

Encrypted Observer-based Control for Linear Continuous-Time Systems

Hung Nguyen¹, Binh Nguyen², Hyung-Gohn Lee¹ and Hyo-Sung Ahn¹, *Senior Member, IEEE*

Abstract—This paper is concerned with the stability analysis of encrypted observer-based control for linear continuous-time systems. Since conventional encryption has limited ability to deploy in continuous-time integral computation, our work presents systematically a new design of encryption for a continuous-time observer-based control scheme. To be specific, in this paper, both control parameters and signals are encrypted by the learning-with-errors (LWE) encryption to avoid data eavesdropping. Furthermore, we propose encrypted computations for the observer-based controller based on its discrete-time model, and present a continuous-time virtual dynamics of the controller for further stability analysis. Accordingly, we present novel stability criteria by introducing linear matrix inequalities (LMIs)-based conditions associated with quantization gains and sampling intervals. The established stability criteria with theoretical proofs based on a discontinuous Lyapunov functional possibly provide a way to select quantization gains and sampling intervals to guarantee the stability of the closed-loop system. Numerical results on DC motor control corresponding to several quantization gains and sampling intervals demonstrate the validity of our method.

Index Terms—LWE-based encryption, observed-based controller, sampled-data system, discontinuous Lyapunov functional, LMIs.

I. INTRODUCTION

In recent years, the development of cloud computing has received great attention in many modern control systems such as smart grids, intelligent transportation systems, and robotics [1]–[5], and the security threat has been one of the main issues [6]–[8]. There are many types of attacks, such as Denial of Service (DoS) attack [9]–[11], zero dynamic attack [7], reply attack [8] and eavesdropping attack [12]. Among these attacks, eavesdropping is a basic one, which is performed to steal confidential information to apply more advanced attacks.

In eavesdropping attacks, communicating and processing data on a third-party platform may lead to data eavesdropping. As can be seen from Fig. 1, an eavesdropper is able to steal data through both communication and collaboration with the controller without encryption. Additionally, even if the communications are encrypted as in Fig. 1b, the attacker can still collaborate with the controller for data eavesdropping. Harnessing a homomorphic encryption (HE), an encrypted controller can perform directly on encrypted signals and parameters without decryption (Fig. 1c), which could protect the

control system from eavesdroppers [12]–[17]. A model predictive control was implemented using additively HE in [18] and [19]. A state-vector estimator using a private Extended Kalman Filter was proposed in [20]. Secure distributed control schemes based on encryption for multi-agent systems were considered in [21]–[24]. The work [25] applied the Paillier encryption [26] to encrypt the control signals for a linear control system, and a static output feedback controller was considered. In [27], the authors provided a dynamic feedback controller over encrypted data utilizing homomorphic features of cryptosystems, whose performance is similar to the linear dynamic controllers over real-valued data. By applying an integer conversion for the state matrix of the controller without scaling, they showed that a system could be converted to another system with the same input-output relation. However, the integer conversion process can only be applied to a class of systems under certain conditions. In [28], the authors proposed a quantization design for a linear control system, in which not only the controller parameters are quantized, but the control signals are also quantized. Using a dynamic quantizer with a sensitivity that depends on the system's state and control signals, they showed that asymptotic stability could be achieved.

However, there have still been many challenging issues in the encrypted control systems. Firstly, the encrypted controller can only perform with integers [27], [28], which requires a quantization process that results in quantization errors. For dynamic controllers such as observer-based controllers, the quantization errors could be accumulated over time if the state matrix of the controller contains at least one non-integer element [27]. Secondly, since plants are continuous-time while the encrypted controllers are formulated in terms of integer computation, that leads to difficulties in the stability analysis of the encrypted control systems in the presence of the quantization errors and sampling-data process. Both quantization gains and sampling intervals have critical impacts on the encrypted observer-based control system analysis. As far as we are concerned, there has been little progress toward the criteria of quantizer and sampling intervals for encrypted observer-based continuous linear time-invariant (LTI) systems.

To address these difficulties, this paper investigates the design of the quantizers and sampling intervals for the encrypted observer-based control systems. The contributions of this work are summarized as follows.

- 1) First, we make the first attempt to consider an encrypted observer-based controller for a continuous-time LTI system. Since encryption does not support continuous-time integral, the observer-based controller should be formulated in the discrete-time form. However, the plant

¹Hung M. Nguyen, Hyung-Gohn Lee and Hyo-Sung Ahn are with the School of Mechanical Engineering, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, South Korea (e-mail: nguyennh@gist.ac.kr; hyunggohnlee@gm.gist.ac.kr; hyosung@gist.ac.kr).

²Binh T. Nguyen is with College of Engineering, Texas A&M University-Corpus Christi, Corpus Christi, TX 78412, United States (email: binh.nguyen@tamucc.edu).

is continuous-time, which results in difficulties in the stability analysis of the encrypted control system. Taking advantage of discretizing continuous-time Luenberger observers, this paper presents a novel encrypted observer-based controller allowing us to analyze the continuous-time stability of the closed-loop system. By introducing continuous-time virtual dynamics of the encrypted controller, we succeed in formulating the closed-loop system in a sampled-data system and providing stability criteria for the system. Unlike many existing works [13]–[15], [28], where the stability analysis is concerned with discrete-time systems, we provide a continuous-time stability analysis taking into account both the quantization and sampling actions.

- 2) Differing from [28], [29], our work presents conditions for the selection of quantization gains and sampling intervals by which all quantization gains can be predetermined independently from system signals (e.g., system outputs and estimated states). It is worth noting that the determination of the quantization gains (or sensitivity) from [28], [29] is required at each time step and also needs the system signals.
- 3) Finally, we introduce novel stability criteria in terms of LMIs-based conditions and give theoretical proof based on a discontinuous Lyapunov functional for sampled-data systems. We also provide some novel results for stability analysis of a linear sampled-data system with disturbances by introducing a framework in which global asymptotic stability of a linear sampled-data system can be ensured under bounded energy disturbance. The proposed criteria are associated with the quantization gains and sampling interval, and by selecting appropriate values for the quantization gains and sampling interval, the global asymptotic stability of the closed-loop system can be ensured.

Notations: The set of real numbers, integers, non-negative real numbers, positive real numbers, positive integers, and natural numbers are denoted by $\mathbb{R}, \mathbb{Z}, \mathbb{R}_+, \mathbb{R}_{++}, \mathbb{Z}_{++}, \mathbb{N}$, respectively. The symbol $\mathbb{R}^{n \times m}$ indicates the set of matrices with n rows and m columns. The set of symmetric matrices with dimension n is denoted by \mathbb{S}^n . Additionally, \mathbb{S}_{++}^n represents the set of positive definite symmetric matrices. Describe the set of modulo $q \in \mathbb{N}$ by $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$. The symbol $\lfloor \cdot \rfloor$ denotes the rounding function. For a vector, $\|\cdot\|$ indicates the Euclidean norm, while for a matrix, $\|\cdot\|$ represents the Frobenius norm. For a symmetric matrix, its minimum and maximum eigenvalues are denoted by $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$, respectively. For any matrix \mathcal{X} , the notations $\mathcal{X} \succ 0$ (or $\mathcal{X} \succeq 0$) and $\mathcal{X} \prec 0$ (or $\mathcal{X} \preceq 0$) mean that \mathcal{X} is a positive definite (or positive semi-definite) matrix and a negative definite (or negative semi-definite) matrix, respectively. The symbols I and 0 represent the identity and zero matrices with suitable dimensions, respectively; additionally, I_n represents the identity matrix with n rows and n columns. For any entity z , $z(t_k)$ denotes the value of z during $[t_k, t_{k+1})$. In symmetric block matrices, the asterisk (*) indicates the terms induced by symmetry. For any square matrix \mathcal{Q} , $\mathbf{He}\{\mathcal{Q}\} = \mathcal{Q} + \mathcal{Q}^\top$. The

notation \times represents the multiplication of two matrices or the Cartesian product of two sets.

II. PRELIMINARIES

A. Encryption

This subsection introduces the cryptosystem utilized in this paper. For an unencrypted value, we call it a plaintext while an encrypted value is called a ciphertext. Denote \mathcal{C} the ciphertext space, let $\text{Enc} : \mathbb{Z}_q \rightarrow \mathcal{C}$ represent the encryption map, and $\text{Dec} : \mathcal{C} \rightarrow \mathbb{Z}_q$ denote the decryption map. We briefly describe LWE-based encryption [30] as follows.

- Choose a private key $k_p \in \mathbb{Z}_q^n$, a random vector $a \in \mathbb{Z}_q^n$, and a small random error $e \in \mathbb{Z}_q$.
- **Encryption:** For a plaintext $m \in \mathbb{Z}_q$, the corresponding ciphertext is computed as

$$\text{Enc}(m) \triangleq \left(\begin{bmatrix} m + k_p^\top a + e \\ a \end{bmatrix} \mod q \right) = c \in \mathbb{Z}_q^{n+1}.$$

- **Decryption:** For the ciphertext $c \in \mathcal{C}$ corresponding to the plaintext $m \in \mathbb{Z}_q$, define

$$\text{Dec}(c) \triangleq [1 \quad -k_p^\top] c \mod q.$$

It is obvious that $\text{Dec}(c) = m + e$. To deal with the error e , let us consider the encryption with gain $G > 0$ as

$$c_G = \text{Enc}(Gm) = \left[\begin{bmatrix} Gm + k_p^\top a + e \\ a \end{bmatrix} \mod q \right] \quad (1)$$

Then, with $G \in \mathbb{Z}_q$ being a positive gain such that $G > 2e$, the plaintext can be recovered as

$$\left\lfloor \frac{\text{Dec}(c_G)}{G} \right\rfloor = \left\lfloor m + \frac{e}{G} \right\rfloor = m.$$

Hereafter, when considering a ciphertext, we always assume that it is encrypted with a suitable gain G .

