2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Conversion of Controllers to have Integer State Matrix for Encrypted Control: Non-minimal Order Approach

Joowon Lee, Donggil Lee, Seungbeom Lee, Junsoo Kim, and Hyungbo Shim

Abstract— **To implement an encrypted dynamic controller based on homomorphic encryption that operates for an infinite time horizon, it is essential for every component of the controller's state matrix to be an integer. In this paper, we tackle the challenge of converting a pre-designed controller into a new one with an integer state matrix, while preserving its control performance. This enables encrypted dynamic systems to be realized without re-encryption and approximation of control parameters. To achieve this, we allow the order of the controller to be increased so that the resulting closed-loop system becomes a non-minimal realization of the original closed-loop, without losing internal stability. Two approaches are proposed to design such controller with an integer state matrix. The first approach is to design the new controller as an estimator of the original closed-loop system, and the conditions on the estimator gain are derived. Our second approach is to formulate a problem of finding certain polynomials, whose solution leads to the design of the new controller. In a special case when the numerator of the plant transfer function is a constant, we provide a constructive method to obtain such solution.**

I. Introduction

In response to the increasing threat of cyber-attacks against networked control systems, encrypted control has emerged as a countermeasure to protect control data from malicious adversaries [1]–[3]. Encrypted control systems execute control operations directly over encrypted signals and parameters without the need to decrypt them beforehand. This is enabled by encrypting the controller using homomorphic encryption, which allows arithmetic operations to be carried out on encrypted messages. Thus, it is ensured that all control data are thoroughly encrypted along the networked portion of the system—from sensors to computing devices and eventually to actuators. The need for enhanced security in networked control systems has led to the introduction of encrypted control to various applications such as [4]–[7].

However, realizing control systems through homomorphic encryption carries significant challenges. This is mainly due to the properties of homomorphic encryption that lies on a bounded set of integers [8] unlike most control systems operating on real signals. Thus, every parameter of the pre-designed controller is converted to integers before encryption, by multiplying a large scaling factor and then rounding it off. In case of dynamic controllers, where the state is recursively multiplied by a real-valued parameter referred as the state matrix, such process causes the state to be multiplied not only by the state matrix but also by the large scaling factor. That is, the magnitude of the state grows exponentially to the scaling factor and eventually overflows the bounded message space of homomorphic encryption [9], [10]. While this issue could potentially be handled by dividing the state into the scaling factor, implementing operations other than addition and multiplication on encrypted data requires the bootstrapping technique [11]. However, this technique is computationally demanding and may not be feasible for real-time control systems.

Previous studies on encrypted dynamic control have addressed this issue by avoiding the infinitely recursive operations of dynamic controllers [2], [12] or converting the state matrix to have only integer components [9]. The former approaches involve transmitting the whole controller state to the actuator [2] or resetting the encrypted state periodically [12]. However, these methods tend to increase communication burden or may degrade the control performance, respectively. The latter approach converts the given state matrix into an integer matrix using the pole placement [9], however, this necessitates re-encryption of the encrypted control output that requires an additional communication link.

Follow-up results [13], [14] reformulate the given controller through approximation techniques, creating an integer state matrix and hence avoiding re-encryption. However, their weakness is the inevitable occurrence of approximation errors: in [13], such errors are not negligible in general so that it may yield performance degradation; in [14], the approximation error can be made arbitrarily small, but for smaller error the encrypted controller should be constructed with higher dimension or increased storage space.

In this paper, a conversion problem of linear dynamic controllers is introduced, aiming to facilitate their operation over encrypted data without relying on re-encryption or approximation of control parameters. The outcome of this conversion is a new dynamic controller having an integer state matrix that preserves the performance of the original controller. Specifically, the closed-loop system of the plant and the new controller should yield the same transfer function (from the reference signal to the plant output) as the original closed-loop system, while being internally stable. This new controller may have a larger state dimension, but cannot make use of any supplementary input or output that requires extra communication resources.

We propose two approaches to the problem. In our first approach, the new controller is designed as an estimator with respect to the original closed-loop system. Then, we

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2022-00165417).

J. Lee, D. Lee, S. Lee, and H. Shim are with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Korea.

J. Kim is with the Department of Electrical and Information Engineering, Seoul National University of Science and Technology, Korea.

provide sufficient conditions on the injection gain of the estimator that addresses the aforementioned problem. The second approach introduces a problem of finding certain polynomials whose solution leads to the design of the new controller. Particularly when the numerator of the plant transfer function is a constant, a constructive algorithm to obtain such polynomials is provided.

The rest of this paper is organized as follows. Section II provides preliminaries on encrypting dynamic controllers and formulates the problem. In Section III, our first approach of converting a pre-designed controller into an estimator of the closed-loop system is presented. Section IV proposes our second approach that formulates a polynomial problem and constructs the new controller based on its solution. Finally, Section V concludes the paper.

