To pursue the analysis in this case, we can use a nominal controller with its matrices A_c, B_c, C_c, and D_c, and treat the reset purely by the uncertainty channel. Similarly, after small modifications, also FIR controllers of length N can be analyzed by Theorem (3.3). Instead of resetting all states, the dropped measurement $y(t-N)$ is fed into the uncertainty channel as $z_u(t)$ at each time step. The uncertainty input yields $w_u(t) = -z_u(t)$, which can correspond to $\gamma = 1$ in the sector notation. The last necessary modification is the change of $B_u = \begin{pmatrix}0\\ A_C^N B_C\end{pmatrix}$. This cancels the effect that $y(t-N)$ would have had on the current controller state. Thus, if nominal dynamic controllers are used in a reset or FIR fashion, our theorems provide stability and performance tests.

5. Main Results

It has been observed, that linear systems having the state matrix as integers can be implemented to operate over ciphertexts, for an infinite time horizon. Motivated from this idea, the approach of this paper is to convert the given linear time-invariant system (1) to a linear time-varying system having the state matrices consisting of integers, which has practically the same input-output relation, and then implement the converted system to operate over ciphertexts.

Consider a linear time-varying system of the form

$$v(t+1) = F_v(t)v(t) + G_v(t)y(t) + e_v(t), \qquad (18)$$

$$u_v(t) = H_v(t)v(t) + J_v(t)y(t) + e_u(t), \qquad (19)$$

$v(0) = v_0 + e_{v,0}$

where $v(t) \in \mathbf{R}^{nv}$, $n_v \in \mathbf{N}$, is the state with the initial value $v_0 \in \mathbf{R}^{nv}$, $y(t) \in \mathbf{R}^p$ is the same input with (1), $u_v(t) \in \mathbf{R}^m$ is the output, $\{e_v(t), e_u(t), e_{v,0}\}$ are the perturbations, and $\{F_v(t),G_v(t),H_v(t), J_v(t)\}_{t=1}^{\infty}$ are time-varying matrices which consist of a finite set of matrices. We first propose a method for converting the given system (1) to the form (5), which has practically the same input-output relation with that of (1), subject to the constraint that the converted system (5) should have the state

matrix as integers, i.e., have $F_v(t) \in \mathbf{Z}^{nv\times nv}$ for all $t \in \mathbf{N}_0$. Then, we demonstrate the validity of the proposed approach; it will be seen in the converted system (5) with the condition $F_v(t) \in \mathbf{Z}^{nv\times nv}$ can be implemented to operate over encrypted data for the infinite time horizon.

A. Conversion to System having State Matrix as Integers We consider decomposition of the system (1) to stable part and anti-stable part, by a transformation to the real Jordan form; with an invertible matrix $W = [W^T_1 ; W^T_2]^T \in \mathbf{R}^{n\times n}$ such that $z_1(t) = W_1x(t) \in \mathbf{R}^{n1}$ and $z_2(t) = W_2x(t) \in \mathbf{R}^{n2}$ where $n_1+n_2 = n$, the system (4.1.1) is transformed as the form

$$z_1(t + 1) = F_1z_1(t) + G_1y(t) + e_{z1}(t), \quad (20)$$
$$z_2(t + 1) = F_2z_2(t) + G_2y(t) + e_{z2}(t), \quad (21)$$
$$u(t) = H_1z_1(t) + H_2z_2(t) + J_y(t) + e_u(t), \quad (22)$$

$z_1(0) = W_1x_0 + e_{z1,0}$, $z_2(0) = W_2x_0 + e_{z2;0}$, where we let the matrix $F_1 \in \mathbf{R}^{n1\times n1}$ be anti-stable, i.e., every eigenvalue $\lambda_1 \in \mathbf{C}$ of F_1 is such that $|\lambda_1| \geq 1$, and let the matrix $F_2 \in \mathbf{R}^{n2\times n2}$ be strictly stable, i.e., every eigenvalue $\lambda_2 \in \mathbf{C}$ of F_2 is such that $|\lambda_2| < 1$, and $\{ez_1(t), ez_2(t), ez_{1,0}, ez_{2,0}\}$ are the perturbations with respect to the states $z_1(t)$ and $z_2(t)$. We present a scheme for converting the system (6) to the form (5) having the state matrices consisting of integers, in which the conversion for the part (20) is based on a novel approximation method for the eigenvalues of the matrix F_1, and the part (21) is proposed to be approximated to have finite impulse response. We make use the following lemma to convert the part (21), which implies that an anti-stable matrix can be slightly perturbed by a small error, so that one of its powers can be transformed to a matrix consisting of integers.

Lemma (5.1) [7] For any $\varepsilon > 0$ and an anti-stable matrix $F_1 \in \mathbf{R}^{n1\times n1}$, there exist $\in \mathbf{R}^{n1\times n1}$, $T \in \mathbf{R}^{n1\times n1}$, and $k_1 \in \mathbf{N}$ such that $\|F_1 - Fp\| \leq \varepsilon$ and $TF_p^{k_1}T^{-1} \in Z^{n_1\times n_2}$.