1) *Additive property:* For $c_1, c_2 \in \mathcal{C}$, $c = c_1 + c_2 \mod q$, and $c' = kc_1 \mod q$ with $k \in \mathbb{Z}_q$, one has

$$\begin{aligned} \text{Dec}(c) &= \text{Dec}(c_1) + \text{Dec}(c_2), \\ \text{Dec}(c') &= k\text{Dec}(c_1). \end{aligned}$$

2) *Multiplication:* To have the ability of multiplication, let us introduce a separate algorithm for encrypting the multipliers utilized in [31]. Consider the ciphertexts $c_1, c_2 \in \mathbb{Z}_q^{n+1}$ corresponding to the plaintexts $m_1, m_2 \in \mathbb{Z}_q$. Choose $q \in \mathbb{Z}_{++}$ such that there exist $\omega, d \in \mathbb{Z}_q$ and $\omega^d = q$. Let $\mathcal{D}(\cdot)$ denote the function that decomposes the argument by its string of digits as $\mathcal{D}(b) = [b_1, \dots, b_d]^\top$ with $0 \leq b_i \leq \omega - 1$, $\forall i \in \{1, 2, \dots, d\}$, and $b \in \mathbb{Z}_q$. Thus, the ciphertext c_2 could be written as

$$c_2 = H\mathcal{D}(c_2), \quad (2)$$

with $H = [I_{n+1} \quad \omega I_{n+1} \quad \dots \quad \omega^{d-1} I_{n+1}]$. To illustrate the decomposition in (2), let us consider an example with $q = 16$, $\omega = 2$ and $d = 4$, it holds $\omega^d = q$. Then, the integer $c_2 = 13$ can be written as $c_2 = H\mathcal{D}(c_2)$ with

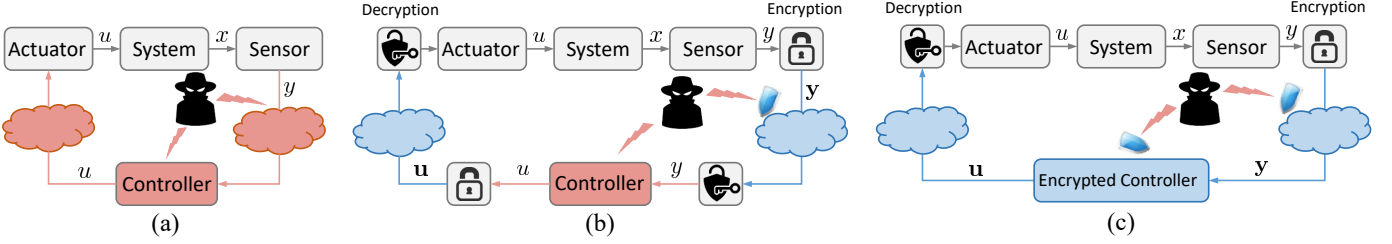


Fig. 1: (a) A cloud-based control scheme without encryption, (b) a cloud-based control scheme with encryption-based secure communications and an unencrypted controller, and (c) a cloud-based control scheme with both encryption-based secure communications and controller. The red indicates the parts of the system vulnerable to the attack, and the blue represents the parts protected against the attack by encryption.

$H = [2^0 \ 2^1 \ 2^2 \ 2^3]$ and $\mathcal{D}(c_2) = [1 \ 0 \ 1 \ 1]^\top$. The multiplier is then encrypted as follows

$$\begin{aligned} \text{Enc}'(m_1) = m_1 H + & \begin{bmatrix} k_p a_1 & k_p a_2 & \dots & k_p a_{d(n+1)} \\ a_1 & a_2 & \dots & a_{d(n+1)} \end{bmatrix} \\ & + \begin{bmatrix} e_1 & e_2 & \dots & e_{d(n+1)} \\ 0_n & 0_n & \dots & 0_n \end{bmatrix} \mod q. \end{aligned} \quad (3)$$

Then, the multiplication between two ciphertexts c_1 and c_2 is defined as

$$c_1 \odot c_2 \triangleq \text{Enc}'(m_1) \mathcal{D}(c_2) \mod q.$$

To see the homomorphic property, we note that

$$\text{Dec}(\text{Enc}'(m_1) \mathcal{D}(c_2)) = m_1 m_2 + e \mod q, \quad (4)$$

with $e = [e_1 \ \dots \ e_{d(n+1)}] \mathcal{D}(c_2)$. To deal with the error in (4), we similarly consider the encryption with a gain G as in (1), and by selecting a large enough value of G , the error in (4) vanishes and the multiplication $m_1 m_2$ could be exactly recovered. Note that the encryption and decryption functions can be applied element-wisely to vectors or matrices.

B. Quantization

Consider the uniform quantizer with the following form

$$Q_\Theta(x) = \frac{1}{\Theta} (\lfloor \Theta x \rfloor), \quad (5)$$

where the quantization gain $\Theta > 0$ is a positive value. For the uniform quantizer (5), with $x \in \mathbb{R}^n$ and $X \in \mathbb{R}^{m \times n}$, the bounds on the quantization errors are always given as

$$\|Q_\Theta(x) - x\| \leq \frac{\sqrt{n}}{2\Theta}, \quad \|Q_\Theta(X) - X\| \leq \frac{\sqrt{mn}}{2\Theta}. \quad (6)$$

We note that if the quantization gain Θ is a fixed value, then the quantizer is static. However, if the quantization gain varies over time, the quantizer is called a dynamic quantizer.

C. Sampled-data observer-based controller

For a linear continuous-time system

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases} \quad (7)$$

let $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^r$ stand for the state vector, control input, and output, respectively. The system's matrices A, B , and C are given in appropriate dimensions. We

consider a sampled-data observer-based controller to stabilize the system (7). Since the system (7) is continuous-time, we take the set of sampling instants $\mathcal{I} = \{t_1, \dots, t_i, \dots\}$, with $\lim_{i \rightarrow \infty} t_i = \infty$, and the constant time interval $h = t_{i+1} - t_i > 0, \forall i \geq 0$. Let $\chi(t)$ be the estimation of $x(t)$ and assume that the matrices L, C, K are given in appropriate dimensions. Then the conventional Luenberger's observer-based controller is given in the following form

$$\dot{\chi}(t) = A\chi(t) + Bu(t) + L(y(t_k) - C\chi(t_k)), \quad (8a)$$

$$u(t) = K\chi(t_k), \quad \forall t \in [t_k, t_{k+1}). \quad (8b)$$

To investigate the stability of the sampled-data observer-based control system (7) and (8), consider the following linear sampled-data system

$$\dot{z}(t) = \mathcal{A}z(t) + \mathcal{A}_c z(t_k) + \eta(t), \quad (9)$$

where $\mathcal{A}, \mathcal{A}_c$ are given constant matrices, and $\eta(t)$ is the disturbance.

Definition 1 (Integral Quadratic Constraint [32]): The system (9) is said to satisfy integral quadratic constraint (IQC) if for any initial condition $z_0 = z(t_0)$, its solution satisfies

$$\lim_{t \rightarrow \infty} \int_{t_0}^t \|z(\tau)\|^2 d\tau < \infty. \quad (10)$$

The IQC in Definition 1 also implies global asymptotic stability of (9). The following lemmas are useful for stability analysis of the sampled-data system (9).

Lemma 1: Let $\Gamma = \Gamma^\top, \Pi_1, \Pi_2, \Omega$ and Δ be the matrices with appropriate dimensions. Then, the inequality $\Gamma + \Pi_1 \Delta^\top \Pi_2 + \Pi_2^\top \Delta \Pi_1^\top + \Delta \Omega \Delta^\top \preceq 0$ holds if there exist $\epsilon, \kappa > 0$ such that

$$\begin{bmatrix} \Gamma + \kappa(\Pi_1 \Pi_1^\top + I) & \Pi_2^\top \\ \Pi_2 & -\epsilon I \end{bmatrix} \preceq 0, \quad (11a)$$

$$\Omega - \epsilon I \preceq 0. \quad (11b)$$

Proof: The proof can be completed using \mathcal{S} -procedure [33].

Lemma 2: [34] Let $R \succ 0$, and $z(t)$ be a differential function. Then for all matrices N_1, N_2 given in appropriate dimensions, the following inequality holds

$$\int_{t_k}^t \dot{z}^\top(\tau) R \dot{z}(\tau) d\tau \geq \xi^\top(t) \Phi \xi(t), \quad (12)$$

where $\Phi = \mathbf{H}\mathbf{e}\{\Phi_1^\top N_1 + \Phi_2^\top N_2\} - (t - t_k)(N_1^\top R^{-1}N_1 + \frac{1}{3}N_2^\top R^{-1}N_2)$, $\Phi_1 = E_1 - E_2$, $\Phi_2 = E_1 + E_2 - 2E_3$, $E_1 = [I \ 0 \ 0]$, $E_2 = [0 \ I \ 0]$, $E_3 = [0 \ 0 \ I]$ and $\xi(t) = [z^\top(t), z^\top(t_k), \frac{1}{t-t_k} \int_{t_k}^t z^\top(\tau)d\tau]^\top$.

III. PROPOSED ENCRYPTED OBSERVER-BASED CONTROL

In this section, we first propose an encrypted observer-based controller for a continuous LTI system in which, the control parameters and signals are encrypted to avoid eavesdropping attacks. Second, we formulate the closed-loop system in the form of a linear sampled-data system with uncertainties and disturbance.