Notation: Let the set of integers, non-negative integers, and real numbers be denoted by $\mathbb{Z}$, $\mathbb{Z}_{\geq 0}$, and $\mathbb{R}$, respectively. The (component-wise) rounding function is denoted by $\lceil \cdot \rfloor$. Let $I_n \in \mathbb{R}^{n\times n}$ be the identity matrix, $\mathbf{0}_{m\times n} \in \mathbb{R}^{m\times n}$ be the zero matrix, and $\mathbf{0}_n \in \mathbb{R}^n$ be the zero vector. The characteristic polynomial of a matrix $A \in \mathbb{R}^{n\times n}$ is denoted by $\mathscr{P}_A(z) := \det(zI_n - A)$, and the degree of a polynomial $p(z)$ is denoted by $\deg(p(z))$.

II. Preliminaries and Problem Formulation

Consider a discrete-time plant written by

$$\begin{aligned} x_p(k+1) &= Ax_p(k) + Bu(k), \\ y(k) &= Cx_p(k), \end{aligned} \tag{1}$$

where $x_p(k) \in \mathbb{R}^{n_p}$, $u(k) \in \mathbb{R}^m$, and $y(k) \in \mathbb{R}$ are the state, the input, and the output, respectively. For simplicity, the plant output is considered to be scalar. Throughout the paper, we assume that the pair (A,C) is observable and the matrix B has full column rank.

A controller has been designed to control the plant (1) as

$$\begin{aligned} x(k+1) &= Fx(k) + Gy(k) + Pr(k), \\ u(k) &= Hx(k), \end{aligned} \tag{2}$$

where $x(k) \in \mathbb{R}^n$ is the state of the controller and $r(k) \in \mathbb{R}$ is a bounded reference signal. This controller stabilizes the closed-loop system of (1) and (2), rewritten as

$$\begin{aligned} x_c(k+1) &= \begin{bmatrix} A & BH \\ GC & F \end{bmatrix} x_c(k) + \begin{bmatrix} \mathbf{0}_{n_p} \\ P \end{bmatrix} r(k) \\ &=: A_c x_c(k) + B_c r(k), \\ y(k) &= \begin{bmatrix} C & \mathbf{0}_{1\times n} \end{bmatrix} x_c(k) =: C_c x_c(k), \end{aligned} \tag{3}$$

where $x_c(k) := \left[x_p(k)^\top, x(k)^\top\right]^\top$, and hence the matrix A_c is Schur stable. It is also assumed that the controller (2) is observable[1].

We aim to design a new controller that substitutes (2) without performance degradation in the closed-loop system (3), but has a better structure in terms of applying homomorphic encryption. Specifically, it is required that the state matrix of the new controller consists only of integers. In the following subsection, we review a method to encrypt a given dynamic controller having an integer state matrix while preserving the original control performance. Then, in Section II-B, the design problem of the new controller is formulated.

A. Systems having Integer State Matrix [9]

Before running the pre-designed dynamic controller (2) on homomorphically encrypted data, one needs to convert it so that every control operation is made up of addition or multiplication over integers. This process is straightforward when the state matrix F is an integer matrix.

For the rest of this subsection, it is assumed that $F \in \mathbb{Z}^{n\times n}$. The other matrices of (2) are converted to integers as $\overline{G} := \lceil G/s_1 \rfloor$, $\overline{P} := \lceil P/s_1 \rfloor$, and $\overline{H} := \lceil H/s_2 \rfloor$, with some scaling parameters $1/s_1 \geq 1$ and $1/s_2 \geq 1$. Then, with another parameter $\mathsf{L} > 1$ for quantization, the system (2) can be converted to operate over integers;

$$\begin{aligned} x_q(k+1) &= Fx_q(k) + \overline{G}\lceil y(k)/\mathsf{L} \rfloor + \overline{P}\lceil r(k)/\mathsf{L} \rfloor, \\ u_q(k) &= \overline{H}x_q(k), \end{aligned} \tag{4}$$

where $x_q(k) \in \mathbb{Z}^n$ is the state with the initial value $x_q(0) = \lceil x(0)/(\mathsf{L}s_1) \rfloor$ and $u_q(k) \in \mathbb{Z}^m$ is the output.

From this conversion process, it is expected that the values of $\mathsf{L}s_1 x_q(k)$ and $\mathsf{L}s_1 s_2 u_q(k)$ approximate the state $x(k)$ and the output $u(k)$, respectively, of the given controller (2) when the round-off errors remain sufficiently small. Indeed, thanks to the closed-loop stability of (3), the output $u(k)$ of (2) can be restored from $u_q(k)$ with an arbitrarily small error, as stated by the following proposition.

Proposition 1 ([9, Proposition 2])**.** *There exists a continuous function $\varepsilon(\mathsf{L}, s_1, s_2) \in \mathbb{R}$ vanishing at the origin such that $\left\|u(k) - \mathsf{L}s_1 s_2 u_q(k)\right\|_\infty \leq \varepsilon(\mathsf{L}, s_1, s_2)$ for all $k \in \mathbb{Z}_{\geq 0}$.* □

To encrypt the "quantized" controller (4), the initial state and the matrices F, $\overline{G}$, $\overline{P}$, and $\overline{H}$ are encrypted, and then the operations in (4) are implemented through homomorphic addition and multiplication [9].