Proof. For a complex number $\lambda = \alpha + i\beta \in \mathbf{C}$ with $\alpha, \beta \in \mathbf{R}$, $\alpha, \beta \in \mathbf{R}$ and $i^2 = -1$, define $[\lambda] := [\alpha] + i[\beta]$. We claim that, for any $\lambda \in \mathbf{C}$ such that $|\lambda| \leq 1$, there exists a sequence $\{\lambda'_k\}_{k=1}^{\infty} \subset C$, such that $\lim_{k\to\infty} \lambda'_k = \lambda$ and $(\lambda'_k)^k = [\lambda_k]$. For each $k \in \mathbf{N}$, since $[\lambda_k] \neq 0$, we can let $\theta_k := \angle[\lambda^k] - [\lambda^k]$. Define $\lambda'_k = \sqrt[k]{|[\lambda^k]|} \cdot e^{i(\angle\lambda + \beta_k/k)}$.

It follows that $(\lambda'_k)^k = \sqrt{|[\lambda^k]|} \cdot e^{i(\angle\lambda^k + \beta_k/k)} = [\lambda^k]$, and

$$\lim_{k\to\infty} \lambda'_k = \lim_{k\to\infty} |\lambda| \cdot \sqrt[k]{1 + \frac{|[\lambda^k]| - |\lambda^k|}{|\lambda^k|}} \cdot e^{i\angle\lambda} = \lambda, \text{ Since } \big|\,|[\lambda^k]| - |\lambda^k|\,\big| \in \sqrt{2}/2.$$ Thus, the claim holds.

Now, let $\{\lambda_j\}_{j=1}^{n_1} \subset C$ be the eigenvalues of F_1. Given $\varepsilon > 0$, according to the claim, there exist $\{\lambda'_j\}_{j=1}^{n_1} \subset C$ and $k_1 \in \mathbf{N}$ such that

$|\lambda_j - \lambda'_j| \leq \alpha / \left(2\|T_1\|\|T_1^{-1}\|\right)$ and $(\lambda'_j)^{k_1} = [\lambda_j^{k_1}]$ hold, $\forall j = 1, \ldots, n_1$, where

$T_1 \in \mathbf{R}^{n1\times n1}$ is the transformation matrix such that the matrix

$J_1 := T_1F^1T_1^{-1} \in \mathbf{R}^{n1\times n1}$ is of the real Jordan form of F_1. Let $J_p \in \mathbf{R}^{n1\times n1}$ be the same matrix with J_1, where the real parts and the imaginary parts of the eigenvalues $\{\lambda'_k\}_{j=1}^{n_1}$ are replaced by those of. Define $F_p := T_1^{-1} J_pT_1$, which ensures $\|F_1 - F_p\| \leq \varepsilon$. Then, every eigenvalue $(\lambda'_j)^{k_1} = [\lambda_j^{k_1}]$ of $F_p^{k_1}$ has the real and imaginary parts as integers, so a transformation $T \in \mathbf{R}^{n1\times n1}$ for $F_p^{k_1}$ to the real Jordan form yields $TF_p^{k_1}T_1^{-1} \in \mathbf{Z}^{n1\times n1}$. This completes the proof.

Remark (5.2) [6] Note that the property $T F_p^{k_1} T_1^{-1} \in \mathbf{Z}^{n1\times n1}$ in Lemma (5.1) implies that the characteristic polynomial of $F_p^{k_1}$ is a monic polynomial having the coefficients as integers, which means, the eigenvalues of F_p are of algebraic integers. Indeed, an eigenvalue $\square \in \mathbf{C}$ of F_p is a root of $\det(s^{k_1} I_{n_1} - F_p^k) = 0$. In this context, the meaning of Lemma (5.1) can be understood that the eigenvalues of the given matrix F_1can be approximated to algebraic integers so that one of its powers can be transformed to a matrix of integers. With the perturbed state matrix F_p and transformation T obtained from Lemma 1, the anti-stable part (20) of system is proposed to be converted as follows; we re-write (20) as

$z_1(t+1) = F_p z_1(t) + G_1 y(t) + (F_1 z_1(t) - F_p z_1(t) + e_{z1}(t)),$
$=: F_p z_1(t) + G_1 y(t) + e'_{z1}(t),$ (22)

and define a time-varying coordinate transformation as

$$v_1(t) := T F_p^{-(t \bmod k_1)} z_1(t), \quad (23)$$

which varies with time, with period k_1. Then, by multiplying both sides of (22) by $TF_p^{-(t+1 \bmod k_1)}$, it is transformed as

$$v_1(t+1) = TF_p^{((t \bmod k_1)+1-(t+1 \bmod k_1))} T^{-1} v_1(t) + TF_p^{-(t+1 \bmod k_1)} (G_1 y(t) + e'z_1(t)) \quad (24)$$

