2022 IEEE 61st Conference on Decision and Control (CDC)
December 6-9, 2022. Cancún, Mexico

Asymptotic Stabilization over Encrypted Data with Limited Controller Capacity and Time-varying Quantizer

Junsoo Kim, Moritz Schulze Darup, Henrik Sandberg, and Karl H. Johansson

2022 IEEE 61st Conference on Decision and Control (CDC) | 978-1-6654-6761-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CDC51059.2022.9993215

***Abstract*— We consider a problem of implementing dynamic controllers over encrypted data for asymptotic stabilization of closed-loop systems. Though a time-varying quantizer is used and it can be infinitesimally fine with time, a major issue is that the underlying space for encrypted messages is unavoidably finite and the controller receives a limited amount of quantized data. To resolve this issue, the proposed method takes advantage of the state matrix consisting of integers, which enables the controller to generate only lower bits of the same output without computing the upper bits. Whenever a portion of the upper bits of output has converged, the computation scope can be moved further lower, receiving only lower bits of the measurement. The quantization is scheduled and the size of the message space is predetermined from the convergence rate, so that the feedback input is restored from the outcome of the lower bits, no matter how fine quantization is performed in the end. As a consequence, asymptotic stabilization can be achieved by encrypted operation, despite the limited controller capacity.**

I. Introduction

The notion of encrypted control has been introduced [1]–[4] to protect all control data in the network layer, by encryption. By the use of cryptosystems that allow arithmetic operations without decryption, more and more control schemes, such as optimization algorithms [5]–[8], distributed protocols [9]–[15], and dynamic systems [16]–[24], are being implemented with digital computers over encrypted signals and parameters.

To implement and run the operation circuits solely based on the homomorphic property of cryptosystem without any concerns of eavesdropping attacks or collusion issues, only the abilities of modular addition and multiplication have been exploited for real-time operation in most cases, as the others may require substantial amount of computing resource [25]. Then, a problem of implementing dynamic systems using modular arithmetic was formulated, and the case of linear systems was introduced as the first step [2]–[4].

The major issue when implementing linear systems is that the state of the system is multiplied by non-integer numbers for every iteration, in general; this is because, unless rounding operation is used for discarding least significant figures, the significand increases exponentially fast so that it causes an overflow and loses its value, in a few iterations (see [21, Section II.D]). As a result, reset or re-encryption for the state was considered in initial studies [2], [16].

Then, considering that the issue is due to the recursive multiplication by a matrix of non-integers, a subclass of linear systems, which has the state matrix consisting of integers, has been studied [17]–[21]. It has been addressed in [17] that systems having the state matrix as integers can be implemented using only modular arithmetic, and it can operate with the significand of the state bounded for an infinite time horizon, under closed-loop stability. With this motivation, stability of integer matrices is investigated in [18], and then, it has been proposed in [19]–[21] that any linear system can be implemented to operate with modular arithmetic over encrypted data, by converting the (non-integer) state matrix to integers while keeping (practically) the same input-output relation.

As the class of systems having "integer state matrix" were not of interest before the homomorphic encryption was introduced, a further benefit of such systems has also been investigated, regarding digital implementation aside from encryption. In [21], it is suggested that systems having integer state matrix, implemented with addition and multiplication over integers, can generate only lower bits of the same output without computing the upper bits, thanks to the modulo operation compatible with addition and multiplication. And, it proposes that the system can keep the same input-output relation as long as the modulus (the size of the message space) covers the range of the output, even if some higher bits of the state are cut off and lost in the system. See Remark 6 and Fig. 3 in [21] for more details.

On the other hand, in terms of performance, the results on encrypted implementation have coincided with that from the existing results on quantized control, as in [26], [27]. Since the modulus of the cryptosystem is unavoidably finite and the system is implemented with digital computers, there must be performance error due to quantization. As a result, most results considering a fixed level of quantization suggest that the performance error is determined depending on the quantization parameter. And, in order for asymptotic stabilization, it has been considered as in [23] that time-varying quantizer is required which can be infinitesimally fine, and corresponding infinite amounts of controller storage and modulus of cryptosystem are required as time goes by.

In this context, we propose a further benefit of the systems having integer state matrix, in that they enable asymptotic

This work was supported in part by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1A6A3A03038953), and in part by the Swedish Research Council, the Knut and Alice Wallenberg Foundation, and the Swedish Strategic Research Foundation.

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

M. Schulze Darup is with the Department of Mechanical Engineering, TU Dortmund, Germany.

H. Sandberg and K. H. Johansson are with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Sweden. They are also affiliated with Digital Futures.

stabilization with a limited amount of controller capacity. More specifically, we propose a method for implementing linear dynamic controllers based on homomorphic encryption with a fixed modulus, which achieves asymptotic stabilization of the closed-loop system with the use of time-varying quantizer. Supposing that the state matrix has been converted to integers using the methods in [21] or [20], we show how to implement the given model of controller to operate with modular arithmetic together with the time-varying quantizer, which generates only a portion of lower bits of the same controller output. Then, a parameter design for the modulus of the cryptosystem and the time-varying quantization is provided considering the convergence rate of the control signals, which lets the scope of the quantization and the computation move further lower only when the upper bits have converged. As a consequence, it guarantees that the upper bits of the controller output can be restored after decryption, no matter how fine quantization is performed in the end. And, asymptotic stabilization is guaranteed despite the predetermined finite modulus, if the quantization level can be infinitesimally fine as time goes by.

The organization of the rest of this paper is as follows. Section II begins with preliminaries on homomorphic encryption and dynamic systems over modular arithmetic, and formulates the problem. Section III presents the main result, where Section III-A proposes implementation over integers with consideration of time-varying quantizers, and Section III-B proposes the implementation with modular arithmetic and parameter design for asymptotic stabilization. Finally, Section IV concludes the paper.

Notation: Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ be the set of natural numbers, integers, rational numbers, and real numbers, respectively. The (component-wise) floor and round functions are denoted by $\lfloor\cdot\rfloor$ and $\lceil\cdot\rfloor$, respectively. For $m \in \mathbb{N}$ and $n \in \mathbb{N}$, let $0_{m\times n} \in \mathbb{R}^{m\times n}$ be the zero matrix, $I_n \in \mathbb{R}^{n\times n}$ be the identity matrix, and let 1_n denote the vector $[1, \cdots, 1]^\top \in \mathbb{R}^n$. The set of integers modulo $q \in \mathbb{N}$ is denoted by $\mathbb{Z}_q$, and the (component-wise) modulo operation is defined as $v \mod q := v - \lfloor v/q \rfloor q$ for $v \in \mathbb{Z}^m$. We further define the "biased" modulo operation as

$$v \mod (q, v_0) := v - \left\lfloor \frac{v - v_0 + \frac{q}{2}\cdot 1_m}{q} \right\rfloor q \qquad (1)$$

for $v \in \mathbb{Z}^m$ and $v_0 \in \mathbb{R}^m$, so that each component of the outcome is greater than or equal to that of $v_0 - \frac{q}{2}$, and less than that of $v_0 + \frac{q}{2}$. The (induced) infinity norm of a vector or a matrix is denoted as $\|\cdot\|$.