B. Problem Formulation

Given the plant (1) and the pre-designed controller (2), the problem of interest is to replace the original controller (2) with a new one that can be converted in the form of (4), keeping the original control performance. We denote the new controller by

$$\begin{aligned} v(k+1) &= F'v(k) + G'y(k) + P'r(k), \\ u(k) &= H'v(k), \end{aligned} \tag{5}$$

where $v(k) \in \mathbb{R}^{\bar{n}}$ is the state with dimension $\bar{n}$, which is possibly larger than the dimension n of (2). The state matrix F' of (5) should be an integer matrix, or in general, should be able to be transformed into an integer matrix.

In the meantime, this conversion of controller from (2) to (5) should preserve both the closed-loop stability and performance in terms of the input-output relation between the reference and the plant output. In other words, the new closed-loop system of the plant (1) and the new controller (5)

[1] If the pair (F,H) is not observable, one can apply Kalman observable decomposition to the controller (2) and take the observable subsystem, which has the same input-output relation.

is expected to be a non-minimal realization of the original closed-loop system (3), while keeping the internal stability. To specify this, we write the transfer function of (3) as $T_{yr}(z) := C_c\left(zI_{n_p+n} - A_c\right)^{-1} B_c$ and the transfer function from $r(k)$ to $y(k)$ in the new closed-loop system as $T'_{yr}(z)$. Then, the problem is stated as follows.

Problem 1. *Given a plant (1) and a controller (2), design a controller (5) satisfying the following conditions:*

(C1) *There exists a nonsingular matrix $T \in \mathbb{R}^{\bar{n}\times\bar{n}}$ such that $T^{-1}F'T \in \mathbb{Z}^{\bar{n}\times\bar{n}}$.*

(C2) *The closed-loop system of (1) and (5) is stable.*

(C3) *The transfer function $T'_{yr}(z)$ equals $T_{yr}(z)$.* □

Remark 1. Although (C3) allows transient error between the signals of (2) and (5), it enforces the new controller to yield the same input-output relation in the closed-loop system on the frequency domain, whereas the previous results [13], [14] approximated the parameters of the original controller, resulting in different transfer functions. □

III. Conversion to Closed-loop Estimator Form

This section proposes a method to convert the given controller (2) into a new form having an integer state matrix, while maintaining the original control performance. To achieve this, we design the new controller (5) in the form of a state estimator for the closed-loop system (3). Furthermore, sufficient conditions for the injection gain of the estimator are provided to solve Problem 1, then interpreted further as an equation of polynomials.

To begin with, since it is desirable that the new controller (5) yields the same output as the given one, we attempt to compute $u(k) = Hx(k)$ in an alternate way. To this end, the new controller needs to construct the state of (2) solely from $y(k)$, its only input other than the external reference signal. Hence, we design an estimator that observes the controller state by viewing $y(k)$ as the output of the closed-loop system then building an estimator with respect to (3) as

$$v(k+1) = (A_c - LC_c)v(k) + Ly(k) + B_c r(k), \tag{6}$$

where $L \in \mathbb{R}^{n_p+n}$ is the estimator gain. Then, the output of the new controller can be computed from the estimated controller state, leading to our proposed design of (5) as follows:

$$\begin{aligned}\begin{bmatrix}\hat{x}_p(k+1)\\ \hat{x}(k+1)\end{bmatrix} &= \begin{bmatrix}A - L_1C & BH\\ (G-L_2)C & F\end{bmatrix}\begin{bmatrix}\hat{x}_p(k)\\ \hat{x}(k)\end{bmatrix}\\ &\quad + \begin{bmatrix}L_1\\ L_2\end{bmatrix} y(k) + \begin{bmatrix}\mathbf{0}_{n_p}\\ P\end{bmatrix} r(k), \qquad (7a)\\ u(k) &= H\hat{x}(k), \qquad (7b)\end{aligned}$$

where (7a) is another expression of (6) by denoting $v(k) =: \left[\hat{x}_p(k)^\top, \hat{x}(k)^\top\right]^\top$ and $L =: \left[L_1^\top, L_2^\top\right]^\top$.

For the rest of this section, we regard the new controller (5) as (7), and accordingly, $F' = A_c - LC_c$, $G' = L$, $P' = B_c$, $H' = \left[\mathbf{0}_{m\times n_p}, H\right]$, and the state dimension $\bar{n} = n_p + n$.