$=: Fv_1(t) v_1(t) + Gv_1(t) y(t) + e_{v1}(t),$
with the initial state given by, $v_1(0) = T(W_1 x_0 + e_{z1,0}) =: v_{1,0} + e_{v1,0}$.
Here, it can be clearly seen that the converted system (24) has the state matrix consisting of integers for all $t \in \mathbf{N}_0$, since

$$Fv_1(t) = TF_p^{((t \bmod k_1)+1-(t+1 \bmod k_1))} T^{-1} = \begin{cases} TF_p^{k_1} T^{-1}, & \text{if } t \bmod k_1 = k_1 + 1, \\ I_{n_1}, & \text{otherwise}, \end{cases}$$

thanks to Lemma (5.1).
Next, for the stable part (21) of the system, we use finite impulse response approximation, to convert the state matrix to integers; since the state $z_2(t)$ of (21) can be computed as

$$z_2(t) = F_2^t W_2 x_0 + \sum_{\tau=0}^{t-1} F_2^{t-1-\tau} G_2 y(\tau), \quad (25)$$

an approximate value of $z_2(t)$ can also be computed as

$$z_2(t) \leftarrow \sum_{\tau=0}^{t-1} F_2^{t-1-\tau} G_2 y(\tau), \quad \text{for } t \geq k_2 + 1, \quad (26)$$

with $k_2 \in \mathbf{N}$ chosen sufficiently large, because the matrix F_2 is strictly stable. Thus, we convert the system (21) as

$$v_2(t+1) = \begin{bmatrix} 0_{k_2 n_2 \times n_2} & I_{k_2 n_2} \\ 0_{n_2 \times n_2} & 0_{n_2 \times k_2 n_2} \end{bmatrix} v_2(t) + \begin{bmatrix} G_2 \\ FG_2 \\ \vdots \\ F_2^{k_2} G_2 \end{bmatrix} y(t) + e_{v_2}(t)$$

$=: Fv_2 v_2(t) + Gv_2 y(t) + e_{v2}(t),$ (27)

$v_2(0) = [W_2 x_0; F_2 W_2 x_0; \ldots; F_2^{k_2} W_2 x_0] + e_{v2,0} =: v_{2,0} + e_{v2,0}$,

where $v_2(t) \in R^{(k2+1)n2}$ is the state, with the parameter $k_2 \in \mathbf{N}$ for the dimension of (27), and $\{e_{v2}(t), e_{v2,0}\}$ are the perturbations with respect to the state $v_2(t)$. Note that the update rule for the first n_2-components of $v_2(t)$ corresponds to (25) for $0 \leq t \leq k_2$, and (26) for $t \geq k_2+1$. And, clearly, the state matrix F_{v2} consists of integers, and it is nilpotent as $F_{v_2}^{k_2+1} = 0$, so the system

(27) is of finite impulse response As the result of the proposed conversion, the proposed form of converted system (20) is now determined; let the part (21) be identified with the combination of (24) and (27), by

$$v(t) := \begin{bmatrix} v_1(t) \\ v_2(t) \end{bmatrix}, \; v_0 := \begin{bmatrix} v_{1,0} \\ v_{2,0} \end{bmatrix}, \quad e_v(t) \begin{bmatrix} e_{v_1}(t) \\ e_{v_2}(t) \end{bmatrix}, \quad v_0 := \begin{bmatrix} e_{v_{1,0}} \\ e_{v_{2,0}} \end{bmatrix},$$

$$F_v(t) := \begin{bmatrix} F_{v_1}(t) & 0_{n_2 \times (k_2+1)n_2} \\ 0_{(k_2+1)n_2 \times n_2} & F_{v_2}(t) \end{bmatrix}, \quad G_v(t) := \begin{bmatrix} G_{v_1}(t) \\ G_{v_2} \end{bmatrix}.$$

To recover the state x(t) from the state v(t), we define

$$x_v(t) := W^{-1} \begin{bmatrix} F_p^{(t \bmod k_1)} T^{-1} & 0_{n_2 \times n_2} 0_{n_1 \times k_2 n_2} \\ 0_{n_2 \times n_1} & I_{n_2} 0_{n_1 \times k_n n_2} \end{bmatrix} v(t)$$

$$= W^{-1} \left[F_p^{(t \bmod k_1)} T^{-1} v_1(t); I_{n_2}, 0_{n_2 \times k_n n_2} \right] v_2(t). \qquad (28)$$

And, to obtain the output u(t) from v(t), by (22), we define

$Hv(t) := [F_p^{(t \bmod k_1)} T^{-1}, H_2, 0_{m \times k2n2}]$, $J_v(t) := J$. Finally, the following theorem states that given any linear time-invariant system (1), it can be converted to the form (1) having the state matrix as integers, and it can have practically the same performance with that of (1), by appropriate choice of the parameters k_1 for the period of time-varying matrices for the part (9), and k_2 for the dimension of the part (27).