A. Observer-based secure control scheme

In this part, we present a secure version of the observer-based controller (8), in which the objective is to stabilize the system (7) while ensuring security with the use of LWE-based encryption. For this purpose, all parameters and control signals in (8) need to be encrypted. It can be seen that (8a) cannot be computed based on encrypted signals since LWE-based encryption does not allow computing on continuous-time integral. Thus, in order to compute the observer-based controller (8a) in an encrypted way, we first take advantage of its solution at each sampling time as follows

$$\chi(t_{k+1}) = A_d \chi(t_k) + B_d u(t_k) + L_d (y(t_k) - C \chi(t_k)), \quad (13a)$$

$$u(t_k) = K \chi(t_k), \quad (13b)$$

with $A_d = e^{A_h}$, $B_d = \int_0^h e^{A\tau} B d\tau$ and $L_d = \int_0^h e^{A\tau} L d\tau$. Given that the controller (13) is executed at the computational unit, which is possibly located far away from the plant, then for security purposes, the unencrypted matrices A_d, B_d, L_d, C, K and values $y(t_k)$ are not sent directly to the computational unit. Instead, the following encrypted values obtained through (1) and (3) based on LWE are utilized

$$\mathbf{y}(t_k) = \text{Enc}(\lfloor \Lambda \Lambda_k y(t_k) \rfloor), \mathbf{A}_d = \text{Enc}'(\lfloor \Lambda^2 A_d \rfloor),$$

$$\mathbf{B}_d = \text{Enc}'(\lfloor \Lambda B_d \rfloor), \mathbf{L}_d = \text{Enc}'(\lfloor \Lambda L_d \rfloor),$$

$$\mathbf{C} = \text{Enc}'(\lfloor \Lambda C \rfloor), \mathbf{K} = \text{Enc}'(\lfloor \Lambda K \rfloor),$$

with a positive value Λ and a possibly time-varying positive value Λ_k . It is worth mentioning that, similar to [27], we use different quantization gains for different entities. The quantizers with static gains are employed to quantize the matrices A_d, B_d, L_d, C and K in the controller (13), while the quantizer with a possible dynamic gain is utilized for quantizing the output measurement $y(t_k)$. By letting $\chi(t_k) = \text{Enc}(\lfloor \Lambda_k \chi(t_k) \rfloor)$ and $\chi'(t_k) = \text{Enc}(\lfloor \Lambda^2 \Lambda_{k-1} \chi(t_k) \rfloor)$, (13) is encrypted as

$$\chi'(t_{k+1}) = \mathbf{A}_d \mathcal{D}(\chi(t_k)) + \mathbf{B}_d \mathcal{D}(u(t_k)) + \mathbf{L}_d (\mathcal{D}(\mathbf{y}(t_k)) - \mathcal{D}(\mathbf{C} \mathcal{D}(\chi(t_k))))), \quad (14a)$$

$$u(t_k) = \mathbf{K} \mathcal{D}(\chi(t_k)). \quad (14b)$$

Here, we deploy a similar approach to that described in [27] to release the control input $u(t)$ from the encrypted controller (14) (see Fig. 2). The proposed controller (14) is performed

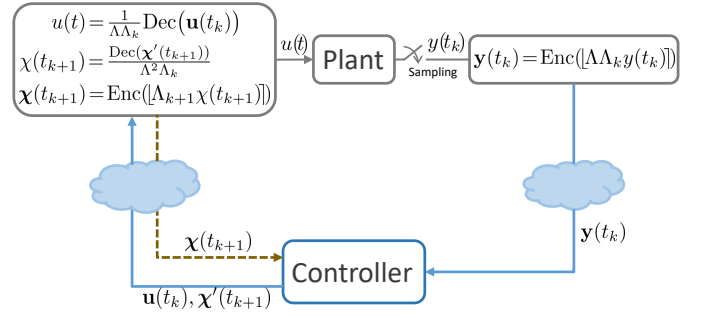


Fig. 2: Encrypted control system diagram

over encrypted data to release encrypted control input $u(t_k)$. Then, the control input $u(t)$ for the plant (7) can be obtained by the decryption $u(t) = \frac{1}{\Lambda \Lambda_k} \text{Dec}(\mathbf{u}(t_k))$, $\forall t \in [t_k, t_{k+1})$. In the update (14a), the encrypted value $\chi'(t_{k+1})$ is computed at time slot t_k ; however, it is not used to compute the encrypted control input (14b) at time t_{k+1} ($\chi'(t_{k+1}) \neq \chi(t_{k+1})$). Thus, besides sending $u(t_k)$, the controller also sends $\chi'(t_{k+1})$ to the plant at time slot t_k . Then, the encrypted value $\chi(t_{k+1})$ can be computed and sent to the controller by the plant as

$$\chi(t_{k+1}) = \frac{\text{Dec}(\chi'(t_{k+1}))}{\Lambda^2 \Lambda_k},$$

$$\chi(t_{k+1}) = \text{Enc}(\lfloor \Lambda_{k+1} \chi(t_{k+1}) \rfloor).$$

Consequently, the controller only holds the encrypted values of the system parameters and control signals; thus, the security of the control system is guaranteed.

B. Linear sampled-data system formulation

We note here that a quantization process for encryption is required; further, when applying to any value, the encryption-decryption procedure generates the same result as the quantization process. Therefore, in terms of stability analysis, the implementation of LWE-based encryption to the observer-based controller (14) is equivalent to the one obtained with only quantization as follows

$$\begin{cases} \chi_d(t_{k+1}) = \bar{A}_d \bar{\chi}_d(t_k) + \bar{B}_d u(t_k) \\ \quad + \bar{L}_d (\bar{y}(t_k) - \bar{C} \bar{\chi}_d(t_k)), \\ \bar{\chi}_d(t_k) = Q_{\Lambda_k}(\chi_d(t_k)), \\ u(t_k) = \bar{K} \bar{\chi}_d(t_k), \end{cases} \quad (15)$$

where $\bar{A}_d = Q_{\Lambda^2}(A_d)$, $\bar{B}_d = Q_{\Lambda}(B_d)$, $\bar{L}_d = Q_{\Lambda}(L_d)$, $\bar{K} = Q_{\Lambda}(K)$, $\bar{C} = Q_{\Lambda}(C)$, and $\bar{y}(t_k) = Q_{\Lambda \Lambda_k}(y(t_k))$.

It is stressed that (15) is in the discrete form. To analyze the stability of the encrypted observer-based control for the continuous-time system, consider the dynamics of $\chi_v(t)$ as

$$\begin{cases} \dot{\chi}_v(t) = A_v \chi_v(t) + B_v u(t_k) \\ \quad + L_v (\bar{y}(t_k) - \bar{C} \bar{\chi}_v(t_k)) + D \bar{\chi}_v(t_k), \\ \bar{\chi}_v(t_k) = Q_{\Lambda_k}(\chi_v(t_k)), \\ u(t_k) = \bar{K} \bar{\chi}_v(t_k), \quad \forall t \in [t_k, t_{k+1}), \end{cases} \quad (16)$$

where, $\bar{\chi}_v(t_k) = \bar{\chi}_v(t_k) - \chi_v(t_k)$, A_v, B_v, L_v are defined as $e^{A_v h} = \bar{A}_d$, $\int_0^h e^{A_v \tau} d\tau B_v = \bar{B}_d$, $\int_0^h e^{A_v \tau} d\tau L_v = \bar{L}_d$, and

$D = \left(\int_0^h e^{A_v \tau} d\tau \right)^{-1} \bar{A}_d$. To see the equivalence between (16) and (15) at each sampling instant, with $h = t_{k+1} - t_k$, we consider the solution of (16) in the interval $[t_k, t_{k+1}]$ as

$$\begin{aligned} \chi_v(t_{k+1}) &= \bar{A}_d \chi_v(t_k) + \bar{B}_d u(t_k) + \bar{L}_d (\bar{y}(t_k) - \bar{C} \bar{\chi}_v(t_k)) \\ &\quad + \left(\int_0^h e^{A_v \tau} d\tau \right) D \tilde{\chi}_v(t_k) \\ &= \bar{A}_d \bar{\chi}_v(t_k) + \bar{B}_d u(t_k) + \bar{L}_d (\bar{y}(t_k) - \bar{C} \bar{\chi}_v(t_k)), \end{aligned}$$

which is the same as the first equation of (15). As a result, $\chi_v(t_k) = \bar{\chi}_v(t_k)$ ($\forall t_k \in \mathcal{I}$) if they have the same initial conditions. The controller (16) is called the continuous-time virtual dynamics of (15) and is only utilized for stability analysis.

To obtain the linear sampled-data closed-loop system, let us rewrite the first equation of (16) as

$$\dot{\chi}_v(t) = A \chi_v(t) + B u(t_k) + L(y(t_k) - C \chi_v(t_k)) + \vartheta(t), \quad (17)$$

with $\vartheta(t) = \Delta A \chi_v(t) + \Delta B \bar{K} \bar{\chi}_v(t_k) + L \tilde{y}(t_k) + \Delta L \bar{y}(t_k) - LC \bar{\chi}_v(t_k) - L \tilde{C} \bar{\chi}_v(t_k) - \Delta L \tilde{C} \bar{\chi}_v(t_k) + D \tilde{\chi}_v(t_k)$, $\tilde{y}(t) = \bar{y}(t) - y(t)$, $\tilde{C} = \bar{C} - C$, $\Delta A = A_v - A$, $\Delta B = B_v - B$, $\Delta L = L_v - L$.