An advantage of this approach is that the state matrix of the estimator, in our case $A_c - LC_c$, can have a characteristic polynomial with integer coefficients arbitrarily assigned by the choice of the estimator gain $L \in \mathbb{R}^{n_p+n}$, if the system to be estimated is observable. This enables the state matrix to be converted to an integer matrix by similarity transformation. Specifically, if the pair (A_c, C_c) is observable, the closed-loop system (3) can be represented in the observable canonical form, and thus $A_c - LC_c$ is similar to

$$\begin{bmatrix}0 & 0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & 0 & \cdots & 0 & -a_1\\ 0 & 1 & 0 & \cdots & 0 & -a_2\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 0 & -a_{\bar{n}-2}\\ 0 & 0 & 0 & \cdots & 1 & -a_{\bar{n}-1}\end{bmatrix} \tag{8}$$

(for multi-input multi-output system, the transformation introduced in [15] can be used), where $\mathscr{P}_{A_c-LC_c}(z) =: z^{\bar{n}} + a_{\bar{n}-1}z^{\bar{n}-1} + \cdots + a_1 z + a_0$. Each coefficient a_i for $i = 0, 1, \ldots, \bar{n}-1$ can be assigned arbitrarily by pole placement, and therefore every component of the matrix (8) can be an integer by appropriate choice of L.

Thus, we assume the following for the original controller (2) to assure that the closed-loop system (3) is observable.

Assumption 1. *The poles of the controller* (2) *do not coincide with the invariant zeros of the plant* (1)*, i.e., for any eigenvalue $\lambda \in \mathbb{C}$ of F, the matrix*

$$\begin{bmatrix}\lambda I_{n_p} - A & -B\\ C & \mathbf{0}_{1\times m}\end{bmatrix}$$

has full column rank. □

In case the plant is a single-input single-output system, Assumption 1 can be understood that there is no cancellation among the zeros of the plant and the poles of the controller.

The following lemma states that Assumption 1 implies the observability of the closed-loop system (3).

Lemma 1. *Under Assumption 1, the pair (A_c, C_c) is observable.* □

Proof. We prove by contradiction. Suppose that there exist $\eta \in \mathbb{R}^{n_p}$ and $\xi \in \mathbb{R}^n$ such that $\left[\eta^\top, \xi^\top\right]^\top$ is nonzero and

$$\begin{bmatrix}sI_{n_p} - A & -BH\\ -GC & sI_n - F\\ C & \mathbf{0}_{1\times n}\end{bmatrix}\begin{bmatrix}\eta\\ \xi\end{bmatrix} = \mathbf{0}_{n_p+n+1} \tag{9}$$

for some $s \in \mathbb{C}$. First, consider the case when $\xi = \mathbf{0}_n$, which implies that $\eta \neq \mathbf{0}_{n_p}$. By (9), η satisfies both $A\eta = s\eta$ and $C\eta = 0$. This contradicts to the assumption that (A, C) is observable. Second, suppose that $\xi \neq \mathbf{0}_n$. Since (9) implies $C\eta = 0$ and $-GC\eta + (sI_n - F)\xi = \mathbf{0}_n$, it is derived that s is an eigenvalue of F. Then, we obtain $H\xi \neq \mathbf{0}_n$ by the observability of (F, H). However, it follows that

$$\begin{bmatrix}sI_{n_p} - A & -B\\ C & \mathbf{0}_{1\times m}\end{bmatrix}\begin{bmatrix}\eta\\ H\xi\end{bmatrix} = \mathbf{0}_{n_p+1}$$

from (9), thus s is an invariant zero of the plant. This contradicts to Assumption 1 and concludes the proof. ■

So far, we have shown that the estimator gain L can assign the characteristic polynomial coefficients of $A_c - LC_c$ to be

integers. Next, we see if the closed-loop system of the given plant (1) and the proposed controller (7) is stable while having the same transfer function as (3).

Since (7a) contains the estimator for the plant state, represented by $\hat{x}_p(k)$, we define the error state as $e(k) := \hat{x}_p(k) - x_p(k)$. Then, the closed-loop system of (1) and (7) is written as

$$\begin{bmatrix} e(k+1) \\ x_p(k+1) \\ \hat{x}(k+1) \end{bmatrix} = \begin{bmatrix} A-L_1C & \mathbf{0}_{n_p\times n_p} & \mathbf{0}_{n_p\times n} \\ \mathbf{0}_{n_p\times n_p} & A & BH \\ (G-L_2)C & GC & F \end{bmatrix} \begin{bmatrix} e(k) \\ x_p(k) \\ \hat{x}(k) \end{bmatrix} + \begin{bmatrix} \mathbf{0}_{1\times n_p} & \mathbf{0}_{1\times n_p} & P^\top \end{bmatrix}^\top r(k). \quad (10)$$

By replacing the controller (2) with (7), an internal dynamics with the state $e(k)$ has emerged in (10). As a result, the state matrix $A-L_1C$ of the error dynamics has to be Schur stable to satisfy the internal stability condition of Problem 1.

The following theorem states that the proposed controller (7) has an integer state matrix with the closed-loop performance equivalent to the original system (3), under certain conditions on the estimator gain L.