Theorem (5.3) [8] Consider the converted system (5), designed as (9) and (27). For any $\varepsilon > 0$, there exist $k_1 \in \mathbf{N}$, $k_2 \in \mathbf{N}$, and $\varepsilon_v \le 0$ such that

$\sup_t(\|[e_v(t); e_u(t); e_v;0]\|) \le \varepsilon_v$ implies $\|x_v(t) - x'(t)\| \le \varepsilon$ and $\|u_v(t) - u'(t)\| \le \varepsilon$, $\forall t \in \mathbf{N}_0$.

Proof. We let $x_v(t)$ of (13) be identified with x(t) of (1);

let $e_x(t) := x_v(t+1) - Fx_v(t) - Gy(t)$, and $e_{x,0} := x_v(0) - x_0$, so that $x(t) = x_v(t)$, $\forall t \in \mathbf{N}_0$. Then,

$$e_{x,0} = W^{-1}\left[T^{-1}e_{v_1,0}; T_2' e_{v_2,0}\right], \; e_x(t) = W^{-1} \begin{bmatrix} F_p^{(t+1 \bmod k_1)} T^{-1} e_{v_1,0}; \\ I_2' e_{v_2}(t) + F_2' \left(F_{v_2}^t e_{v_2,0} + \sum_{\tau=t-k_2-1}^{t-1} F_{v_2}^{t-1-\tau} e_{v_2}(\tau) \right) \end{bmatrix}$$

$$+ W^{-1}\left[\left(F_p - F_1\right) W_1 x_v(t), -F_2^{k_2+1} G_2 y(t-k_2-1) \right] =: e_{x,1} + e_{x,2},$$

where $F'_2 := [-F_2, In_2 ; 0n_{2\times(k2-1)n2}]$, $I'_2 := [In_2 ; 0n_{2\times k2n2}]$, and $y(t - k_2 - 1) := 0$ for $t < k_2 + 1$. Let $\varepsilon > 0$ be given, and the constants $M > 0$ and ε_x be given from the conditions A_1 and A_2. Thanks to Lemma (5.1), we choose $k_1 \in \mathbf{N}$ such that $\|F_p - F_1\| \le \varepsilon_x / (2\|W^{-1}\| \|W_1\|M+\varepsilon))$. And, since $\lim_{k\to\infty} \|F^k{}_2 k = 0$, we choose

$k_2 \in \mathbf{N}$ such that $\left\|F_2^{k_2+1}\right\| \le \eta_x / \left(2\left\|W^{-1}\right\|\left\|G_2\right\|\left(M+\varepsilon\right)\right)$. Then, it is clear that

$\|[x_v(t); y(t - k_2 - 1)]\| \le M + \varepsilon$ implies $\|e_{x,2}(t)\| \le \varepsilon\varepsilon_x/2$. Next, since $\left\{F_p^{(t+1 \bmod k_1)}\right\}_{t=0}^{\infty}$ is a finite set, there exists a constant $C > 0$ such that $\|[e_{x,0}; e_{x,1}(t)]\| \le C \max\left\{\left\|e_{v,0}\right\|, \left\{\left\|e_v(\tau)\right\|\right\}_{\tau=t-k_2-1}^{t}\right\}$. Now, we choose $\varepsilon_v := \varepsilon/(2C)$, and suppose that $\sup_t \left(\left\|e_v(t); e_u(t); e_{v,0}\right\| \le \eta_v\right)$. Then, it directly implies $\|e_{x,0}\| \le \varepsilon\varepsilon_x/2$ and $\|e_{x,1}\| \le \varepsilon\varepsilon_x/2$, $\forall t \in \mathbf{N}_0$. Based on the assumptions A_1 and A_2, it can be shown that $\|e_{x,2}\| \le \varepsilon\varepsilon_x/2$, $\|x_v(t)\| \le M + \varepsilon$, and $\|y(t)\| \le M + \varepsilon$, $\forall t \in \mathbf{N}_0$, and hence $\|x_v(t) - x'(t)\| \le \varepsilon$ and $\|u_v(t) - u'(t)\| \le \varepsilon$, $\forall t \in \mathbf{N}_0$. This ends the proof.

The meaning of Theorem (5.3) can be understood as follows. The difference between the trajectories $\{x_v(t), u_v(t)\}$ of the converted system (5) and those of $\{x'(t), u'(t)\}$ of the given system (1) for the ideal case is due to three things; the error $\|F_1 - F_p\|$ for approximation of the eigenvalues of the state matrix F1 of (20) to algebraic integers, the error due to finite impulse approximation for the part (21), and the presence of the perturbations $\{e_v(t), e_u(t), e_{v,0}\}$ in (5). Since the two approximation errors can be made arbitrarily small by increasing the parameters $\{k_1, k_2\}$, it follows that the condition A_2 for the system (1)

also holds with respect to the converted system (5) and the perturbations f{$e_v(t)$, $e_{u(t)}$, $e_{v,0}$}, with appropriate choice of {k_1, k_2}.