II. Preliminaries and Problem Formulation

We first describe a sort of homomorphic cryptosystem with which a class of dynamic system can be implemented to run over encrypted data, based on the homomorphic property.

A. Dynamic System over Encrypted Data

The cryptosystem used throughout the paper is denoted by $(\mathbb{Z}_q, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec})$, where $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ is the plaintext (un-encrypted message) space, $\mathcal{C}$ is the ciphertext (encrypted message) space, and $\mathsf{Enc} : \mathbb{Z}_q^n \to \mathcal{C}^n$ and $\mathsf{Dec} : \mathcal{C}^n \to \mathbb{Z}_q^n$, $n \in \mathbb{N}$, are the (component-wise) encryption and decryption algorithm for vectors of messages, respectively. We omit the argument of key for encryption and decryption.

The cryptosystem is assumed to satisfy (at least) the homomorphic properties of addition and integer multiplication over ciphertexts, so that it satisfies the followings:

H1: For all $m \in \mathbb{Z}_q^n$ with $n \in \mathbb{N}$, $\mathsf{Dec}(\mathsf{Enc}(m)) = m$ holds.

H2: There exists an operation $\mathsf{Add}_n : \mathcal{C}^n \times \mathcal{C}^n \to \mathcal{C}^n$ for each $n \in \mathbb{N}$, such that $\mathsf{Dec}(\mathsf{Add}_n(\mathbf{c}_1, \mathbf{c}_2)) = \mathsf{Dec}(\mathbf{c}_1) + \mathsf{Dec}(\mathbf{c}_2) \mod q$, for all $\mathbf{c}_1 \in \mathcal{C}^n$ and $\mathbf{c}_2 \in \mathcal{C}^n$.

H3: There exists $\mathsf{IntMult}_{m,n} : \mathbb{Z}_q^{m\times n} \times \mathcal{C}^n \to \mathcal{C}^m$ for each $m \in \mathbb{N}$ and $n \in \mathbb{N}$, such that $\mathsf{Dec}(\mathsf{IntMult}_{m,n}(K, \mathbf{c})) = K \cdot \mathsf{Dec}(\mathbf{c}) \mod q$, for all $K \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{c} \in \mathcal{C}^n$.

The properties H2 and H3 refer to the ability of addition and integer multiplication on ciphertexts, respectively, so we abuse notion and use $\mathbf{c}_1 + \mathbf{c}_2 := \mathsf{Add}_n(\mathbf{c}_1, \mathbf{c}_2)$ and $K \cdot \mathbf{c}_1 := \mathsf{IntMult}_{m,n}(K, \mathbf{c}_1)$, for $\mathbf{c}_1 \in \mathcal{C}^n$, $\mathbf{c}_2 \in \mathcal{C}^n$, and $K \in \mathbb{Z}_q^{m\times n}$.

Thanks to the properties H1–H3, dynamic systems over the set $\mathbb{Z}_q$ operating with modular arithmetic can be implemented to run over encrypted data. Consider a system over $\mathbb{Z}_q$, as

$$\begin{aligned} \mathsf{x}(t+1) &= \mathsf{F}(t)\mathsf{x}(t) + \mathsf{G}(t)\mathsf{y}(t) \mod q, \quad \mathsf{x}(0) = \mathsf{x}_0, \\ \mathsf{u}(t) &= \mathsf{H}(t)\mathsf{x}(t) + \mathsf{J}(t)\mathsf{y}(t) \mod q, \quad t = 0, 1, \cdots, \end{aligned} \qquad (2)$$

where $\mathsf{x}(t) \in \mathbb{Z}_q^{\mathsf{n}_e}$ is the state with the initial value $\mathsf{x}_0 \in \mathbb{Z}_q^{\mathsf{n}_e}$, $\mathsf{y}(t) \in \mathbb{Z}_q^{\mathsf{p}_e}$ is the input, $\mathsf{u}(t) \in \mathbb{Z}_q^{\mathsf{m}_e}$ is the output, and $\{\mathsf{F}(t), \mathsf{G}(t), \mathsf{H}(t), \mathsf{J}(t)\}$ are (time-varying) matrices consisting of elements in $\mathbb{Z}_q$, with respective dimensions.

Then, the following proposition shows that the operation of (2) can be implemented directly over encrypted signals.

Proposition 1: Consider a dynamic system over $\mathcal{C}$, as

$$\begin{aligned} \mathbf{x}(t+1) &= \mathsf{F}(t)\cdot\mathbf{x}(t) + \mathsf{G}(t)\cdot\mathsf{Enc}(\mathsf{y}(t)), \quad \mathbf{x}(0) = \mathsf{Enc}(\mathsf{x}_0), \\ \mathbf{u}(t) &= \mathsf{H}(t)\cdot\mathbf{x}(t) + \mathsf{J}(t)\cdot\mathsf{Enc}(\mathsf{y}(t)), \end{aligned} \qquad (3)$$

in which $\mathbf{x}(t) \in \mathcal{C}^{\mathsf{n}_e}$ and $\mathbf{u}(t) \in \mathcal{C}^{\mathsf{m}_e}$. Then, it ensures that $\mathsf{Dec}(\mathbf{x}(t)) = \mathsf{x}(t)$ and $\mathsf{Dec}(\mathbf{u}(t)) = \mathsf{u}(t)$ hold, $\forall t \geq 0$. □

Proof: Take $\mathsf{Dec}(\cdot)$ to both sides of (3). Then, by H1–H3, it is obvious that $\mathsf{Dec}(\mathbf{x}(t+1)) = \mathsf{x}(t+1)$ and $\mathsf{Dec}(\mathbf{u}(t)) = \mathsf{u}(t)$, $\forall t \geq 0$, and $\mathsf{Dec}(\mathbf{x}(0)) = \mathsf{x}_0$. It completes the proof.■