Defining $e(t) = x(t) - \chi_v(t)$, from (8) and (17), one gets

$$\dot{e}(t) = A e(t) - L C e(t_k) - \vartheta(t).$$

By letting $z(t) = [e^\top(t), \chi_v^\top(t)]^\top \in \mathbb{R}^{2n}$, the following closed-loop system is given in the same form of (9) as

$$\dot{z}(t) = (\mathcal{A} + \Delta \mathcal{A}) z(t) + (\mathcal{A}_c + \Delta \mathcal{A}_c) z(t_k) + \eta(t), \quad (18)$$

where

$$\begin{aligned} \mathcal{A} &= \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}, \mathcal{A}_c = \begin{bmatrix} -LC & 0 \\ LC & BK \end{bmatrix}, \Delta \mathcal{A} = \begin{bmatrix} 0 & -\Delta A \\ 0 & \Delta A \end{bmatrix}, \\ \Delta \mathcal{A}_c &= \begin{bmatrix} -\Delta LC & (L + \Delta L) \tilde{C} - \Delta B(K + \tilde{K}) \\ \Delta LC & \Delta B(K + \tilde{K}) + B \tilde{K} - (L + \Delta L) \tilde{C} \end{bmatrix}, \end{aligned}$$

and

$$\eta(t) = \begin{bmatrix} \mathcal{M}_{11} & \mathcal{M}_{12} \\ \mathcal{M}_{21} & \mathcal{M}_{22} \end{bmatrix} \begin{bmatrix} \tilde{\chi}_v(t_k) \\ \tilde{y}(t_k) \end{bmatrix} = \mathcal{M} \begin{bmatrix} \tilde{\chi}_v(t_k) \\ \tilde{y}(t_k) \end{bmatrix}, \quad (19)$$

$$\begin{aligned} \mathcal{M}_{11} &= -\Delta B(K + \tilde{K}) + (L + \Delta L)(C + \tilde{C}) - D, \\ \mathcal{M}_{21} &= (B + \Delta B)(K + \tilde{K}) - (L + \Delta L)(C + \tilde{C}) + D, \\ \mathcal{M}_{12} &= -(L + \Delta L), \mathcal{M}_{22} = L + \Delta L, \tilde{K} = \bar{K} - K. \end{aligned}$$

In the closed-loop system (18), $\Delta \mathcal{A}, \Delta \mathcal{A}_c$ are considered as the uncertainties, and $\eta(t)$ is considered as the disturbance of the system. Obviously, the uncertainties and disturbance are directly associated with the quantizers, and their bounds can be chosen arbitrarily small by selecting large enough quantization gains. Furthermore, the uncertainties $\Delta \mathcal{A}$ and $\Delta \mathcal{A}_c$ can be adjusted by choosing the appropriate static quantizers, while the disturbance $\eta(t)$ depends on the dynamic quantizer.

The following lemma provides a useful evaluation for bound of uncertainties in (18).

Lemma 3: Let $\tilde{A}_d = \bar{A}_d - A_d$, $\tilde{B}_d = \bar{B}_d - B_d$, $\tilde{L}_d = \bar{L}_d - L_d$, and assume that $\|\tilde{A}_d\| \leq \gamma_A$, $\|\tilde{B}_d\| \leq \gamma_B$, $\|\tilde{L}_d\| \leq \gamma_L$, and

small enough h such that $\|e^{-Ah}\|_{\gamma_A} < 1$. Then, the following inequalities hold

$$\|\Delta A\| \leq \frac{\|e^{-Ah}\|_{\gamma_A}}{h(1 - \|e^{-Ah}\|_{\gamma_A})} = \delta_A(h, \gamma_A), \quad (20a)$$

$$\|\Delta B\| \leq \frac{\alpha}{1 - \alpha\beta} (\gamma_B + \beta\|B\|) = \delta_B(h, \gamma_B, \gamma_A), \quad (20b)$$

$$\|\Delta L\| \leq \frac{\alpha}{1 - \alpha\beta} (\gamma_L + \beta\|L\|) = \delta_L(h, \gamma_L, \gamma_A), \quad (20c)$$

where $\alpha = \left\| \left(\int_0^h e^{A\tau} d\tau \right)^{-1} \right\| > 0$, $\beta = \frac{e^{\|A\|_h h^2 \delta_A}}{1 - \delta_A} > 0$.

Proof: See Appendix A.

Remark 1: This paper exploits a particular case of Lemma 3, where in accordance with the property (6), one has $\|\tilde{A}_d\| \leq \frac{n}{2\Lambda^2}$, $\|\tilde{B}_d\| \leq \frac{\sqrt{mn}}{2\Lambda}$, $\|\tilde{L}_d\| \leq \frac{\sqrt{nr}}{2\Lambda}$. Then, by choosing $\gamma_A = \frac{n}{2\Lambda^2}$, $\gamma_B = \frac{\sqrt{mn}}{2\Lambda}$, $\gamma_L = \frac{\sqrt{nr}}{2\Lambda}$, we can assess the bounds of $\|\Delta A\|$, $\|\Delta B\|$ and $\|\Delta L\|$ as functions of h and Λ , i.e., $\delta_A(h, \Lambda)$, $\delta_B(h, \Lambda)$ and $\delta_L(h, \Lambda)$.

IV. STABILITY ANALYSIS

This section provides the stability analysis of the sampled-data system (18). In the subsection IV-A, some results are presented for stability analysis of the system (9). The only difference between the systems (9) and (18) is the presence of the uncertainties in (18). In the subsection IV-B, the LMIs-based conditions are proposed to cope with the uncertainties, then the results in the subsection IV-A could be implemented.

A. Modified discontinuous Lyapunov functional for sampled-data systems

The following theorems provide sufficient conditions for the stability analysis of the sampled-data system (9).

Theorem 1: Let $V(z) : \mathbb{R}^n \rightarrow \mathbb{R}_+$ be a continuous differentiable function, and there exist $\mu_1, \mu_2 > 0$ such that $\mu_1 \|z\|^2 \leq V(z) \leq \mu_2 \|z\|^2$. Suppose that there exist differentiable functionals $\mathcal{U}(t, z)$, $\mathcal{W}(t, z)$ over $t \in \mathbb{R} \setminus \mathcal{I}$, and positive scalars μ_3, μ_4 such that

$$\mathcal{U}_{k+1}^- - \mathcal{W}_k^+ \geq 0, \quad (21)$$

$$\dot{\mathcal{F}}(t, z) \leq -\mu_3 \|z\|^2 + \mu_4 \|\eta\|^2, \quad (22)$$

where $\mathcal{F}(t, z) = V(z) + (t - t_k)\mathcal{U}(t, z) + (t_{k+1} - t)\mathcal{W}(t, z)$, $\mathcal{U}_k^- = \lim_{t \rightarrow t_k^-} \mathcal{U}(t, z(t))$ and $\mathcal{W}_k^+ = \lim_{t \rightarrow t_k^+} \mathcal{W}(t, z(t))$. Then, for the bounded energy disturbance $\eta(t) \left(\int_0^\infty \|\eta(t)\|^2 dt < \mathcal{E}_\eta \right)$, the system (9) satisfies IQC.

Proof: To begin with, let us take time derivative of $\mathcal{F}(t, z)$: $\dot{\mathcal{F}}(t, z) = \dot{V}(z) + \mathcal{U}(t, z) - \mathcal{W}(t, z) + (t - t_k)\dot{\mathcal{U}}(t, z) + (t_{k+1} - t)\dot{\mathcal{W}}(t, z)$. For simple notations, let $V_k = V(t_k, z(t_k))$. By integrating from t_k to t_{k+1} both sides of (22) along the solution of (9), it yields

$$\begin{aligned} \int_{t_k}^{t_{k+1}} \dot{\mathcal{F}}(t, z) dt &= \lim_{t \rightarrow t_{k+1}^-} \mathcal{F}(t, z(t)) - \lim_{t \rightarrow t_k^+} \mathcal{F}(t, z(t)) \\ &= V_{k+1} - V_k + h(\mathcal{U}_{k+1}^- - \mathcal{W}_k^+) \\ &\leq -\mu_3 \int_{t_k}^{t_{k+1}} \|z(\tau)\|^2 d\tau + \mu_4 \int_{t_k}^{t_{k+1}} \|\eta(\tau)\|^2 d\tau. \end{aligned}$$

According to (21), we further obtain

$$V_{k+1} - V_k + \mu_3 \int_{t_k}^{t_{k+1}} \|z(\tau)\|^2 d\tau \leq \mu_4 \int_{t_k}^{t_{k+1}} \|\eta(\tau)\|^2 d\tau. \quad (23)$$

Summing up (23) from 0 to $k+1$, we have $\int_0^{t_{k+1}} \|z(\tau)\|^2 d\tau \leq \mu_3^{-1} (V_0 + \mu_4 \mathcal{E}_\eta)$. As a result, the system (9) satisfies the IQC defined in Definition 1. ■

In Theorem 1, the disturbance $\eta(t)$ satisfies the bounded energy condition; it also means that $\eta(t) \rightarrow 0$ as $t \rightarrow \infty$. However, in some situations, the disturbance always exists and does not vanish. The following theorem considers the case that the disturbance $\eta(t)$ is only bounded, i.e., $\|\eta(t)\| \leq \bar{\eta}$, $\forall t \geq 0$ for some $\bar{\eta} > 0$.