Definition (5.4) [8] The p-form representation of a vector $x \in R^n$, where $p \in \mathbb{N}$, is defined as follows:

$$x[p] = \left(x_1^p, x_1^{p-1}x_2, x_1^{p-1}x_3, \ldots, x_1^{p_1}x_2^{p_2}, \ldots, x_n^{p_n}, x_n^p\right) \quad (29)$$

This p-form representation contains sentences as $x^{p_1}, x^{p_2}, x^{p_n}$ which

$$p_1 + p_2 + \cdots + p_n = p,\ p_i \in N_0 \quad (30)$$

Where $N_0 = N\ \{0\}$.

To create the z[P] representation in a standard way, lexicography can be used. For instance, when p = 5 and n = 3, the lexicographic order is as follows:

$$\begin{aligned} x^{[5]} = \Big(&x_1^5, x_1^4x_2, x_1^4x_3, x_1^3x_2^2, x_1^4x_2x_3, x_1^3x_3^2, \\ &x_1^2x_2^3, x_1^2x_2^2x_3, x_1^2x_2x_3^2, x_1^3x_3^3, x_1x_2^3x_2, \\ &x_2x_2^2x_3^2, x_1x_2x_3^3, x_1x_3^4, x_x^5, x_2^4x_3, x_2^3x_3^2, x_2^2x_3^3, x_2x_3^4, x_3^5\Big) \end{aligned} \quad (31)$$

For any integers p and n, it can be demonstrated that there exist m. These systems involve functions of a single sentence of p degree in a p-form representation. We utilize homogeneous dynamic systems with useful features. It is assumed that the equilibrium point of the system is at the origin.

Lemma (5.5) [8] Assuming that the dynamic system $\dot{z} = (z)$ is homogeneous. If the vector field is continuous and the equilibrium point of the system is stable, then a homogeneous Lyapunov function can be used to prove the stability of the system. This lemma actually limits the search scope to the Lyapunov function for homogeneous functions, which can be valuable from the computational point of view. The following lemma provides a comprehensive version of this proposition.

Lemma (5.6) [8] For the homogeneous dynamical system $\dot{z} = (z)$, which belongs to Sk, the derivative $\dot{V} \in Hp+k-1$ of the function $V \in Hp+k-1$ along the solutions of the system is a homogeneous function of degree, p + k − 1.

The Lyapunov theorem (Lyapunov's direct method) is the most well-known theorem for analyzing and designing nonlinear systems. It provides sufficient conditions for the stability of the equilibrium point. Additionally, the instability theory demonstrates the unstable equilibrium point for unstable systems. We discussed equilibrium stability by first deriving the Lyapunov candidate function with a negative definite term and then determining the sign of the function.

Theorem (5.7) [6] Assume the dynamical system $\dot{z}= (z)$. If there exists a continuous partial function V(z) such that V(0) = 0 and $\dot{V}(z)$ is negative definite along the system responses, then the equilibrium point of the system is asymptotically stable if V(X) is positive. Otherwise, the equilibrium point is unstable. We prove that the function V(x) is neither positive nor negative semi-definite for the given dynamical system. Assuming the contrary, if V(x) is positive semi-definite, then at a point x_0 outside the origin, we have $V(x_0) = 0$. However, this contradicts the theorem's assumption. The hypothesis is invalidated because, out of origin, V(x) Passing point x_0 contradicts the positive semi-definiteness of the V(x) function. characteristic of the V(x) function. Similarly, it can be demonstrated that V(x), never negative semi-definite. So we may say that V(z) has three states: totally positive definite, totally negative definite, and undetermined. We will examine each of these three modes one by one:

i. If Situation V(x) > 0, then the Lyapunov theorem applies. This theorem states that if there exists a positive function V(x) whose derivative is always negative definite, then the equilibrium point is asymptotically stable.

ii. When Situation V(s) is less than zero, the hypotheses of the instability theory can be obtained by setting Λ equal to negative In summary, the dynamical system studied exhibits instability of the equilibrium point due to $\Lambda > 0$ and $\Lambda > 0$.

iii. V(x) is an indeterminate situation. The change of sign of V(x) around the equilibrium point indicates a negative sign of V(x) in the region surrounding the point. For this situation, the small area adjacent to the equilibrium point has both negative sign V(x) and $\dot{V}(x)$. According to condition 2, we can conclude that the equilibrium point is unstable. This section focuses on homogeneous systems and proposes two methods for forming the Lyapunov function. The global stability of the equilibrium point is then concluded using these methods. Consider the homogeneous nonlinear dynamical system x = f(x) where f ∈ Sk. The basic functions $V_i(x)$ in the i-th entry of the representation corresponding to state vector $x \in \mathbf{R}^n$ are as follows:

$$V_i(x) = x_j^{[p]} \quad (32)$$

The function of the Lyapunov candidate is constructed as a linear combination of these basic functions.