B. Problem Formulation

We consider a discrete-time closed-loop system of plant and controller. Let the plant be written as

$$\begin{aligned} x_p(t+1) &= Ax_p(t) + Bu(t), \quad x_p(0) = x_{p,0}, \\ y(t) &= Cx_p(t), \end{aligned} \qquad (4)$$

where $x_p(t) \in \mathbb{R}^{\mathsf{n}_p}$, $u(t) \in \mathbb{R}^{\mathsf{m}}$, $y(t) \in \mathbb{R}^{\mathsf{p}}$, and $x_{p,0} \in \mathbb{R}^{\mathsf{n}_p}$ are the state, input, output, and initial state, respectively. And, let a feedback controller have been designed as

$$\begin{aligned} x(t+1) &= Fx(t) + Gy(t) + Pr(t), \quad x(0) = x_0, \\ u(t) &= Hx(t) + Jy(t) + Qr(t), \end{aligned} \qquad (5)$$

where $x(t) \in \mathbb{R}^{\mathsf{n}}$ is the state with the initial value x_0, and $r(t) \equiv r_\infty \in \mathbb{R}^{\mathsf{q}}$ is the constant reference. For digital implementation of the controller (5), we assume that the elements of the matrices are designed to be rational numbers.

The closed loop of (4) and (5) is assumed to be stable, as the design of the controller (5) is supposed to stabilize the plant (4); let the closed loop system be written at once, as

$$\begin{bmatrix} x_p(t+1) \\ x(t+1) \end{bmatrix} = \begin{bmatrix} A+BJC & BH \\ GC & F \end{bmatrix} \begin{bmatrix} x_p(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} BQ \\ P \end{bmatrix} r(t)$$
$$=: A_{\mathsf{cl}} \begin{bmatrix} x_p(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} BQ \\ P \end{bmatrix} r(t), \tag{6}$$

where the state matrix A_{cl} is Schur stable, so that there exist $M_{\mathsf{cl}} > 0$ and $\lambda_{\mathsf{cl}} < 1$ such that $\|A_{\mathsf{cl}}^t\| \le M_{\mathsf{cl}}\lambda_{\mathsf{cl}}^t$, $\forall t \ge 0$. Then, with $r(t) \equiv r_\infty$, the equilibrium of (6) is found as

$$\begin{bmatrix} x_{p,\infty} \\ x_\infty \end{bmatrix} := (I_{\mathsf{n}_p+\mathsf{n}} - A_{\mathsf{cl}})^{-1} \begin{bmatrix} BQ \\ P \end{bmatrix} r_\infty, \tag{7}$$

so that the state asymptotically (exponentially) converges, as

$$\left\| \begin{bmatrix} x_p(t) - x_{p,\infty} \\ x(t) - x_\infty \end{bmatrix} \right\| = \left\| A_{\mathsf{cl}}^t \begin{bmatrix} x_{p,0} - x_{p,\infty} \\ x_0 - x_\infty \end{bmatrix} \right\| \le 2M_0 M_{\mathsf{cl}} \lambda_{\mathsf{cl}}^t,$$

where we let $M_0 > 0$ be a constant such that

$$\max\{\|x_{p,0}\|, \|x_0\|, \|x_{p,\infty}\|, \|x_\infty\|, \|r_\infty\|\} \le M_0.$$

We also assume that the constants $\{M_{\mathsf{cl}}, \lambda_{\mathsf{cl}}, M_0\}$ are known.

Now, we state the problem of interest which we call "asymptotic stabilization over encrypted data," as follows.

Problem 1: Given the parameters of (5), construct a controller of the form (3) over ciphertexts, which guarantees that $\lim_{t\to\infty} x_p(t) = x_{p,\infty}$. Especially, the modulus $q \in \mathbb{N}$ of the cryptosystem should not be changed with time. □

Equivalently, the problem is to convert the controller (5) to the form (2), to operate over $\mathbb{Z}_q$ with modular arithmetic.

A major issue on this problem is "limited capacity" of the controller of the form (2) over the space $\mathbb{Z}_q$; once (2) starts operating and the modulus $q \in \mathbb{N}$ is fixed and is not changed with time. The controller operation is limited to deal with only a finite number of messages in $\mathbb{Z}_q$ for the whole time. The controller inputs $y(t)$ and $r(t)$ of real signals should be quantized to the elements in $\mathbb{Z}_q$ and there must be a quantization error. Nonetheless, the effect of the quantization error should vanish to zero as time goes by, and the asymptotic stability should be preserved.

Finally, we add an assumption that the state matrix F of (5) has been designed as integers, i.e., $F \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$. This is not to restrict the applicable class of controllers but to omit the process of converting the state matrix of non-integers to integers for simplicity, as a couple of state matrix conversion methods have been presented[1] for arbitrary linear systems, as in [21] or [20]. In fact, this condition (or the state matrix conversion) is required for implementing dynamic controllers to operate over ciphertexts for an infinite time horizon, leaving the issue of asymptotic stabilization aside.

[1]For example, given any system (5) with $F \notin \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$, a system of form

$$\begin{aligned} z(t+1) &= F'z(t) + G'y(t) + P'r(t) + Ru'(t), \quad z(t) \in \mathbb{R}^{\mathsf{n}'},\ \mathsf{n}' \le \mathsf{n}, \\ u'(t) &= H'z(t) + Jy(t) + Qr(t), \qquad\qquad u'(t) \in \mathbb{R}^{\mathsf{m}}, \end{aligned}$$

can be found such that $F' \in \mathbb{Z}^{\mathsf{n}'\times\mathsf{n}'}$, $u'(t) \equiv u(t)$, and $z(t) \equiv Tx(t)$ with some $T \in \mathbb{R}^{\mathsf{n}'\times\mathsf{n}}$. See [21, Section III.A] for more details.

III. Main Result

We first convert the given controller (5) to operate over integers in Section III-A, and propose the encrypted controller over $\mathbb{Z}_q$ together with a parameter design, in Section III-B.

A. Implementation over $\mathbb{Z}$

We begin with quantization of input signals to integers. Let the controller inputs $y(t) \in \mathbb{R}^{\mathsf{p}}$ and $r(t) \in \mathbb{R}^{\mathsf{q}}$ be quantized with a parameter $l(t) > 0$ of quantization level, as

$$\overline{y}(t) := \left\lceil \frac{y(t)}{l(t)} \right\rfloor \in \mathbb{Z}^{\mathsf{p}}, \quad \overline{r}(t) := \left\lceil \frac{r(t)}{l(t)} \right\rfloor \in \mathbb{Z}^{\mathsf{q}}. \tag{8}$$

Furthermore, let the rational matrix elements in (5) (except the state matrix $F \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$) be stored as integers, as

$$\overline{G} := \frac{G}{\mathsf{s}_1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{p}}, \quad \overline{P} := \frac{P}{\mathsf{s}_1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{q}},$$
$$\overline{H} := \frac{H}{\mathsf{s}_2} \in \mathbb{Z}^{\mathsf{m}\times\mathsf{n}}, \quad \overline{J} := \frac{J}{\mathsf{s}_1\mathsf{s}_2} \in \mathbb{Z}^{\mathsf{m}\times\mathsf{p}}, \ \overline{Q} := \frac{Q}{\mathsf{s}_1\mathsf{s}_2} \in \mathbb{Z}^{\mathsf{m}\times\mathsf{q}},$$

with some positive rational numbers $\mathsf{s}_1 \in \mathbb{Q}$ and $\mathsf{s}_2 \in \mathbb{Q}$.