Theorem 2: Suppose that the conditions (21) and (22) are satisfied, and the disturbance $\eta(t)$ is bounded by $\bar{\eta} > 0$ as $\|\eta(t)\| \leq \bar{\eta}$, $\forall t \geq 0$. Then, if $z(t_k) \notin \Omega_\rho$ where

$$\Omega_\rho = \{z \in \mathbb{R}^n : V(z) \leq \bar{V}_\rho\}, \quad \bar{V}_\rho = \max_{z \in \mathcal{B}_\rho} V(z), \quad (24)$$

$$\mathcal{B}_\rho = \left\{z \in \mathbb{R}^n : \|z\|^2 \leq \rho = \frac{\mu_4 \bar{\eta}^2 + \sigma}{\mu_3}, 0 < \sigma\right\}, \quad (25)$$

the solution of (9) in $[t_k, t_{k+q}]$ enters Ω_ρ at least once when $t_{k+q} \geq \frac{V_k - \bar{V}_\rho}{\sigma} + t_k$.

Proof: For $z_k \notin \Omega_\rho$, let $q \in \mathbb{N}$ such that $z(t) \notin \Omega_\rho$ for all $t \in \mathcal{T}_{k,q} \triangleq [t_k, t_{k+q}]$. Accordingly, $V(z(t)) \geq \bar{V}_\rho = \max_{z \in \mathcal{B}_\rho} V(z)$, and then $z(t) \notin \mathcal{B}_\rho$ for all $t \in \mathcal{T}_{k,q}$. As a result, $\mu_3 \|z(t)\|^2 - \mu_4 \bar{\eta}^2 > \sigma$. From (23), we have that $V_{k+1} - V_k \leq (t_k - t_{k+1})\sigma$. The summation of the inequality from t_k to t_{k+q} results in $V_{k+q} - V_k = \sum_{i=0}^{q-1} (V_{k+i+1} - V_{k+i}) < (t_k - t_{k+q})\sigma$. Thus, since $V_{k+q} > \bar{V}_\rho$ with $t \in \mathcal{T}_{k,q}$, we have that $V_k - \bar{V}_\rho > V_k - V_{k+q} > (t_{k+q} - t_k)\sigma$, that is, $t_{k+q} - t_k < \frac{V_k - \bar{V}_\rho}{\sigma}$. Therefore, for $z_k \notin \Omega_\rho$ and $t_{k+q} \geq t_k + \frac{V_k - \bar{V}_\rho}{\mu_3 \sigma}$, $\exists t \in [t_k, t_{k+q}]$ such that $z(t) \in \Omega_\rho$. ■

B. Stability analysis of the closed-loop system

This subsection provides sufficient conditions for the stability of the system (18). For convenience, let us denote

$$\begin{aligned} \xi(t) &= [z^\top(t) \quad z^\top(t_k) \quad \phi_k^\top(t)]^\top \in \mathbb{R}^{6n}, \\ \phi_k(t) &= \frac{1}{t - t_k} \int_{t_k}^t z(\tau) d\tau \in \mathbb{R}^{2n}, \Phi_0 = [\mathcal{A}, \mathcal{A}_c, 0] \in \mathbb{R}^{2n \times 6n}, \\ E_1 &= [I \ 0 \ 0], E_2 = [0 \ I \ 0], E_3 = [0 \ 0 \ I] \in \mathbb{R}^{2n \times 6n}, \\ \Phi_1 &= E_1 - E_2, \Phi_2 = E_1 + E_2 - 2E_3, \\ \Phi_3 &= [0 \ \mathcal{A}_c \ \mathcal{A}] \in \mathbb{R}^{2n \times 6n}, \Phi_4 = [E_1^\top \ E_2^\top]^\top, \\ \Phi_5 &= [\Phi_0^\top \ 0]^\top \in \mathbb{R}^{4n \times 6n}, \Phi_6 = [I \ 0]^\top \in \mathbb{R}^{4n \times 2n}, \\ \Delta_0 &= [\Delta \mathcal{A} \ \Delta \mathcal{A}_c \ 0], \Delta_2 = [\Delta_5^\top \ \Delta_0^\top \ \Delta_3^\top]^\top, \\ \Delta_3 &= [0, \Delta \mathcal{A}_c, \Delta \mathcal{A}] \in \mathbb{R}^{2n \times 6n}, \Delta_5 = [\Delta_0^\top \ 0]^\top \in \mathbb{R}^{4n \times 6n}. \end{aligned}$$

Considering the uncertainty terms in (18), it follows that

$$\|\Delta \mathcal{A}\| = \sqrt{2} \|\Delta \mathcal{A}\| \leq \sqrt{2} \delta_A(h, \Lambda), \quad (26)$$

$$\begin{aligned} \|\Delta \mathcal{A}_c\| &\leq 2\|\Delta L\| \|C\| + (\|L\| + \|\Delta L\|) \|\tilde{C}\| \\ &\quad + 2\|\Delta B\| (\|K\| + \|\tilde{K}\|) + \|B\| \|\tilde{K}\| \\ &\quad + \|\tilde{C}\| (\|L\| + \|\Delta L\|) \\ &\leq 2 \left(\|C\| + \frac{\sqrt{nr}}{2\Lambda} \right) \delta_L(h, \Lambda) \\ &\quad + \frac{\sqrt{nr} \|L\|}{2\Lambda} + 2 \left(\|K\| + \frac{\sqrt{mn}}{2\Lambda} \right) \delta_B(h, \Lambda) \\ &\quad + \frac{\sqrt{mn} \|B\|}{2\Lambda} = \varphi(h, \Lambda). \end{aligned} \quad (27)$$

Let a positive value \mathcal{M}_U be an upper bound of $\|\mathcal{M}\|$; then, from (19), we have

$$\begin{aligned} \|\eta(t)\| &\leq \mathcal{M}_U (\|\tilde{x}_v(t_k)\| + \|\tilde{y}(t_k)\|) \\ &\leq \mathcal{M}_U \left(\frac{\sqrt{n}}{2} + \frac{\sqrt{r}}{2\Lambda} \right) \frac{1}{\Lambda_k}. \end{aligned} \quad (28)$$

Thus,

$$\begin{aligned} \int_0^\infty \|\eta(t)\|^2 dt &\leq \int_0^\infty \mathcal{M}_U^2 \left(\frac{\sqrt{n}}{2} + \frac{\sqrt{r}}{2\Lambda} \right)^2 \frac{1}{\Lambda_k^2} dt \\ &= h \mathcal{M}_U^2 \left(\frac{\sqrt{n}}{2} + \frac{\sqrt{r}}{2\Lambda} \right)^2 \sum_{k=0}^\infty \frac{1}{\Lambda_k^2}. \end{aligned} \quad (29)$$

The following theorem provides sufficient conditions for the stability of the system (18) based on LMIs.

Theorem 3: Assume that there exist $h, \varepsilon_1, \varepsilon_2, \epsilon_1, \epsilon_2 \in \mathbb{R}_{++}$, matrices $U_1 \in \mathbb{S}^{4n \times 4n}$; $F, W_1, H, U_4 \in \mathbb{S}^{2n \times 2n}$; $P, R \in \mathbb{S}_{++}^{2n \times 2n}$; $U_2, U_3, W_2 \in \mathbb{R}^{2n \times 2n}$, $\Psi \in \mathbb{S}_{++}^{6n \times 6n}$, and $Q, N_1, N_2 \in \mathbb{R}^{2n \times 6n}$ such that

$$0 \preceq \mathbf{U} - E_2^\top H E_2, \quad (30)$$

$$0 \succeq \begin{bmatrix} \Xi_0 + h \Xi_1 + \varepsilon_1 I & Y_{01} \\ Y_{01}^\top & -\epsilon_1 I \end{bmatrix}, \quad (31)$$

$$0 \succeq hR - \epsilon_1 I, \quad (32)$$

$$0 \succeq \begin{bmatrix} \Xi_0 + h \Xi_2 + \varepsilon_2 I & (*) & (*) & (*) \\ hN_1 & -hR & (*) & (*) \\ hN_2 & 0 & -3hR & (*) \\ Y_{02}^\top & 0 & 0 & -\epsilon_2 I \end{bmatrix}, \quad (33)$$

where

$$\mathbf{U} = \begin{bmatrix} U_1 & (*) \\ [U_2 \ U_3] & U_4 \end{bmatrix},$$

$$\begin{aligned} \Xi_0 &= \mathbf{He} \left\{ E_1^\top P \Phi_0 \right\} + U - \Phi_1^\top W_1 \Phi_1 - \mathbf{He} \left\{ \Phi_1^\top W_2 E_2 \right\} \\ &\quad - E_1^\top H E_1 + \mathbf{He} \left\{ -\Phi_1^\top N_1 - \Phi_2^\top N_2 + (E_1 - E_3)^\top \right. \\ &\quad \times (U_2 E_1 + U_3 E_2 + U_4 E_3) + \Phi_1^\top Q \left. \right\} + \Psi, \\ \Xi_1 &= \mathbf{He} \left\{ \Phi_0^\top (W_1 (E_1 - E_2) + W_2 E_2 + H E_1) \right\} \\ &\quad + E_2^\top F E_2 + \Phi_0^\top R \Phi_0, \\ \Xi_2 &= -E_2^\top F E_2 + \mathbf{He} \left\{ \Phi_4^\top U_1 \Phi_5 + E_3^\top U_2 \Phi_0 - \Phi_3^\top Q \right\}, \\ Y_0 &= E_1^\top P, \quad Y_1 = (E_1 - E_2)^\top W_1 + \Phi_0^\top R, \quad Y_{01} = Y_0 + h Y_1, \\ Y_2 &= [\Phi_4^\top U_1 \quad E_3^\top U_2 \quad -Q^\top], \quad Y_{02} = [Y_0 \quad h Y_2]; \end{aligned}$$

and the value Λ is chosen such that

$$2\delta_A^2(h, \Lambda) + \varphi^2(h, \Lambda) \leq \min \left\{ \frac{\varepsilon_1}{2\epsilon_1}, \frac{\varepsilon_2}{6\epsilon_2} \right\}. \quad (34)$$

1) If the value Λ_k is chosen such that

$$\sum_{k=0}^{\infty} \frac{1}{\Lambda_k^2} < \infty, \quad (35)$$

then, the system (18) is globally asymptotically stable.