$$V(x)=\sum_{j=1}^{m} a_i v_j(x) = a^T\left(x^{[p]}\right)^T \qquad (33)$$

It called Equation (4.2.7) in this section.

$$m=\begin{pmatrix} p+k-1 \\ p \end{pmatrix} \qquad (34)$$

The number of terms in p-form is represented by 's', while 'a_i' are coefficients that need to be calculated as the process continues. It is important to note that the p-form exhibitions are considered to be linearly independent. Equation (34) has unique linear composition coefficients. However, it is evident that V(0) equals zero. Additionally, based on the symbol presented in Equation (34), the coefficient vector is as follows: $a=[a_1 \;\; a_2 \ldots a_m]$. Now, by deriving the proposed Lyapunov Equation (34) for the homogeneous system x = f(x) we have:

$$\dot{V}(x)=\sum_{i=1}^{m} a_i \dot{v}_j(x) \equiv a^T H^T\left(x^{[p+k-1k]}\right)^T < 0 \qquad (35)$$

It called Equation (35) in this section.

The problem involves calculating an intermediate matrix H, which depends on the specific problem. It is important to note that, according to Lemma (5.5), $\dot{V}(X)$ is homogeneous of degree p + k − 1, and the linear combination of the base functions $V_i(X)$ in Eq. (36) is also homogeneous of degree p + k − 1. The method for calculating the intermediate matrix is explained in the following section. Thus, the task is to compute a vector that satisfies Eq. (36). To accomplish this, we set $\dot{V}(x)$ equal to a specific negative function and calculate the unknown coefficients. To illustrate general methods, let us first explain the subject with an example. To do this, let us consider the following dynamic system with an equilibrium point at the origin.

$$\begin{cases} \dot{x}_1 = -x_1^3 - 2x_2^3 \\ \dot{x}_2 = 3x_1^3 - 3x_2^3 \end{cases} \qquad (36)$$

The following lines analyze the stability status of the equilibrium point. It is obvious that the aforementioned system is homogeneous. Therefore, we can select the Lyapunov function to assess stability. The function is a homogeneous form of degree 4.

$$V(x)=a_1x_1^4+a_2x_1^3x_2+a_3x_1^2x_2^2+a_4x_1x_2^3,a_5x_2^4 \qquad (37)$$

Calculate the derivation of the system along its paths.

$$\begin{aligned} \dot{V}(x) &= (-4a_1+3a_2)x_1^6+(-3a_2+6a_3)x_1^5x_2 \\ &+(-2a_3+9a_2)x_1^4x_2^2+(-8a_1+3a_2-a_4+12a_5)x_1^6x_2^3 \\ &+(-6a_2-6a_3)x_1^2x_2^4+(-4a_3-9a_4)x_1x_2^5+(-2a_4-12a_2)x_2^6 \end{aligned} \qquad (38)$$

derivation of the system along its paths.

By replacing the above phrase with a negative phrase such as $-12x^{16} - 24x^{26}$, we can obtain the following unique solutions for the coefficients:

$a_1 = 3$, $a_2 = a_3 = a_4 = 0$, $a_5 = 2$. Thus, we obtain the following Lyapunov function.

$$V(x)=3x_1^4+2x_2^4 \qquad (39)$$

This clearly shows the equilibrium point's asymptotic stability. As demonstrated in this example, the number of required equations was also adequate to determine the unique factors of the unknown coefficients. And so the Lyapunov function was discovered. However, there is no guarantee that the equations produced from the unification of a derivative function with a desired negative definite phrase provide a unique result. We will explain the preceding example in a more-broad context, resulting in a method for determining the Lyapunov function. The method described here is easily adaptable to more general systems. Think about the following: degree 3 nonlinear homogeneous system.

$$\begin{cases} \dot{x}_1 = b_{11}x_1^3 + b_{12}x_2^3 \\ \dot{x}_2 = b_{21}x_1^3 + b_{22}x_2^3 \end{cases} \quad (40)$$

It called Equation (40) in this research. To begin, select a homogeneous Lyapunov candidate function of degree 4 as follows:

$$\begin{aligned} V(x) &= a_1x_1^4 + a_2x_1^3x_2 + a_2x_1^2x_2^2 + a_5x_1^4 \\ &= a^T\left(x^{[4]}\right)^T \end{aligned} \quad (41)$$