Now, we propose the controller over $\mathbb{Z}$ be designed as

$$\overline{x}(t+1) = \frac{l(t)}{l(t+1)} \cdot (F\overline{x}(t) + \overline{G}\overline{y}(t) + \overline{P}\overline{r}(t)), \tag{9}$$
$$\overline{u}(t) = \overline{H}\overline{x}(t) + \overline{J}\overline{y}(t) + \overline{Q}\overline{r}(t), \quad \overline{x}(0) = \left\lceil \frac{x_0}{\mathsf{s}_1 l_0} \right\rfloor,$$

where the parameter $l(t)$ for quantization is chosen such that

$$l_{\mathsf{r}}(t) := \frac{l(t)}{l(t+1)} \in \mathbb{N}, \tag{10}$$

with some $l(0) = l_0 > 0$. We let a real-valued output that corresponds to that of (5) be obtained as

$$u_q(t) := \mathsf{s}_1\mathsf{s}_2 l(t) \cdot \overline{u}(t) \in \mathbb{R}^{\mathsf{m}}. \tag{11}$$

Clearly, the system (9) with (10) operates over $\mathbb{Z}$ using addition and multiplication only, where $l(t)$ is monotonically decreasing. Note that the parameter $l(t)$ determining the quantization level is fixed as constant while $l_{\mathsf{r}}(t) = 1$, and whenever $l_{\mathsf{r}}(t) > 1$, the quantization in (8) start keeping further lower bits of signals with an increased scale factor, and the factor $l_{\mathsf{r}}(t) \in \mathbb{N}$ is also multiplied to $\overline{x}(t)$ in (9) so that its scale matches with the increased level of quantization.

The performance of the controller (9) with (11) is equivalent to that of (5) with presence of quantization error. Define

$$x_q(t) := \mathsf{s}_1 l(t) \cdot \overline{x}(t) \in \mathbb{R}^{\mathsf{n}}. \tag{12}$$

Then, it can be easily verified that $x_q(t)$ and $u_q(t)$ obey

$$\begin{aligned} x_q(t+1) &= Fx_q(t) + G\left\lceil \frac{y(t)}{l(t)} \right\rfloor l(t) + P\left\lceil \frac{r(t)}{l(t)} \right\rfloor l(t) \\ &=: Fx_q(t) + Gy(t) + Pr(t) + e_x(t), \\ u_q(t) &= Hx_q(t) + J\left\lceil \frac{y(t)}{l(t)} \right\rfloor l(t) + Q\left\lceil \frac{r(t)}{l(t)} \right\rfloor l(t) \\ &=: Hx_q(t) + Jy(t) + Qr(t) + e_u(t), \end{aligned} \tag{13}$$

with $x_q(0) = \mathsf{s}_1 l_0 \lceil x_0/(\mathsf{s}_1 l_0) \rfloor =: x_0 + e_0$, where the errors $\{e_x(t), e_u(t)\}$ are bounded by a linear function of $l(t)$, as

$$\left\| \begin{bmatrix} e_x(t) \\ e_u(t) \end{bmatrix} \right\| \le \frac{1}{2} \left\| \begin{bmatrix} G & P \\ J & Q \end{bmatrix} \right\| l(t) =: M_e l(t), \tag{14}$$

and e_0 is such that $\|e_0\| \le (\mathsf{s}_1 l_0)/2$.

As a result, as stability of linear systems implies stability with respect to perturbations, the following lemma states that the designed controller (9) can ensure convergence of the closed-loop state to the equilibrium (7), as much as the quantization parameter $l(t)$ can be smaller, as time goes by.

Lemma 1: The controller (9) in the closed-loop ensures

$$\left\| \begin{bmatrix} x_p(t) - x_{p,\infty} \\ x_q(t) - x_\infty \end{bmatrix} \right\| \le M_{\mathsf{exp}} \lambda_{\mathsf{cl}}^t + M_{\mathsf{conv}} \sum_{\tau=0}^{t-1} \lambda_{\mathsf{cl}}^{t-1-\tau} l(\tau) =: \delta_x(t) \tag{15}$$

for all $t \ge 0$, where

$$M_{\mathsf{exp}} := \left(2M_0 + \frac{\mathsf{s}_1 l_0}{2}\right) M_{\mathsf{cl}}, \;\; M_{\mathsf{conv}} := M_e M_{\mathsf{cl}} \max\{\|B\|, 1\}.$$

Furthermore, if $\lim_{t\to\infty} l(t) = 0$, then $\lim_{t\to\infty} \delta_x(t) = 0$, $\lim_{t\to\infty} x_p(t) = x_{p,\infty}$, and $\lim_{t\to\infty} x_q(t) = x_\infty$. □

Proof: Let the closed-loop of (4) and (13) be re-written as

$$\begin{aligned} \xi(t+1) &:= \begin{bmatrix} x_p(t+1) - x_{p,\infty} \\ x_q(t+1) - x_\infty \end{bmatrix} \\ &= A_{\mathsf{cl}} \xi(t) + \begin{bmatrix} 0_{\mathsf{n}_p \times \mathsf{n}} & B \\ I_{\mathsf{n}} & 0_{\mathsf{n}\times\mathsf{m}} \end{bmatrix} \begin{bmatrix} e_x(t) \\ e_u(t) \end{bmatrix} \\ &=: A_{\mathsf{cl}} \xi(t) + B_e e(t), \end{aligned}$$

using (6) and (7), where $\|\xi(0)\| \le 2M_0 + (\mathsf{s}_1 l_0)/2$. Note that

$$\begin{aligned} \|\xi(t)\| &= \left\| A_{\mathsf{cl}}^t \xi(0) + \textstyle\sum_{\tau=0}^{t-1} A_{\mathsf{cl}}^{t-1-\tau} B_e e(\tau) \right\| \\ &\le \|A_{\mathsf{cl}}^t\| \cdot \|\xi(0)\| + \textstyle\sum_{\tau=0}^{t-1} \|A_{\mathsf{cl}}^{t-1-\tau}\| \cdot \|B_e\| \cdot \|e(\tau)\|. \end{aligned}$$