2) If Λ_k is a fixed value, there exist $\mu_3, \mu_4, \sigma > 0$, $q \in \mathbb{N}$ such that any solution of (18) in $[t_k, t_{k+q})$ enters Ω_ρ at least once where Ω_ρ is defined in (24) and (25), and $\bar{\eta}$ is obtained from (28).

Proof: See Appendix B.

Remark 2: By preselecting the sampling interval h , the conditions (30) - (33) can be considered as the LMIs. Thus, Theorem 3 provides a stability criterion for the selection of sampling interval h . Moreover, through the inequality (34), Theorem 3 exposes a relationship between h and Λ to ensure the stability of the encrypted control system. By checking the feasibility of the LMIs in (30)-(33), we can obtain the range for h such that there exists at least one quantization scheme such that the system (18) is stable.

V. EVALUATION

This section considers the angular control problem for DC motor with the dynamics described as (see [35])

$$\frac{di_a(t)}{dt} = -\frac{R_a}{L_a}i_a(t) - \frac{k_d}{L_a}\omega(t) + \frac{1}{L_a}v_s(t), \quad (36a)$$

$$\frac{d\omega(t)}{dt} = \frac{k_d}{J_M}i_a(t) - \frac{B_M}{J_M}\omega(t), \quad (36b)$$

$$\frac{d\theta(t)}{dt} = \omega(t), \quad (36c)$$

where i_a, v_s, θ and ω represent the armature current, armature voltage, angular position, and angular velocity of the rotor, respectively. The system's parameters include the armature resistance $R_a = 7.2[\Omega]$, the armature inductance $L_a = 0.0917[H]$, the frictional constant $B_M = 0.0004[N.m.s/rad]$, the torque constant $k_d = 0.1236[N.m/Wb.A]$, and the moment of inertia $J = 0.0007046[kg.m^2]$.

Our target is to derive the DC motor to a reference angle, i.e., $\theta(t) \rightarrow \theta_r$, where θ_r is the desired angle and is assumed to be a constant. Define the angular position error as $\theta_e(t) = \theta(t) - \theta_r$, the equation (36c) can be rewritten as $\dot{\theta}_e(t) = \omega(t)$. Denoting the state variable $x(t) = [i_a(t) \ \omega(t) \ \theta_e(t)]^\top$ and the output $y(t) = \theta_e(t)$, the system dynamic (36) can be rewritten in the state space form as

$$\dot{x}(t) = Ax(t) + Bu(t), \quad (37a)$$

$$y(t) = Cx(t), \quad (37b)$$

where

$$A = \begin{bmatrix} -\frac{R_a}{L_a} & -\frac{k_d}{L_a} & 0 \\ \frac{k_d}{J_M} & -\frac{B_M}{J_M} & 0 \\ 0 & 1 & 0 \end{bmatrix}, B = \begin{bmatrix} \frac{1}{L_a} \\ 0 \\ 0 \end{bmatrix}, C = [0 \ 0 \ 1].$$

By pole-placement method [36], let us choose $K = [1.65, -6.26, -43.08]$, and $L = [69.11, 71.91, 24.13]^\top$.

TABLE I: Minimal values of Λ provided by (34) corresponding to several choices of sampling interval h .

h	0.083	0.07	0.05	0.03	0.01
Λ	1.92×10^5	2.15×10^4	9.88×10^3	6.01×10^3	4.16×10^3

TABLE II: MRMS values corresponding to several choices of varying values of Λ_k at $t = 53[s]$ with the window length $T_{RMS} = 50[s]$.

Λ_k	$k^{0.4}$	k^1	$k^{1.5}$	k^2	k^3
MRMS	4.2×10^{-2}	1.7×10^{-3}	1.5×10^{-4}	3.2×10^{-5}	2.5×10^{-7}

With such setups, Theorem 3 can provide feasible solutions with maximal sampling interval \bar{h} up to 0.083. In addition, the minimal values for Λ corresponding to several sampling intervals are given in Table I. It can be seen from Table I that the larger the sampling period is, the larger value of Λ is needed. That is, the quantization is required to be more accurate when the sampling interval becomes larger.

For more detail, let us consider three cases $h = 0.03, h = 0.05$, and $h = 0.07$. The corresponding values for Λ are chosen according to Table I as $\Lambda = 6.01 \times 10^3, \Lambda = 9.88 \times 10^3$ and $\Lambda = 2.15 \times 10^4$; and the value Λ_k for the dynamic quantizer is chosen as $\Lambda_k = k^2$. The results in Fig. 3 figure out that choosing a smaller sampling period h gives better results in terms of both control input and output. To be specific, the increment of h leads to fluctuation in the angular position error and also increases the convergence time. Further, a larger value of h needs a larger maximal value of the control input that could exceed the physical limitations of the control system.

Apart from this, Fig. 4 presents the time evolution of the angular position errors with different Λ_k . The sampling period is chosen as $h = 0.05$ with $\Lambda = 9.88 \times 10^3$. We choose $\Lambda_k = k^p$ with $p > 0$; it is obvious that, if $p > 0.5$, then the condition (35) can be ensured. Fig. 4 confirms that larger p results in better convergence of the angular position error. Specifically, with $p = 0.4$, which does not satisfy the condition (35), asymptotic convergence cannot be achieved (see Fig. 4a) while, with $p = 2$ which satisfy (35), asymptotic convergence can be guaranteed as in Fig. 4b. In Fig. 5, we use the same setup as in the case of Fig. 4, but Λ_k is fixed to 10 and 30. As we can see, Fig. 5b with a larger value of Λ_k ($\Lambda_k = 30$) shows better results compared to Fig. 5a with a smaller Λ_k ($\Lambda_k = 10$).

To see the asymptotic stability property of the system in accordance with Λ_k , let us introduce the moving root mean square (MRMS) [37], which is computed by the mean square of a signal over a given window length. For a function $\theta_e(t)$, the MRMS with window length $T_{RMS} > 0$ at time $t > T_{RMS}$

TABLE III: MRMS values corresponding to several choices of fixed values of Λ_k at $t = 53[s]$ with the window length $T_{RMS} = 50[s]$.

Λ_k	10	30	50	70	100
MRMS	4.8×10^{-2}	1.5×10^{-2}	9.7×10^{-3}	6.2×10^{-3}	4.2×10^{-3}

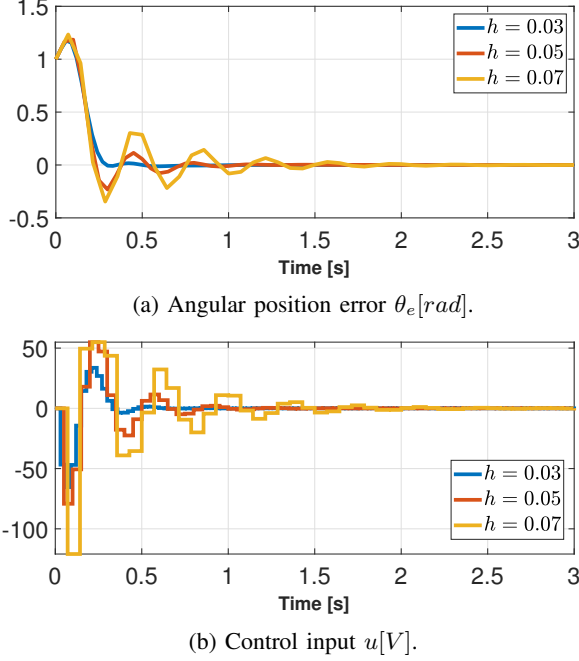


Fig. 3: The angular position error and control input of the system in three cases $h = 0.03, 0.05, 0.07$ in accordance with Λ shown in Table I, and $\Lambda_k = k^2$.

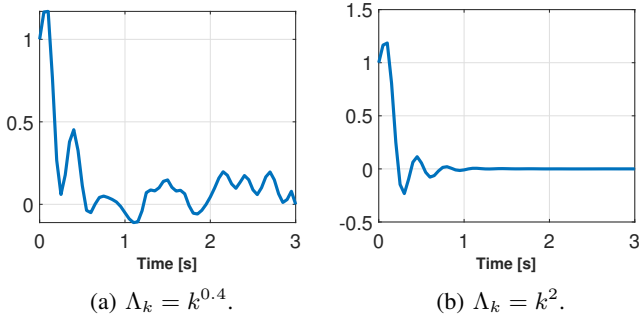


Fig. 4: The angular position error θ_e [rad] with different time-varying Λ_k , $h = 0.05$, and $\Lambda = 9.88 \times 10^3$.