It called Equation (41). Deriving this function in time gives:

$$\begin{aligned} \dot{V}(x) &= 4\dot{x}_1x_1^3a_1 + \left(3\dot{x}_1x_1^2x_2 + x_1^2\dot{x}_2\right)a_2 \\ &+ \left(2\dot{x}_1x_2^2x_1 + 2x_1^2\dot{x}_2x_2\right)a_2 \\ &+ \left(\dot{x}_1x_2^3 + 3x_1\dot{x}_2x_2^2\right)a_4 + 4\dot{x}_2x_2^3a_5 \end{aligned} \quad (42)$$

When the dynamics of Eq. (42) are included into V, the preceding statement is reduced to:

$$\begin{aligned} \dot{V}(x) &= \left(4b_{11}a_1 + b_{21}a_2\right)x_1^6 + \left(3b_{11}a_2 + b_{21}a_3\right)x_1^5x_2 \\ &+ \left(2b_{11}a_3 + 3b_{21}a_2\right)x_1^4x_2^2 \\ &+ \left(4b_{12}a_1 + b_{22}a_2 + b_{11}a_4 + 4b_{21}a_5\right)x_1^3x_2^3 \\ &+ \left(3b_{12}a_2 + 2b_{22}a_3\right)x_1^2x_2^4 \\ &+ \left(2b_{12}a_3 + b_{22}a_4\right)x_1x_2^5 + \left(b_{12}a_4 + 4b_{22}a_5\right)x_2^6 \end{aligned} \quad (43)$$

It called Equation (43).

Which is obtained in the matrix format:

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{bmatrix}^T \begin{bmatrix} 4b_{11} & 0 & 0 & 4b_{12} & 0 & 0 & 0 \\ b_{21} & 3b_{11} & 0 & b_{22} & 3b_{12} & 0 & 0 \\ 0 & 2b_{21} & 2b_{11} & 0 & 2b_{22} & 2b_{12} & 0 \\ 0 & 0 & 3b_{21} & b_{11} & 0 & 2b_{22} & b_{12} \\ 0 & 0 & 0 & 4b_{21} & 0 & 0 & 4b_{22} \end{bmatrix} \begin{bmatrix} x_1^6 \\ x_2^5x_2 \\ x_1^4x_2^2 \\ x_1^3x_1^3 \\ x_1^2x_2^4 \\ x_1x_2^5 \\ x_2^6 \end{bmatrix} = a^TH^T\left(x^{[6]}\right)^T$$

(44)

It called Equation (44).

$$H=\begin{bmatrix} 4b_{11} & b_{21} & 0 & 0 & 0 \\ 0 & 3b_{11} & 2b_{21} & 0 & 0 \\ 0 & 0 & 2b_{11} & 3b_{21} & 0 \\ 4b_{12} & b_{22} & 0 & b_{11} & 4b_{21} \\ 0 & 3b_{12} & 2b_{22} & 0 & 0 \\ 0 & 0 & 2b_{12} & 2b_{22} & 0 \\ 0 & 0 & 0 & b_{12} & 4b_{22} \end{bmatrix} \quad (45)$$

It called Equation (45).

We now equalize Eq. (44) with a negative function, such as $Z^T(x^{[p+k-1]})^T$:

$$\dot{V}(x) \equiv Z^T(x^{[p+k-1]})^T \quad (46)$$

It called Equation (46) in this section.

In the two-variable mode n = 2, for example, the decision for Z can be as follows:

$$Z=\begin{bmatrix}-1 & 0 & -1 & 0 \ldots 0 & -1\end{bmatrix}^T \quad (47)$$

It called Equation (47).

As a result of comparing Equation. (44) and (46), the unknown coefficients a can be derived by solving the following equation.

$$Ha = Z \quad (48)$$

It called Equation (48).

According to the coefficients of the basic functions, since the number of unknowns (a_i) (the vector length of x[p]) in the resulting Equation (48) is less than the number of equations (that is, the vector length of x[p+k1]) and the coefficients are not exactly determined, one method to determine the optimal of these abnormalities is to use The least squares method, which proposes the following response from Equation (48).

$$a = (H^TH)^{-1} H^TZ \quad (49)$$

It called Equation (49).

Following the calculation of the a′s coefficients, the sign of V (x) should be confirmed. In the event that the required signs are not obtained, two options are suggested:

i. Reselect the Z vector, then confirm the required sign for the V (x) and assign the V(x) sign.

ii. Increase the degree of Lyapunov's function and then repeat the preceding algorithm stages.

6. Result

Theorem (6.1) For any linear time-invariant system (1) satisfying stability assumptions A_1 and A_2, it can be converted into a linear time-varying system (5) with integer state matrices, capable of operating on encrypted data over an infinite time horizon, by achieving the following conditions:

- The unstable component's state matrix (F_1) is approximated to an algebraically integer matrix Fp such that $\|F_1 - Fp\| \le \alpha$ for any $\alpha > 0$, with a transformation T and integer $k_1 \in \mathbb{N}$ satisfying $T\,Fp^{k1}\,T^{-1} \in \mathbb{Z}^{n1xn1}$.
- The stable component (F_2) is approximated using Finite Impulse Response (FIR) with parameter $k_2 \in \mathbb{N}$ such that $\|F_2^{k2}\| \le \eta$ for any $\eta > 0$.