Then, from (14) and $\|A_{\mathsf{cl}}^t\| \le M_{\mathsf{cl}} \lambda_{\mathsf{cl}}^t$, we simply obtain (15). Next, suppose $\lim_{t\to\infty} l(t) = 0$ and $\epsilon > 0$ be given. Choose $t' \ge 0$ such that $l(t') \le \epsilon(1 - \lambda_{\mathsf{cl}})/(2M_{\mathsf{conv}})$. Then, we have

$$\begin{aligned} \delta_x(t) &\le M_{\mathsf{exp}} \lambda_{\mathsf{cl}}^t + M_{\mathsf{conv}} \textstyle\sum_{\tau=0}^{t'-1} \lambda_{\mathsf{cl}}^{t-1-\tau} l(\tau) + \frac{\epsilon}{2} \\ &\le M_{\mathsf{exp}} \lambda_{\mathsf{cl}}^t + M_{\mathsf{conv}} t' \lambda_{\mathsf{cl}}^{t-t'} l(0) + \frac{\epsilon}{2}, \quad \forall t \ge t', \end{aligned}$$

since $l(t)$ is monotonically decreasing. Now, we can choose $t'' \ge 0$ such that $\delta_x(t) \le \epsilon$, $\forall t \ge t''$. It ends the proof. ■

We have seen that asymptotic convergence is achieved for ideal cases when $\lim_{t\to\infty} l(t) = 0$, i.e., the quantization at (8) can be infinitesimally fine as time goes by. We note that Lemma 1 also considers cases in practice; when $l(t)$ stops decreasing and is fixed from time t^* as $l(t) \equiv l^*$, $\forall t \ge t^*$, then (15) implies "practical convergence" of the state, as

$$\limsup_{t\to\infty} \left\| \begin{bmatrix} x_p(t) - x_{p,\infty} \\ x_q(t) - x_\infty \end{bmatrix} \right\| \le \frac{M_{\mathsf{conv}}}{1 - \lambda_{\mathsf{cl}}} l^*, \tag{16}$$

where the bound is linear to the eventual quantization level.

B. Implementation over $\mathbb{Z}_q$ and Parameter Design

Now, for the sake of encrypted implementation, let us again convert the controller (9) to the system of the form (2), which operates over the message space $\mathbb{Z}_q$ based on modular arithmetic. In fact, as the controller (5) already operates over integers with addition and multiplication only, the conversion to the form (2) itself is straightforward, by simply defining

$$\begin{aligned} &\mathsf{F}(t) := l_{\mathsf{r}}(t) F \mod q, && \mathsf{H}(t) := \overline{H} \mod q, \\ &\mathsf{G}(t) := l_{\mathsf{r}}(t) \left[\overline{G}, \overline{P}\right] \mod q, && \mathsf{J}(t) := \left[\overline{J}, \overline{Q}\right] \mod q, \\ &\mathsf{y}(t) := \begin{bmatrix} \overline{y}(t) \\ \overline{r}(t) \end{bmatrix} \mod q, && \mathsf{x}_0 := \overline{x}(0) \mod q. \end{aligned} \tag{17}$$

This is because the modulo operation simply projects the integers to the set $\mathbb{Z}_q$ and it is compatible with addition and multiplication. Indeed, it can be easily shown that under the relation (17), the state $\mathsf{x}(t)$ and the output $\mathsf{u}(t)$ of (2) keep the remainders of $\overline{x}(t)$ and $\overline{u}(t)$ in (9) divided by q, as

$$\begin{aligned} \mathsf{x}(t) &= \overline{x}(t) \mod q, \\ \mathsf{u}(t) &= \overline{u}(t) \mod q, \end{aligned} \quad \forall t \ge 0. \tag{18}$$

But then, in order for the performance, the original output $\overline{u}(t) \in \mathbb{Z}^{\mathsf{m}}$ should be restored from the projected signal $\mathsf{u}(t) \in \mathbb{Z}_q^{\mathsf{m}}$; that is, the "upper bits" of $\overline{u}(t)$ cut off by the modulo operation should be recovered from the "lower bits" signal $\mathsf{u}(t)$. For this, the following lemma shows that, if the "variation" of the output $\overline{u}(t)$ is bounded by the modulus as[2]

$$\|\overline{u}(t+1) - l_{\mathsf{r}}(t)\overline{u}(t)\| < \frac{q}{2}, \quad \forall t \ge 0, \tag{19}$$

then the signal $\overline{u}(t)$ can be recovered from the information of $\{\mathsf{u}(\tau)\}_{\tau=0}^t$ and $\overline{u}(0)$.

Lemma 2: Consider the systems (2) and (9), with (17). Let a signal $\overline{u}_r(t)$ be defined from $\{\mathsf{u}(\tau)\}_{\tau=0}^t$ and $\overline{u}(0)$, as

$$\begin{aligned} &\overline{u}_r(0) = \overline{u}(0), \\ &\overline{u}_r(t) = \mathsf{u}(t) \mod (q,\; l_{\mathsf{r}}(t-1)\overline{u}_r(t-1)), \quad \text{for } t \ge 1. \end{aligned} \tag{20}$$

If (19) holds, then it satisfies $\overline{u}_r(t) = \overline{u}(t)$, for all $t \ge 0$. □

Proof: Suppose $\overline{u}_r(\tau) = \overline{u}(\tau)$ at some $\tau \ge 0$. From (19), note that all the components of $\overline{u}(\tau+1) - l_{\mathsf{r}}(\tau)\overline{u}(\tau) + \frac{q}{2} \cdot 1_{\mathsf{m}}$ are positive and less than q. Since (18) implies that $\mathsf{u}(\tau+1) = qv + \overline{u}(\tau+1)$ with some $v \in \mathbb{Z}^{\mathsf{m}}$, (1) and (20) imply that

$$\begin{aligned} \overline{u}_r(\tau+1) &= \mathsf{u}(\tau+1) - \left\lfloor \frac{\mathsf{u}(\tau+1) - l_{\mathsf{r}}(\tau)\overline{u}_r(\tau) + \frac{q}{2}\cdot 1_{\mathsf{m}}}{q} \right\rfloor q \\ &= \overline{u}(\tau+1) - \left\lfloor \frac{\overline{u}(\tau+1) - l_{\mathsf{r}}(\tau)\overline{u}_r(\tau) + \frac{q}{2}\cdot 1_{\mathsf{m}}}{q} \right\rfloor q \\ &= \overline{u}(\tau+1). \end{aligned}$$