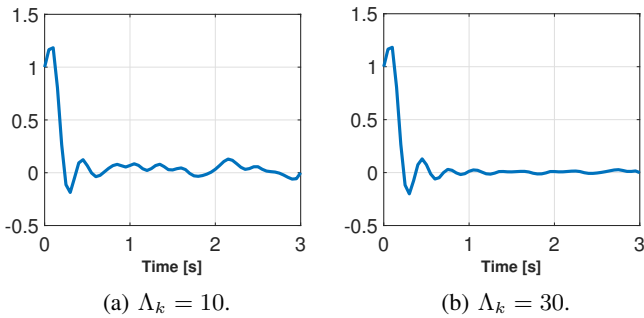


Fig. 5: The angular position error θ_e [rad] with fixed values of Λ_k , $h = 0.05$, and $\Lambda = 9.88 \times 10^3$.

can be computed as

$$\text{MRMS} = \sqrt{\frac{1}{T_{\text{RMS}}} \int_{t-T_{\text{RMS}}}^t \theta_e^2(\tau) d\tau}. \quad (38)$$

The MRMS computed in (38) is used to measure the difference between $\theta_e(t)$ and 0 during $[t - T_{\text{RMS}}, t)$. Let us consider the MRMS of $\theta_e(t)$ at $t = 53[s]$ with the window length $T_{\text{RMS}} = 50[s]$. Table II shows the MRMS values according to $\Lambda_k = k^p$, with $p \in \{0.4, 1.0, 1.5, 2.0, 2.5\}$. It can be seen that, with a larger p which leads to larger values and a higher divergence speed of $\{\Lambda_k\}$, the MRMS is smaller. Accordingly, with a larger p , the angular position error $\theta_e(t)$ is closer to the horizontal axis which results in better convergence of the angular position error. Similarly, with fixed values of Λ_k , Table III shows that the larger Λ_k is, the smaller MRMS can be computed; that is, a larger value of Λ_k results in better convergence of the angular position error.

VI. CONCLUSIONS

This paper provided the stability analysis of continuous LTI systems with an encrypted observer-based controller. Due to encryption, computations for the observer-based controller were conducted based on its discrete-time model. Thus, the continuous-time virtual dynamics of the controller was also introduced for the stability analysis. Due to the fact that the encryption-decryption process does not affect the stability of the system, we formulated the sampled-data closed-loop system with the presence of the uncertainties and disturbance associated with the static quantizers and the dynamic quantizer, respectively. Based on the discontinuous Lyapunov functional, we theoretically proved that, with suitable selections of the quantization gains and sampling interval, the system is globally asymptotically stable. For future works, we will consider the same design for the aperiodic sampled-data system and provide more stability analysis in the case with only static quantizers.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2022R1A2B5B03001459).

APPENDIX

A. Proof of Lemma 3

First, \tilde{A}_d could be written as $\tilde{A}_d = e^{A_v h} - e^{A h} = e^{A h} (e^{(A_v - A) h} - I)$; thus, $e^{\Delta A h} - I = e^{-A h} \tilde{A}_d$. One can obtain the error ΔA as: $\Delta A = \frac{1}{h} \ln(e^{-A h} \tilde{A}_d + I)$ with matrix logarithm defined in [38]. Note that, for any matrix M with $\|M - I\| < 1$, we always have

$$\ln M = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(M - I)^k}{k}.$$

Then, with γ_A and h chosen such that $\|e^{-Ah}\|_{\gamma_A} < 1$, we have

$$\begin{aligned}\|\Delta A\| &= \frac{1}{h} \left\| \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(e^{-Ah} \tilde{A}_d)^k}{k} \right\| \leq \frac{1}{h} \sum_{k=1}^{\infty} (\|e^{-Ah}\|_{\gamma_A})^k \\ &= \frac{\|e^{-Ah}\|_{\gamma_A}}{h(1 - \|e^{-Ah}\|_{\gamma_A})} = \delta_A(h, \gamma_A).\end{aligned}$$

Next, we prove that $\|\Delta B\|, \|\Delta L\|$ are bounded by δ_B, δ_L . First, we have

$$\begin{aligned}\tilde{B}_d &= \bar{B}_d - B_d = \int_0^h e^{A_v \tau} d\tau B_v - \int_0^h e^{A\tau} d\tau B \\ &= \int_0^h (e^{A_v \tau} - e^{A\tau}) d\tau B_v + \int_0^h e^{A\tau} d\tau \Delta B.\end{aligned}$$

It can be seen that $\int_0^h e^{A\tau} d\tau$ is nonsingular, one gets

$$\Delta B = \left(\int_0^h e^{A\tau} d\tau \right)^{-1} \left(\tilde{B}_d - \int_0^h (e^{A_v \tau} - e^{A\tau}) d\tau B_v \right).$$

Therefore,

$$\begin{aligned}\|\Delta B\| &\leq \alpha \left(\|\tilde{B}_d\| + \left\| \int_0^h (e^{A_v \tau} - e^{A\tau}) d\tau \right\| \|B_v\| \right) \\ &\leq \alpha \left(\|\tilde{B}_d\| + \int_0^h \|e^{A_v \tau} - e^{A\tau}\| d\tau (\|B\| + \|\Delta B\|) \right).\end{aligned}\quad (39)$$

Further, for all $\tau \in [0, h]$, we have

$$\begin{aligned}\|e^{A_v \tau} - e^{A\tau}\| &= \|e^{A\tau} (e^{\Delta A \tau} - I)\| \leq \|e^{A\tau}\| \|e^{\Delta A \tau} - I\| \\ &\leq e^{\|A\|\tau} \left\| \sum_{k=1}^{\infty} \frac{(\Delta A \tau)^k}{k} \right\| \leq e^{\|A\|h} \sum_{k=1}^{\infty} (\|\Delta A\|h)^k \\ &= e^{\|A\|h} \frac{\delta_A h}{1 - \delta_A}.\end{aligned}$$

Substituting the above result into (39) gives

$$\|\Delta B\| \leq \frac{\alpha}{1 - \alpha\beta} (\gamma_B + \beta\|B\|) = \delta_B(h, \gamma_B, \gamma_A).$$

By a similar way, we also have $\|\Delta L\| \leq \delta_L(h, \gamma_L, \gamma_A)$, which completes the proof. ■

B. Proof of Theorem 3

Based on Theorem 1, select the following functions

$$V(z) = z^\top(t) P z(t), \quad (40a)$$

$$\begin{aligned}\mathcal{U}(t, z) &= \zeta^\top(t) U_1 \zeta(t) + 2\phi_k^\top(t) (U_2 z(t) + U_3 z(t_k)) \\ &\quad + \phi_k^\top(t) U_4 \phi_k(t),\end{aligned}\quad (40b)$$

$$\begin{aligned}\mathcal{W}(t, z) &= (t - t_k) z^\top(t_k) F z(t_k) + z^\top(t) H z(t) \\ &\quad + (z(t) - z(t_k))^\top (W_1(z(t) - z(t_k)) + 2W_2 z(t_k)) \\ &\quad + \int_{t_k}^t \dot{z}^\top(\tau) R \dot{z}(\tau) d\tau,\end{aligned}\quad (40c)$$

where $\zeta(t) = [z^\top(t) \ z^\top(t_k)]^\top$. It is obvious that the condition (21) is satisfied under the condition (30). Taking the time derivatives of (40a), (40b) and (40c) gives

$$\begin{aligned}\dot{V} &= \xi^\top(t) \mathbf{He} \left\{ E_1^\top P (\Phi_0 + \Delta_0) \right\} \xi(t) \\ &\quad + 2\eta^\top(t) P E_1 \xi(t),\end{aligned}\quad (41a)$$

$$\begin{aligned}\dot{\mathcal{U}} &= \xi^\top(t) \mathbf{He} \left\{ \Phi_4^\top U_1 (\Phi_5 + \Delta_5) + E_3^\top U_2 (\Phi_0 + \Delta_0) \right. \\ &\quad \left. + \frac{1}{t - t_k} (E_1 - E_3)^\top (U_2 E_1 + U_3 E_2 + U_4 E_3) \right\} \xi(t) \\ &\quad + 2\eta^\top(t) (\Phi_6^\top U_1 \Phi_4 + U_2 E_3) \xi(t),\end{aligned}\quad (41b)$$

$$\begin{aligned}\dot{\mathcal{W}} &= \xi^\top(t) \left(E_2^\top F E_2 + (\Phi_0 + \Delta_0)^\top R (\Phi_0 + \Delta_0) \right. \\ &\quad \left. + \mathbf{He} \left\{ (\Phi_0 + \Delta_0)^\top (W_1(E_1 - E_2) + W_2 E_2 + F E_1) \right\} \right) \xi(t) \\ &\quad + 2\eta^\top(t) \left(H E_1 + W_1(E_1 - E_2) + W_2 E_2 + R (\Phi_0 + \Delta_0) \right) \xi(t) \\ &\quad + \eta^\top(t) R \eta(t).\end{aligned}\quad (41c)$$

Additionally, integrating both sides of (18) gives

$$z(t) - z(t_k) = (t - t_k) \left((\mathcal{A} + \Delta \mathcal{A}) \phi_k(t) + (\mathcal{A}_c + \Delta \mathcal{A}_c) z(t_k) \right).$$

Further, by multiplying both sides of the above equation with $Q\xi(t)$, we obtain

$$\xi^\top(t) \mathbf{He} \left\{ \Phi_1^\top Q - (t - t_k) (\Phi_3 + \Delta_3)^\top Q \right\} \xi(t) = 0. \quad (42)$$

Therefore, from (41), (42) and with the help of Lemma 2, we have

$$\begin{aligned}\dot{V}(z) + \mathcal{U}(t, z) - \mathcal{W}(t, z) &+ (t - t_k) \dot{\mathcal{U}}(t, z) + (t_{k+1} - t) \dot{\mathcal{W}}(t, z) \\ &\leq \xi^\top(t) \left(\Xi_0 + \mathbf{He} \{ Y_0 \Delta_0 \} + (t_{k+1} - t) (\Xi_1 + \mathbf{He} \{ Y_1 \Delta_0 \} \right. \\ &\quad \left. + \Delta_0^\top R \Delta_0) + (t - t_k) (\Xi'_2 + \mathbf{He} \{ Y_2 \Delta_2 \}) - \Psi \right) \xi(t) \\ &\quad + \eta^\top(t) \Upsilon(t) \xi(t) + \eta^\top(t) R \eta(t),\end{aligned}\quad (43)$$

where $\Xi'_2 = \Xi_2 + N_1^\top R^{-1} N_1 + \frac{1}{3} N_2^\top R^{-1} N_2$.