Theorem 1. *Under Assumption 1, if there exists an estimator gain $L = \left[L_1^\top, L_2^\top\right]^\top \in \mathbb{R}^{n_p+n}$ such that every coefficient of $\mathscr{P}_{A_c-LC_c}(z)$ is an integer and $A-L_1C$ is Schur stable, then the controller* (7) *is a solution to Problem 1.* □

Proof. By Lemma 1, the state matrix $A_c - LC_c$ is similar to the matrix (8), and hence (C1) is satisfied. Next, the state matrix of (10) is a block triangular matrix with $A-L_1C$ and A_c being the diagonal blocks. Since they are both Schur stable matrices, (C2) holds. Finally, the transfer function $T'_{yr}(z)$ is calculated as

$$\begin{bmatrix} \mathbf{0}_{1\times n_p} & C_c \end{bmatrix} \begin{bmatrix} zI_{n_p} - (A-L_1C) & \mathbf{0}_{n_p\times(n_p+n)} \\ * & zI_{n_p+n} - A_c \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{0}_{n_p} \\ B_c \end{bmatrix}$$

with some nonzero terms in $*$, and thus equals to $T_{yr}(z)$. This satisfies (C3) and concludes the proof. ■

Theorem 1 gives sufficient conditions on the estimator gain L that makes our proposed controller (7) a solution to Problem 1. Although there exists an additional constraint that $A-L_1C$ must be Schur stable, such design problem assures more capability to obtain an integer state matrix than converting the given state matrix F only by coordinate transformation. The following example illustrates the proposed conversion and elaborate on this increased capability.

Example 1: Let the plant (1) be given as

$$A = \begin{bmatrix} 0 & 1 \\ 1.5 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

which is unstable, and let the controller (2) be given as

$$F = \begin{bmatrix} -0.2 & 1 \\ -1.7 & 1.2 \end{bmatrix}, \quad G = \begin{bmatrix} 0.2 \\ 1.35 \end{bmatrix}, \quad H = \begin{bmatrix} -1.85 & 1.2 \end{bmatrix},$$

with some $P \in \mathbb{R}^{2\times 1}$. The resulting state matrix of the closed-loop system is

$$A_c = \begin{bmatrix} A & BH \\ GC & F \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1.5 & 0 & -1.85 & 1.2 \\ 0.2 & 0 & -0.2 & 1 \\ 1.35 & 0 & -1.7 & 1.2 \end{bmatrix},$$

which is Schur stable. Although the characteristic polynomial of F has non-integer coefficients, we can choose a gain $L = [l_1, l_2, l_3, l_4]^\top$ so that the proposed controller (7) solves Problem 1 by applying Theorem 1. First, by letting $[l_1, l_2] = [1, 0]$, every eigenvalue of $A - L_1C$ becomes zero. Then, from the observation that

$$\det\left(zI_4 - A_c + \begin{bmatrix} 1 \\ 0 \\ l_3 \\ l_4 \end{bmatrix} C_c\right) = \det\left(zI_4 - \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1.5 & 0 & -1.85 & 1.2 \\ 0.2 & -l_3 & -0.2 & 1 \\ 1.35 & -l_4 & -1.7 & 1.2 \end{bmatrix}\right)$$
$$= z^4 - z^3 + (1.46 - 1.85\,l_3 + 1.2\,l_4)z^2 + (0.18\,l_3 - 1.61\,l_4)z,$$

it can be found that $l_3 = 841/3137$ and $l_4 = 828/27625$ will exactly yield $\mathscr{P}_{A_c-LC_c}(z) = z^4 - z^3 + z^2$. □

However, one should not design L_1 and L separately by regarding that the two conditions in Theorem 1 are independent, since L_1 is a part of L. Thus, we analyze how these two conditions are related on the frequency domain.

For the rest of this section, we consider the case when the plant is a single-input single-output system. The transfer function of the plant (1) and that of the controller (2) (from $y(k)$ to $u(k)$) are denoted by

$$\frac{N_p(z)}{D_p(z)} := C\left(zI_{n_p} - A\right)^{-1}B, \; \frac{N_{c,y}(z)}{D_c(z)} := H\left(zI_n - F\right)^{-1}G, \quad (11)$$

where the denominators $D_p(z)$ and $D_c(z)$ are both monic polynomials with degree n_p and n, respectively.

Now we show that $\mathscr{P}_{A_c-LC_c}(z)$ can be represented by $\mathscr{P}_{A-L_1C}(z)$, $D_c(z)$, and $N_p(z)$, motivated by the equation

$$\mathscr{P}_{A_c}(z) = D_p(z)D_c(z) - N_p(z)N_{c,y}(z). \quad (12)$$

One can interpret that the blocks A, F, BH, and GC comprising the matrix A_c determine the polynomials $D_p(z)$, $D_c(z)$, $N_p(z)$, and $N_{c,y}(z)$, respectively, on the right hand side of (12). This is trivial for the blocks A and F since $\mathscr{P}_A(z) = D_p(z)$ and $\mathscr{P}_F(z) = D_c(z)$. For the blocks BH and GC, consider the plant and the controller in the observable canonical form without loss of generality, as both of them are observable. Then, we obtain

$$BH = \begin{bmatrix} \mathbf{0}_{n_p} & \cdots & \mathbf{0}_{n_p} & B \end{bmatrix} \text{ and } GC = \begin{bmatrix} \mathbf{0}_n & \cdots & \mathbf{0}_n & G \end{bmatrix},$$

where the elements of B and G are the coefficients of $N_p(z)$ and $N_{c,y}(z)$, respectively.