With appropriate selection of parameters k_1 and k_2, and given an upper bound on perturbations $\eta_v > 0$, the converted system achieves:

$\|x_v(t) - x'(t)\| \le \varepsilon$, $\|u_v(t) - u'(t)\| \le \varepsilon$, for any $\varepsilon > 0$ and all $t \in \mathbb{N}_0$

- Moreover, the lifted system satisfies a quadratic performance test where there exist matrices $X > 0$ and $\tau > 0$ satisfying inequalities (14)-(16), yielding improved ℓ_2-gain values compared to traditional tests (as shown in the numerical example: from 5.13 to 3.97).

Proof. The proof follows directly from applying Theorems (3.3) and (3.5), Lemmas (3.4), (5.1), and (5.3), where robust stability analysis is combined with system conversion to integer form, ensuring implement ability on encrypted data while maintaining performance asymptotically equivalent to the original system.

7. Conclusion:

This paper concluded that the use of homomorphic encryption in control systems represents an effective solution for protecting data from cyber-attacks in networked systems. The proposed methodology for converting linear systems to systems with integer state matrices proved effective in enabling control operations on encrypted data for unlimited time periods, eliminating the need for re-encryption or resetting. The stability and performance tests presented using robust control theory with lifting techniques showed superior accuracy compared to traditional methods, especially when applied to Reset and FIR controllers. Furthermore, the analysis was extended to include homogeneous nonlinear systems using Lyapunov functions, enhancing the comprehensiveness of the approach. The paper recommends applying these methodologies in critical industrial applications requiring high data protection, while suggesting future improvements to reduce errors resulting from quantization and encryption.

References:

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.
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.
K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in Proc. 54th IEEE Conf. Decision and Control (CDC), 2015.
A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Towards private data-driven control," in Proc. 59th IEEE Conf. Decision and Control (CDC), 2020, pp. 5449–5456.
M. Schulze Darup, "Encrypted model predictive control in the cloud," in Privacy in Dynamical Systems, Singapore, Springer, 2019, pp. 231–265.
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), 2022.
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.
C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semihomomorphic encryption," IEEE Trans. Autom. Control, vol. 65, no. 9, pp. 3950–3957, 2020.
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), 2021, pp. 952–957.
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), 2024, pp. 2037–2042.
C. Gentry, A Fully Homomorphic Encryption Scheme, Ph.D. thesis, Stanford University, 2009.
J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song, "Bootstrapping for approximate homomorphic encryption," in Advances in Cryptology – EUROCRYPT 2018, Tel Aviv, Israel, Springer Cham, 2018, pp. 360–384.
A. Al Badawi and Y. Polyakov, "Demystifying bootstrapping in fully homomorphic encryption," Cryptol. ePrint Arch., Paper 2023/149, 2023.
C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. P. Fitzek, and N. Aaraj, "Survey on fully homomorphic encryption, theory, and applications," Proc. IEEE, vol. 110, no. 10, pp. 1572–1609, 2022.
S. Schlor and F. Allgöwer, "Bootstrapping guarantees: Stability and performance analysis for dynamic encrypted control," IEEE Control Syst. Lett., vol. 8, pp. 2235–2240, 2024.
J. Kim et al., "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," IFAC-PapersOnLine, vol. 49, no. 22, pp. 175–180, 2016.
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), 2018, pp. 5020–5025.
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), 2021.
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), 2023, pp. 5091–5096.
J. Lee, D. Lee, and J. Kim, "Stabilization by controllers having integer coefficients," 2025. Preprint: https://arxiv.org/abs/2505.00481.
C. Scherer and S. Weiland, Linear Matrix Inequalities in Control, vol. 3, Delft, The Netherlands, Lecture Notes, Dutch Institute for Systems and Control, 2000.
S. Lang, M. Seidel, and F. Allgöwer, "Robust performance for switched systems with constrained switching and its application to weakly hard real-time control systems," in Cyber-physical Networking (in publication), Springer, 2024. Preprint: https://arxiv.org/abs/2411.08436v1.
M. Green and D. J. N. Limebeer, Linear Robust Control, Englewood Cliffs, NJ, Prentice-Hall, 1995.

MOSEK ApS, MOSEK Optimization Toolbox for MATLAB 10.2.17, 2024.
J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in Proc. CACSD Conf., Taipei, Taiwan, 2004.
P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology – EUROCRYPT 1999, Springer, 1999, pp. 223–238.
O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in Proc. 37th Annual ACM Symp. Theory of Computing (STOC), 2005, pp. 84–93.
Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci. (FOCS), 2011, pp. 97–106.
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.