In addition, according to (26) and (27), one has $\|\Delta_0\|^2 = \|\Delta \mathcal{A}\|^2 + \|\Delta \mathcal{A}_c\|^2 \leq 2\delta_A^2(h, \Lambda) + \varphi^2(h, \Lambda)$; and $\|\Delta_2\|^2 = \|\Delta_5\|^2 + \|\Delta_0\|^2 + \|\Delta_3\|^2 = 3\|\Delta_0\|^2 \leq 3(2\delta_A^2(h, \Lambda) + \varphi^2(h, \Lambda))$. Thus, based on (34) and Lemma 1 with $\Gamma = \Xi_0 + h\Xi_1$, $\Pi_1 = I$, $\Delta = \Delta_0$, $\Pi_2 = Y_{01}^\top$, $\kappa = \frac{\varepsilon_1}{2}$, and $\Omega = hR$, the conditions (31) and (32) give

$$\Xi_0 + \mathbf{He} \{ Y_0 \Delta_0 \} + h(\Xi_1 + \mathbf{He} \{ Y_1 \Delta_0 \} + \Delta_0^\top R \Delta_0) \preceq 0. \quad (44)$$

Similarly, by using Lemma 1 with $\Pi_1 = I$, $\Pi_2 = Y_{02}^\top$, $\Delta = \Delta_2$, $\kappa = \frac{\varepsilon_2}{2}$, and $\Omega = \mathbf{0}$, and with the help of the Schur's complement, the condition (33) yields

$$\Xi_0 + \mathbf{He} \{ Y_0 \Delta_0 \} + h(\Xi'_2 + \mathbf{He} \{ Y_2 \Delta_2 \}) \preceq 0. \quad (45)$$

Thus, from (43)-(45), we obtain

$$\begin{aligned}\dot{V} + \mathcal{U} - \mathcal{W} &+ (t - t_k) \dot{\mathcal{U}} + (t_{k+1} - t) \dot{\mathcal{W}} \\ &\leq -\xi^\top(t) \Psi \xi(t) + \eta^\top(t) \Upsilon(t) \xi(t) + \eta^\top(t) R \eta(t) \\ &\leq -\lambda_{\min}(\Psi) \|\xi(t)\|^2 + \varsigma \|\eta(t)\| \|\xi(t)\| + \lambda_{\max}(R) \|\eta(t)\|^2 \\ &\leq -\left(\lambda_{\min}(\Psi) - \frac{\varsigma s^2}{2} \right) \|\xi(t)\|^2 + \left(\lambda_{\max}(R) + \frac{\varsigma}{2s^2} \right) \|\eta(t)\|^2 \\ &\leq -\left(\lambda_{\min}(\Psi) - \frac{\varsigma s^2}{2} \right) \|z(t)\|^2 + \left(\lambda_{\max}(R) + \frac{\varsigma}{2s^2} \right) \|\eta(t)\|^2,\end{aligned}$$

where $0 < s < \sqrt{\frac{2\lambda_{\min}(\Psi)}{\varsigma}}$ is a small positive scalar, and $\varsigma > 0$ is an upper bound of $\|\Upsilon(t)\|$ with

$$\Upsilon(t) = 2PE_1 + 2(t - t_k)(\Phi_6^\top U_1 \Phi_4 + U_2 E_3) + 2(t_{k+1} - t) \times (HE_1 + W_1(E_1 - E_2) + W_2 E_2 + R(\Phi_0 + \Delta_0)).$$

Further, the conditions (29) and (35) guarantee the bounded energy disturbance condition. Therefore, according to Theorem 1, the system (18) is IQC, then the first statement of Theorem 3 is proven. In addition, based on Theorem 2 with $\mu_3 = \lambda_{\min}(\Psi) - \frac{\varsigma s^2}{2}$, and $\mu_4 = \lambda_{\max}(R) + \frac{\varsigma}{2s^2}$, the second statement of Theorem 3 is proven. ■

REFERENCES

- [1] C. Zijian, L. Jin, W. Can, S. Yonghua, Z. Yi, and W. Xiaohui, "Optimal cloud computing resource allocation for demand side management in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1943–1955, 2017.
- [2] M. Shengdong, X. Zhengxian, and T. Yixiang, "Intelligent traffic control system based on cloud computing and big data mining," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6583–6592, 2019.
- [3] X. Yin, Z. Gao, D. Yue, and S. Hu, "Cloud-based event-triggered predictive control for heterogeneous nmass under both dos attacks and transmission delays," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022.
- [4] L. Wang, M. Liu, and M. Q.-H. Meng, "A hierarchical auction-based mechanism for real-time resource allocation in cloud robotic systems," *IEEE Transactions on Cybernetics*, vol. 47, no. 2, pp. 473–484, 2016.
- [5] M. Jiang, T. Wu, Z. Wang, Y. Gong, L. Zhang, and R. P. Liu, "A multi-intersection vehicular cooperative control based on end-edge-cloud computing," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 3, pp. 2459–2471, 2022.
- [6] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multi-agent systems against malicious attacks: A brief survey," *IEEE Transactions on Industrial Informatics*, 2021.
- [7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.
- [8] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 11, pp. 3254–3264, 2018.
- [9] Y. Yang, Y. Li, D. Yue, Y.-C. Tian, and X. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under dos attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 6, pp. 2916–2928, 2020.
- [10] Y. Liu, "Secure control of networked switched systems with random dos attacks via event-triggered approach," *International Journal of Control, Automation and Systems*, vol. 18, no. 10, pp. 2572–2579, 2020.
- [11] J.-W. Zhu, C.-Y. Liang, D.-F. He, and X. Wang, "A novel intermediate estimator based secure consensus control for multi-agent systems with application to networked multi-axis motion synchronization," *International Journal of Control, Automation and Systems*, vol. 19, no. 4, pp. 1470–1479, 2021.
- [12] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Systems Magazine*, vol. 41, no. 3, pp. 58–78, 2021.
- [13] K. Teranishi, N. Shimada, and K. Kogiso, "Stability analysis and dynamic quantizer for controller encryption," in *2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 7184–7189.
- [14] C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semihomomorphic encryption," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3950–3957, 2020.
- [15] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 6836–6843.
- [16] T. Fujita, K. Kogiso, K. Sawada, and S. Shin, "Security enhancements of networked control systems using rsa public-key cryptosystem," in *2015 10th Asian Control Conference (ASCC)*. IEEE, 2015, pp. 1–6.
- [17] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.
- [18] M. Schulze Darup, "Encrypted model predictive control in the cloud," in *Privacy in Dynamical Systems*. Springer, 2020, pp. 231–265.
- [19] M. S. Darup, A. Redder, I. Shames, F. Farokhi, and D. Quevedo, "Towards encrypted mpc for linear constrained systems," *IEEE Control Systems Letters*, vol. 2, no. 2, pp. 195–200, 2017.
- [20] F. J. Gonzalez-Serrano, A. Amor-Martin, and J. Casamayon-Anton, "State estimation using an extended kalman filter with privacy-protected observed inputs," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2014, pp. 54–59.
- [21] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.
- [22] C. Gao, Z. Wang, X. He, and H. Dong, "Encryption–decryption-based consensus control for multi-agent systems: Handling actuator faults," *Automatica*, vol. 134, p. 109908, 2021.
- [23] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on paillier encryption," *Systems & Control Letters*, vol. 148, p. 104869, 2021.
- [24] C. Gao, Z. Wang, X. He, and H. Dong, "Fault-tolerant consensus control for multiagent systems: An encryption-decryption scheme," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2560–2567, 2021.
- [25] F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Engineering Practice*, vol. 67, pp. 13–20, 2017.
- [26] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on The Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.
- [27] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Transactions on Automatic Control*, 2022.
- [28] K. Teranishi and K. Kogiso, "Dynamic quantizer for encrypted observer-based control," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 5477–5482.
- [29] —, "Encrypted gain scheduling with quantizers for stability guarantee," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 5628–5633.
- [30] J. Kim, H. Shim, and K. Han, "Comprehensive introduction to fully homomorphic encryption for dynamic feedback controller via lwe-based cryptosystem," in *Privacy in Dynamical Systems*. Springer, 2020, pp. 209–230.
- [31] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Annual Cryptology Conference*. Springer, 2013, pp. 75–92.
- [32] M. Fetzter and C. W. Scherer, "A general integral quadratic constraints theorem with applications to a class of sampled-data systems," *SIAM Journal on Control and Optimization*, vol. 54, no. 3, pp. 1105–1125, 2016.
- [33] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. SIAM, 1994.
- [34] É. Gyurkovics, "A note on wirtinger-type integral inequalities for time-delay systems," *Automatica*, vol. 61, pp. 44–46, 2015.
- [35] S. Mehta and J. Chiasson, "Nonlinear control of a series dc motor: Theory and experiment," *IEEE Transactions on Industrial Electronics*, vol. 45, no. 1, pp. 134–141, 1998.
- [36] P. J. Antsaklis and A. N. Michel, *A Linear Systems Primer*. Springer Science & Business Media, 2007.
- [37] J. F. Kenney, *Mathematics of Statistics*. D. Van Nostrand, 1939.
- [38] N. J. Higham, *Functions of matrices: Theory and computation*. SIAM, 2008.