Observe that the matrix $A_c - LC_c$ has the same block matrix structure as A_c, except that the blocks A and G of A_c are replaced by $A-L_1C$ and $G-L_2$ in $A_c - LC_c$. Hence, the characteristic polynomial of $A_c - LC_c$ can be written as

$$\mathscr{P}_{A_c-LC_c}(z) = \alpha(z)D_c(z) + \beta(z)N_p(z) \quad (13)$$

with some polynomials $\alpha(z)$ and $\beta(z)$ determined by $A - L_1C$ and $G-L_2$, respectively. Indeed, the coefficients of $\beta(z)$ can be arbitrarily assigned by the choice of L_2 within the maximum degree $n-1$, and $\alpha(z) = \mathscr{P}_{A-L_1C}(z)$.

Therefore, finding the gain L that satisfies the two conditions of Theorem 1 is equivalent to finding a monic and Schur stable polynomial $\alpha(z)$ with degree n_p and a polynomial $\beta(z)$ with maximum degree $n-1$ such that (13) is an integer polynomial. However, the pair of such $\alpha(z)$ and $\beta(z)$ does

not always exist, partly due to the limit on their degrees. Such limit comes from the fixed dimension of the gain L, which is also the dimension of the proposed controller (7) by design. Meanwhile, recall that the new controller (5) is formulated without restricting the state dimension $\bar{n}$.

Accordingly, in the next section, we approach to Problem 1 by deriving (13) under rather relaxed conditions, through analyzing the general controller (5) on the frequency domain.

IV. Approach to General Conversion by Polynomial Equation

We return to the general form (5) of the new controller and construct its transfer function matrix which solves Problem 1, in case where the plant is a single-input single-output system. To this end, a problem on finding certain polynomials is formulated, whose solution directly leads to the solution of Problem 1. In contrast to Section III, we do not pre-determine the form of the matrices in (5) nor their dimensions.

We denote the transfer function matrix of (5) by

$$\frac{1}{D'_c(z)}\begin{bmatrix} N'_{c,y}(z) & N'_{c,r}(z)\end{bmatrix} := H'\left(zI_{\bar{n}}-F'\right)^{-1}\begin{bmatrix} G' & P'\end{bmatrix}, \quad (14)$$

where $D'_c(z)$ is a monic polynomial of degree $\bar{n}$, *i.e.*, the characteristic polynomial of F'. The transfer functions of the plant (1) and the original controller (2) are written as (11) and $N_{c,r}(z) := D_c(z)H\left(zI_n-F\right)^{-1}P$. Subsequently, we derive the closed-loop transfer functions $T_{yr}(z)$ and $T'_{yr}(z)$ with respect to the plant output from the reference, and rewrite the three conditions of Problem 1.

It is easily calculated that

$$T_{yr}(z) = \frac{N_{c,r}(z)N_p(z)}{D_p(z)D_c(z)-N_p(z)N_{c,y}(z)},$$

and $T'_{yr}(z)$ can be obtained likewise. Then, the condition (C3), $T_{yr}(z) = T'_{yr}(z)$, will be ensured if there exists a monic polynomial $\alpha(z)$ of degree $\bar{n}-n$ such that

$$N'_{c,r}(z)N_p(z) = N_{c,r}(z)N_p(z)\alpha(z) \quad (15a)$$

and

$$\begin{aligned} &D_p(z)D'_c(z)-N_p(z)N'_{c,y}(z)\\ &\qquad = (D_p(z)D_c(z)-N_p(z)N_{c,y}(z))\alpha(z), \quad (15b)\end{aligned}$$

because the roots of the polynomial $\alpha(z)$ as both poles and zeros of the system will be cancelled out. Since (C2) only allows stable pole-zero cancellations, we enforce $\alpha(z)$ to be a Schur stable polynomial. Moreover, if the denominator $D'_c(z)$ of the new transfer function matrix is an integer polynomial, the new controller can be realized to have an integer state matrix, satisfying (C1).

Under these conditions, we obtain the relation

$$D'_c(z) = \alpha(z)D_c(z) + \frac{N'_{c,y}(z)-\alpha(z)N_{c,y}(z)}{D_p(z)}N_p(z) \quad (16)$$

from (15). Observe that (16) has a form similar to (13), where $\mathscr{P}_{A_c-LC_c}(z)$ is in fact $D'_c(z)$ when the new controller is designed as (7). In this perspective, consider the following problem of solving an indeterminate polynomial equation, which resembles (16), under certain constraints.