Hence, $\overline{u}_r(t) = \overline{u}(t)$, $\forall t$, by induction. It ends the proof. ■

In (20), the value of $\overline{u}(t) = \overline{u}_r(t)$ is restored from $\overline{u}(t-1) = \overline{u}_r(t-1)$ and $\mathsf{u}(t)$, inductively. We also note that the initial value $\overline{u}(0)$ can also be recovered from $\mathsf{u}(0)$, by

$$\overline{u}(0) = \mathsf{u}(0) \mod (q, 0_{\mathsf{m}\times 1}) \tag{21}$$

as long as $\|\overline{u}(0)\| < \frac{q}{2}$; i.e., as long as q is chosen such that

$$\begin{aligned} \|\overline{u}(0)\| &= \frac{1}{\mathsf{s}_1 \mathsf{s}_2 l(0)} \|H x_q(0) + JC x_p(0) + Q r(0) + e_u(0)\| \\ &\le \frac{\|[H, JC, Q]\| M_0}{\mathsf{s}_1 \mathsf{s}_2 l_0} + \frac{\|H\|}{2\mathsf{s}_2} + \frac{M_e}{\mathsf{s}_1 \mathsf{s}_2} < \frac{q}{2}. \end{aligned} \tag{22}$$

[2]The ratio $l_r(t)$ from (10) considers the relative scale difference between the outputs $\overline{u}(t+1)$ and $\overline{u}(t)$, as in (9).

So far, we have argued that the designed controller over $\mathbb{Z}_q$ can keep the same performance of (9) when the condition (19) holds, which we re-write for real output using (11), as

$$\frac{\|u_q(t+1)-u_q(t)\|}{l(t+1)} < \mathsf{s}_1\mathsf{s}_2\frac{q}{2}, \quad \forall t \geq 0. \tag{23}$$

So, we provide a condition for the parameter $\{l(t)\}_{t=0}^{\infty}$ under which the left-hand-side of (23) is bounded, so that the choice of q will guarantee that (19) holds. Let an upper bound for the left-hand-side calculated from (13), (14), and (15), as

$$\begin{aligned}
&\frac{\|u_q(t+1)-u_q(t)\|}{l(t+1)} \\
&= \frac{1}{l(t+1)}\left\| \begin{bmatrix} JC & H \end{bmatrix} \begin{bmatrix} x_p(t+1)-x_p(t) \\ x_q(t+1)-x_q(t) \end{bmatrix} + e_u(t+1)-e_u(t) \right\| \\
&\leq \left\| \begin{bmatrix} JC & H \end{bmatrix} \right\| \cdot \left(\frac{\delta_x(t+1)+\delta_x(t)}{l(t+1)} \right) + M_e(1+l_{\mathsf{r}}(t)) \\
&\leq \left\| \begin{bmatrix} JC & H \end{bmatrix} \right\| \cdot \left(\frac{2\delta_x(t)}{l(t+1)} + M_{\mathsf{conv}} l_{\mathsf{r}}(t) \right) + M_e(1+l_{\mathsf{r}}(t)) \\
&=: M_\delta \frac{\delta_x(t)}{l(t+1)} + M_l l_{\mathsf{r}}(t) + M_e.
\end{aligned} \tag{24}$$

Next, let the ratio $l_{\mathsf{r}}(t)$ in (24) from (10) be bounded as

$$l_{\mathsf{r}}(t) \leq l'_{\mathsf{r}}, \qquad \forall t \geq 0, \quad \text{with some} \;\; l'_{\mathsf{r}} \in \mathbb{N}, \tag{25}$$

so that the remaining task is to have the term

$$\frac{\delta_x(t)}{l(t+1)} = \frac{M_{\mathsf{exp}}\lambda_{\mathsf{cl}}^t + M_{\mathsf{conv}}\sum_{\tau=0}^{t-1}\lambda_{\mathsf{cl}}^{t-1-\tau} l(\tau)}{l(t+1)} \tag{26}$$

in (24) bounded; considering the convergence rate λ_{cl}^t, we propose that the parameter $\{l(t)\}_{t=0}^{\infty}$ be chosen to satisfy

$$\exists\, \tau_{\mathsf{d}} \in \mathbb{N} \;\; \text{such that} \;\; \frac{l(t)}{l(t+\tau_{\mathsf{d}})} \leq \left(\frac{1}{\lambda_{\mathsf{d}}}\right)^{\tau_{\mathsf{d}}}, \;\; \forall t \geq 0, \tag{27}$$

with some λ_{d} such that $\lambda_{\mathsf{cl}} < \lambda_{\mathsf{d}} < 1$, which will limit the increase of the factor $1/l(t)$ for each period of length τ_d.

As a result, the following lemma states that the constraint (27) for quantization ensures that the term (26) in (24) be bounded, so the condition (19) for Lemma 2 can be satisfied.

Lemma 3: If the parameter $\{l(t)\}_{t=0}^{\infty}$ satisfies (27), then

$$\frac{\delta_x(t)}{l(t+1)} \leq \frac{1}{\lambda_{\mathsf{d}}^{1+\tau_{\mathsf{d}}}} \left(\frac{M_{\mathsf{exp}}}{l_0} + \frac{M_{\mathsf{conv}}}{\lambda_{\mathsf{d}}-\lambda_{\mathsf{cl}}} \right). \tag{28}$$

□

Proof: Note that (27) implies $(l(t)/l(t+k)) \leq 1/(\lambda_{\mathsf{d}})^{k+\tau_{\mathsf{d}}}$, for all $t \geq 0$ and $k \geq 0$, so that it follows from (26) that

$$\frac{\delta_x(t)}{l(t+1)} \leq \frac{M_{\mathsf{exp}}\lambda_{\mathsf{cl}}^t}{l_0\lambda_{\mathsf{d}}^{t+1+\tau_{\mathsf{d}}}} + \frac{M_{\mathsf{conv}}}{\lambda_{\mathsf{d}}^{2+\tau_{\mathsf{d}}}} \sum_{\tau=0}^{t-1} \frac{\lambda_{\mathsf{cl}}^{t-1-\tau}}{\lambda_{\mathsf{d}}^{t-1-\tau}}.$$

Since $\lambda_{\mathsf{cl}}/\lambda_{\mathsf{d}} < 1$, and $\sum_{\tau=0}^{t-1}(\lambda_{\mathsf{cl}}/\lambda_{\mathsf{d}})^{t-1-\tau} \leq (\lambda_{\mathsf{d}}/(\lambda_{\mathsf{d}} - \lambda_{\mathsf{cl}}))$, for all $t \geq 0$, it completes the proof. ■