Problem 2. *Given $n_p \in \mathbb{N}$, a polynomial $N_p(z)$ with degree less than n_p, and a monic polynomial $D_c(z)$, find polynomials $\alpha(z)$, $\beta(z)$, and $I(z)$ such that*

$$\alpha(z)D_c(z)+\beta(z)N_p(z) = I(z) \quad (17)$$

and satisfy the followings:

(P1) *$\alpha(z)$ is a monic and Schur stable polynomial.*
(P2) *$I(z)$ is a monic integer polynomial.*
(P3) $\deg(\beta(z)) < \deg(I(z)) - n_p$. □

Problem 2 does not restrict the degree of $I(z)$, and therefore is solved if any such integer polynomial $I(z)$ is found. From any existing solution to Problem 2, one is able to construct the transfer function matrix (14) as

$$\begin{aligned} D'_c(z) &= I(z),\\ N'_{c,y}(z) &= \beta(z)D_p(z)+\alpha(z)N_{c,y}(z), \quad (18)\\ N'_{c,r}(z) &= N_{c,r}(z)\alpha(z),\end{aligned}$$

so that (15) holds and (14) is strictly proper.

The following theorem states that given the plant (1) and the original controller (2), the new controller (18) built from a solution to Problem 2 becomes a solution to Problem 1.

Theorem 2. *Suppose that there exist polynomials $\alpha(z)$, $\beta(z)$, and $I(z)$ solving Problem 2. Then, the controller (14) designed as (18) is a solution to Problem 1.* □

Proof. Since every coefficient of $D'_c(z) = I(z)$ is an integer, the state matrix F' has an integer characteristic polynomial and can be transformed into the form of (8), thus (C1) holds. By construction, (18) implies (16), and hence (15) is satisfied, ensuring the condition (C3). Since the right hand side of (15b) is Schur stable, (C2) follows. ■

Note that the condition (P3) of Problem 2 enforces the degree of $\beta(z)N_p(z)$ to be less than $\deg(I(z)) - r_p$, where r_p is the relative degree of the plant (1). In other words, the first r_p+1 higher order terms of $\alpha(z)D_c(z)$ must have integer coefficients. At the same time, the remaining part of $\alpha(z)D_c(z)$ and $\beta(z)N_p(z)$ should be summed up to yield an integer polynomial.

Meanwhile, in the special case when $r_p = n_p$, *i.e.*, the denominator $N_p(z)$ is a nonzero constant, one can first find a Schur stable $\alpha(z)$ so that $\alpha(z)D_c(z)$ has integer coefficients for the higher order terms, and then choose $\beta(z)$. In this case, Algorithm 1 provides a constructive method to find such $\alpha(z)$, as well as $I(z)$ and $\beta(z)$.

Proposition 2. *If $N_p(z)$ is a nonzero constant, the output of Algorithm 1 is a solution to Problem 2.* □

Proof. Throughout Algorithm 1, it is clear that (P1) and (P2) hold since $|r-\lceil r\rfloor| \le \frac{1}{2}$ for any $r \in \mathbb{R}$. By construction, the output $\beta(z)$ of Algorithm 1 satisfies (17) and (P3) since $\deg(\beta(z)) = \deg(\gamma(z))$. Now we show that the condition $N-m > n_p$ is achieved within a finite number of iterations. After Step 5 is executed, the leading terms of $\gamma(z)$ and $I(z)$ are rz^m

Algorithm 1 Solving Problem 2 when $\deg(N_p(z)) = 0$

Input: $D_c(z)$, $N_p(z)$, n_p

1: $N \leftarrow \deg(D_c(z))$
2: $\alpha(z) \leftarrow 1$, $I(z) \leftarrow z^N$, $\gamma(z) \leftarrow \alpha(z)D_c(z) - I(z)$
3: $m \leftarrow \deg(\gamma(z))$
4: **while** $N - m \le n_p$ **do**
5: $\quad r \leftarrow$ the leading coefficient of $\gamma(z)$
6: $\quad \alpha(z) \leftarrow \left(z^{N-m} + \lceil r \rfloor - r\right)\alpha(z)$
7: $\quad I(z) \leftarrow z^{N-m}I(z) + \lceil r \rfloor z^N$
8: $\quad \gamma(z) \leftarrow \alpha(z)D_c(z) - I(z)$
9: $\quad m \leftarrow \deg(\gamma(z))$, $N \leftarrow \deg(I(z))$
10: **end while**
11: $\beta(z) \leftarrow -\gamma(z)/N_p(z)$

Output: $\alpha(z)$, $\beta(z)$, $I(z)$

and z^N, respectively. Then, by writing $\gamma(z) =: rz^m + \gamma'(z)$ and $I(z) =: z^N + I'(z)$, one can compute the following:

$$\begin{aligned}
&\left(z^{N-m} + \lceil r \rfloor - r\right)\alpha(z)D_c(z) \\
&= \left(z^{N-m} + \lceil r \rfloor - r\right)(I(z) + \gamma(z)) \\
&= z^{N-m}I(z) + \lceil r \rfloor z^N + (\lceil r \rfloor - r)\left(I'(z) + \gamma'(z)\right) + z^{N-m}\gamma'(z) \\
&=: z^{N-m}I(z) + \lceil r \rfloor z^N + l(z),
\end{aligned}$$

which turns into $\alpha(z)D_c(z) = I(z) + l(z)$ after Step 7. Subsequently, Step 8 substitutes $l(z)$ to $\gamma(z)$, whose degree is now less than N. Since $\deg(I(z)) = 2N - m$ at this point, we obtain $\deg(I(z)) - \deg(\gamma(z)) > N - m$. This implies that $N - m$ at Step 9 is strictly greater than that evaluated before, and thus $N - m$ eventually exceeds n_p. ■

The outcome $I(z)$ from Algorithm 1 has degree at most $\frac{1}{2}n_p(n_p+1) + n$, which is the case when $N - m$ increases by one through every iteration. Note that the output of Algorithm 1 is not the only solution of Problem 2.

The following example illustrates how the polynomials $\alpha(z)$, $\beta(z)$, and $I(z)$ are found through Algorithm 1.

Example 2: Given $n_p = 3$, $N_p(z) = 1$, and

$$D_c(z) = z^3 + 1.2z^2 + 0.5z + 0.3,$$

we run Algorithm 1 as follows. Initially, we obtain

$$\alpha(z)D_c(z) = 1 \cdot D_c(z) = I(z) + 1.2z^2 + 0.5z + 0.3,$$

hence $N - m = 1$ and $r = 1.2$. Then, the polynomials are updated as $\alpha(z) = z - 0.2$ and $I(z) = z^4 + z^3$, resulting

$$\alpha(z)D_c(z) = (z - 0.2)D_c(z) = z^4 + 1 \cdot z^3 + 0.26z^2 + \cdots.$$

Now we have $N - m = 2$ and $\alpha(z)D_c(z)$ is computed as

$$(z^2 - 0.26)(z - 0.2)D_c(z) = z^2\left(z^4 + z^3\right) - 0.06z^3 + \cdots.$$

As $N - m = 3$, we move on to the next iteration and obtain

$$\begin{aligned}
&(z^3 + 0.06)(z^2 - 0.26)(z - 0.2)D_c(z) \\
&\qquad = z^3\left(z^6 + z^5\right) - 0.0676z^5 + \cdots = z^9 + z^8 + \gamma(z),
\end{aligned}$$

which leads to $N - m = 4 > n_p$. Therefore, Algorithm 1 returns $I(z) = z^9 + z^8$, $\alpha(z) = (z^3 + 0.06)(z^2 - 0.26)(z - 0.2)$, and $\beta(z) = -\gamma(z)$ with $\deg(\beta(z)) = 5$. □

V. Conclusion

We have proposed two approaches to convert a pre-designed controller into a new one having an integer state matrix, which can operate on encrypted data without re-encryption or approximation of the given model while preserving the original control performance in the closed-loop system. In our first approach, we have designed the new controller as an estimator of the closed-loop system, providing sufficient conditions for the estimator gain to induce an integer state matrix without losing the internal stability. The second approach formulates a problem on polynomials whose solution directly leads to the design of the new controller. We provide an algorithm to solve this problem in case when the numerator of the plant transfer function is a constant. Therefore, solving this polynomial problem in general is considered as our future work.

References

[1] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Syst. Mag.*, vol. 41, no. 3, pp. 58–78, 2021.

[2] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Proc. 54th IEEE Conf. Decision Control*, 2015, pp. 6836–6843.

[3] J. Kim, D. Kim, Y. Song, H. Shim, H. Sandberg, and K. H. Johansson, "Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption," *Annu. Rev. Control*, vol. 54, pp. 200–218, 2022.

[4] M. Schulze Darup, A. Redder, I. Shames, F. Farokhi, and D. Quevedo, "Towards encrypted MPC for linear constrained systems," *IEEE Control Syst. Lett.*, vol. 2, no. 2, pp. 195–200, 2018.

[5] A. B. Alexandru, K. Gatsis, Y. Shoukry, S. A. Seshia, P. Tabuada, and G. J. Pappas, "Cloud-based quadratic optimization with partially homomorphic encryption," *IEEE Trans. Autom. Control*, vol. 66, no. 5, pp. 2357–2364, 2021.

[6] K. Teranishi, M. Kusaka, N. Shimada, J. Ueda, and K. Kogiso, "Secure observer-based motion control based on controller encryption," in *Proc. 2019 Am. Control Conf.*, 2019, pp. 2978–2983.

[7] J. Suh and T. Tanaka, "Encrypted value iteration and temporal difference learning over leveled homomorphic encryption," in *Proc. 2021 Am. Control Conf.*, 2021, pp. 2555–2561.

[8] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, 2009.

[9] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Trans. Autom. Control*, vol. 68, no. 2, pp. 660–672, 2023.

[10] 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 Control*, 2018, pp. 5020–5025.

[11] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in *Advances in Cryptology – EUROCRYPT 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 129–148.

[12] 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.

[13] M. S. Tavazoei, "Nonminimality of the realizations and possessing state matrices with integer elements in linear discrete-time controllers," *IEEE Trans. Autom. Control*, vol. 68, no. 6, pp. 3698–3703, 2023.

[14] 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 Control*, 2021, pp. 5614–5619.

[15] J. Kim, "Further methods for encrypted linear dynamic controllers utilizing re-encryption," arXiv:2307.16445 [eess.SY], 2023.