Remark 1: An easy way to ensure the condition (27) is to introduce "dwell-time" for the signal $l(t)$; let l'_{r} and λ_{d} be first chosen such that $(l(t)/l(t+1)) \leq l'_{\mathsf{r}}$ and $\lambda_{\mathsf{cl}} < \lambda_{\mathsf{d}} < 1$, and let the time constant $\tau_{\mathsf{d}} \in \mathbb{N}$ be chosen such that

$$\tau_{\mathsf{d}} \geq \frac{\log l'_{\mathsf{r}}}{\log \frac{1}{\lambda_{\mathsf{d}}}}, \qquad \text{so that} \quad \left(\frac{1}{\lambda_{\mathsf{d}}}\right)^{\tau_{\mathsf{d}}} \geq l'_{\mathsf{r}}.$$

And, we use the constant τ_{d} for dwell-time of $l(t)$, so that

$$\text{if } l(t+1) < l(t), \;\; \text{then } l(t+1) = l(t+2) = \cdots = l(t+\tau_{\mathsf{d}})$$

holds. Then, it can be easily verified that (27) is satisfied. □

Finally, we choose the modulus q for the plaintext space $\mathbb{Z}_q$, and state the main result of asymptotic stabilization over encrypted data with fixed modulus. Let q be chosen such that

$$\frac{M_\delta}{\mathsf{s}_1\mathsf{s}_2\lambda_{\mathsf{d}}^{1+\tau_{\mathsf{d}}}} \left(\frac{M_{\mathsf{exp}}}{l_0} + \frac{M_{\mathsf{conv}}}{\lambda_{\mathsf{d}}-\lambda_{\mathsf{cl}}} \right) + \frac{M_l l'_{\mathsf{r}} + M_e}{\mathsf{s}_1\mathsf{s}_2} < \frac{q}{2} \tag{29}$$

and (22) hold, considering the arguments (23), (24), and (28).

And, through the proposed conversion of the given controller (5) to the form (9) over $\mathbb{Z}$, and to the form (2) over $\mathbb{Z}_q$, the controller over the ciphertext space $\mathcal{C}$ is designed as

$$\begin{bmatrix} \mathbf{x}(t+1) \\ \mathbf{u}(t) \end{bmatrix} = \begin{bmatrix} \mathsf{F}(t) & \mathsf{G}(t) \\ \mathsf{H} & \mathsf{J} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x}(t) \\ \mathbf{y}(t) \\ \mathbf{r}(t) \end{bmatrix} \tag{30}$$

with (17), where $\mathbf{x}(t) \in \mathcal{C}^{\mathsf{n}}$ is the encrypted state with the initial value $\mathbf{x}(0) = \mathsf{Enc}(\lceil x_0/(\mathsf{s}_1 l_0) \rfloor \bmod q)$, $\mathbf{y}(t) \in \mathcal{C}^{\mathsf{p}}$ and $\mathbf{r}(t) \in \mathcal{C}^{\mathsf{q}}$ are the plant output and reference encrypted as

$$\mathbf{y}(t) = \mathsf{Enc}\left(\left\lceil \frac{y(t)}{l(t)} \right\rfloor \bmod q \right), \;\; \mathbf{r}(t) = \mathsf{Enc}\left(\left\lceil \frac{r(t)}{l(t)} \right\rfloor \bmod q \right),$$

respectively, $\mathbf{u}(t) \in \mathcal{C}^{\mathsf{m}}$ is the controller output, and the operation $\cdot$ is defined over the space $\mathcal{C}$. The plant input $u(t) \in \mathbb{R}^{\mathsf{m}}$ is restored from the decryption of $\mathbf{u}(t)$, as

$$\begin{aligned}
u(0) &= \mathsf{s}_1\mathsf{s}_2 l_0 \cdot (\mathsf{Dec}(\mathbf{u}(0)) \mod (q, 0_{\mathsf{m}\times 1})) \\
u(t) &= \mathsf{s}_1\mathsf{s}_2 l(t) \cdot \left(\mathsf{Dec}(\mathbf{u}(t)) \mod \left(q, \frac{u(t-1)}{\mathsf{s}_1\mathsf{s}_2 l(t)} \right) \right),
\end{aligned} \tag{31}$$

analogously to (21) and (20) with the relation (11) considered. We assume that the previous output $u(t-1)$ is stored at the decryption device and used for the recovery of $u(t)$.

Putting all together, the main theorem is stated as follows.

Theorem 1: Consider the closed-loop of the plant (4) and the encrypted controller (30) with (31). The constraints (22), (27), and (29) for the parameters $l(t)$ and q guarantee that

$$\begin{aligned}
\|x_p(t) - x_{p,\infty}\| &\leq M_{\mathsf{exp}}\lambda_{\mathsf{cl}}^t + M_{\mathsf{conv}} \sum_{\tau=0}^{t-1} \lambda_{\mathsf{cl}}^{t-1-\tau} l(\tau) = \delta_x(t), \\
\|u(t) - u_\infty\| &\leq \|[JC, H]\| \delta_x(t) + M_e l(t), \qquad \forall t \geq 0,
\end{aligned}$$

hold, where $u_\infty := JCx_{p,\infty} + Hx_\infty + Qr_\infty$. Furthermore,

$$\lim_{t\to\infty} x_p(t) = x_{p,\infty} \quad \text{and} \quad \lim_{t\to\infty} u(t) = u_\infty$$

are guaranteed, in case $\lim_{t\to\infty} l(t) = 0$ holds. □

Proof: Consider the closed-loop of (4) and (9) as an auxiliary system with the plant input obtained as (11). From (30), let $\mathsf{x}(t) := \mathsf{Dec}(\mathbf{x}(t))$ and $\mathsf{u}(t) := \mathsf{Dec}(\mathbf{u}(t))$. They obey

$$\begin{aligned}
\mathsf{x}(t+1) &= l_{\mathsf{r}}(t) \cdot (F\mathsf{x}(t) + \overline{G}\overline{y}(t) + \overline{P}\overline{r}(t)) \mod q \\
\mathsf{u}(t) &= \overline{H}\mathsf{x}(t) + \overline{J}\overline{y}(t) + \overline{Q}\overline{r}(t) \mod q
\end{aligned}$$

with $\mathsf{x}(0) = \lceil x_0/(\mathsf{s}_1 l_0) \rfloor \bmod q$, by Proposition 1. With the auxiliary system, we claim that the output $u(t)$ from (31) satisfies $u(t)/(\mathsf{s}_1\mathsf{s}_2 l(t)) = \overline{u}(t)$, $\forall t \geq 0$. First, from (31), the

constraint (22) ensures $u(0)/(\mathsf{s}_1\mathsf{s}_2 l_0) = \overline{u}(0)$. Then, according to Lemma 2, the claim is true if the auxiliary system satisfies the condition (19), since $\overline{u}_r(t) := u(t)/(\mathsf{s}_1\mathsf{s}_2 l(t))$ obeys (20) with $u(t-1)/(\mathsf{s}_1\mathsf{s}_2 l(t)) = l_{\mathsf{r}}(t-1)\overline{u}_r(t-1)$. Thus, we show that the condition (23) holds, which is equivalent to (19). Note that (23) holds if (28) and (29) hold, according to (24). Then, the constraints (27) and (29) ensure that (23) holds, since (27) implies (28) by Lemma 3. Therefore, $u(t)/(\mathsf{s}_1\mathsf{s}_2 l(t)) = \overline{u}(t)$ and $u(t) = u_q(t)$, $\forall t \geq 0$. Finally, Lemma 1 with (13), (12), and (14) completes the proof, since $u_q(t) - u_\infty = JC(x_p(t) - x_{p,\infty}) + H(x_q(t) - x_\infty) + e_u(t)$. ■

Note that, while Theorem 1 guarantees convergence of the plant state $x_p(t)$ to the equilibrium, the proposed controller computes only "lower bits" of the state without computing the upper bits, because of the constraint that the modulus q is fixed and finite. Indeed, the message $\mathsf{Dec}(\mathbf{x}(t)) = \overline{x}(t) \mod q$ of the state keeps only lower bits of the state $\overline{x}(t)$ of the model (9). Nonetheless, the parameter $l(t)$ is scheduled such that, the controller moves the computation scope further lower (i.e., the quantization level becomes finer by $l(t) > l(t+1)$, with the same modulus q) only when the corresponding upper bits have converged. Thus, the real output $u(t)$ converging to the u_∞ can be restored by (31).

We also note that Theorem 1 considers cases in practice just as in (16); if $l(t) \equiv l^* > 0$ from some $t \geq t^*$, then

$$\limsup_{t\to\infty} \|x_p(t) - x_{p,\infty}\| \leq \frac{M_{\mathsf{conv}}}{1 - \lambda_{\mathsf{cl}}} l^*.$$

IV. Conclusion

We have proposed an implementation method for linear dynamic controllers over encrypted data, which maintains asymptotic convergence of the controlled trajectories. The controller state matrix consisting of integers ensures that the dynamics for the lower bits of the controller state is well defined with modular arithmetic, so that it can generate the same lower bits of the output without computing the upper bits. As a result, it not only allows the operation over encrypted data to be continued for an infinite time horizon using only addition and multiplication over integers, but also achieves asymptotic convergence of the trajectories, as fine as the time-varying quantization can be performed in the end.

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 Systems Magazine*, 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 Conference on Decision and Control*, 2015, pp. 6836–6843.

[3] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," *IFAC-PapersOnline*, vol. 49, iss. 22, pp. 175–180, 2016.

[4] F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Engineering Practice*, vol. 67, pp. 13–20, 2017.

[5] M. Schulze Darup, A. Redder, and D E. Quevedo, "Encrypted cloud-based MPC for linear systems with input constraints," *IFAC-PapersOnLine*, Vol. 51, no. 20, Pp. 535–542, 2018.

[6] 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 Transactions on Automatic Control*, vol. 66, no. 5, pp. 2357–2364, 2021.

[7] A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Encrypted distributed lasso for sparse data predictive control," in *Proc. 60th IEEE Conference on Decision and Control*, 2021, pp. 4901–4906.

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

[9] S. Schlor, M. Hertneck, S. Wildhagen, and F. Allgöwer, "Multi-party computation enables secure polynomial control based solely on secret-sharing," in *Proc. 60th IEEE Conference on Decision and Control*, 2021, pp. 4882–4887.

[10] T. Hossienalizadeh, F. Turkmen, and N. Monshizadeh, "Private computation of polynomials over networks," in *Proc. 60th IEEE Conference on Decision and Control*, 2021, pp. 4895–4900.

[11] C. N. Hadjicostis and A. D. Domínguez-García, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3887–3894, 2020.

[12] 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.

[13] M. P. Chaher, B. Jayawardhana, and J. Kim, "Homomorphic encryption-enabled distance-based distributed formation control with distance mismatch estimators," in *Proc. 60th IEEE Conference on Decision and Control*, 2021, pp. 4915–4922.

[14] W. E. Curran, C. A. Rojas, L. Bobadilla, and D. A. Shell, "Oblivious sensor fusion via secure multi-party combinatorial filter evaluation," in *Proc. 60th IEEE Conference on Decision and Control*, 2021, pp. 5620–5627.

[15] A. Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. Srivastava, "Proloc: Resilient localization with private observers using partial homomorphic encryption," in *Proc. 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2017, pp. 41–52.

[16] C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semi-homomorphic encryption," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3950–3957, 2020.

[17] 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 Conference on Decision and Control*, 2018, pp. 5020–5025.

[18] N. Schlüter and M. Schulze Darup, "On the stability of linear dynamic controllers with integer coefficients," *IEEE Transactions on Automatic Control*, doi: 10.1109/TAC.2021.3131126.

[19] N. Schlüter, M. Neuhaus, and M. Schulze Darup,"Encrypted dynamic control with unlimited operating time via FIR filters," in *Proc. European Control Conference*, 2021, pp. 952–957.

[20] 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 Conference on Decision and Control*, 2021, pp. 5614–5619.

[21] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Transactions on Automatic Control*, doi: 10.1109/TAC.2022.3142124.

[22] R. Fritz, M. Fauser, and P. Zhang, "Controller encryption for discrete event systems," in *Proc. American Control Conference*, 2019, pp. 5633–5638.

[23] K. Teranishi, N. Shimada, and K. Kogiso, "Stability analysis and dynamic quantizer for controller encryption," in *Proc. 58th Conference on Decision and Control*, 2019, pp. 7184–7189.

[24] N. Genise, C. Gentry, S. Halevi, B. Li, and D. Micciancio, "Homomorphic encryption for finite automata," in *Proc. Advances in Cryptology – ASIACRYPT*, 2019, pp. 473–502.

[25] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. STOC*, vol. 9, 2009, pp. 169–178.

[26] R. W. Brockett and D. Liberzon, "Quantized feedback stabilization of linear systems," *IEEE Transactions on Automatic Control*, vol. 45, no. 7, pp. 1279–1289, 2000.

[27] G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans, "Feedback control under data rate constraints: an overview," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 108–137, 2007.