2021 60th IEEE Conference on Decision and Control (CDC)
December 13-15, 2021. Austin, Texas

Method for Running Dynamic Systems over Encrypted Data for Infinite Time Horizon without Bootstrapping and Re-encryption

Junsoo Kim, Hyungbo Shim, Henrik Sandberg, and Karl H. Johansson

2021 60th IEEE Conference on Decision and Control (CDC) | 978-1-6654-3659-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDC45484.2021.9682828

***Abstract*— In this paper, we propose a method for dynamic systems to operate over homomorphically encrypted data for an infinite time horizon, where we do not make use of reset, re-encryption, or bootstrapping for the encrypted messages. The given system is first decomposed into the stable part and the anti-stable part. Then, the stable part is approximated to have finite impulse response, and by a novel conversion scheme, the eigenvalues of the state matrix of the anti-stable part are approximated to algebraic integers. This allows that the given system can be implemented to operate for an infinite time horizon using only addition and multiplication over encrypted data, without re-encrypting any portion of data. The performance error caused by the approximation and quantization can be made arbitrarily small, with appropriate choice of parameters.**

I. Introduction

As a countermeasure for the threat of cyber-attacks on networked control system, the notion of encrypted control has been introduced, to conceal and protect control data from third parties of malicious adversaries [1]–[4]. It aims for control operation directly performed over encrypted signals and parameters via homomorphic encryption, which allows arithmetic operation over encrypted messages without decryption. By doing so, all control data can be protected by encryption thoroughly, while they are encrypted at sensors, processed at computing devices, and eventually transmitted and decrypted at actuators. Security problems are being regarded as more and more urgent in most applications that involve network communication, so the use of homomorphic encryption have been introduced for more and more methods and algorithms, for example, for model predictive control [5], [6], optimization problems [7], average consensus or distributed aggregation [8]–[10], quantized control [11], reset control [12], and learning based control [13], [14].

Since bootstrapping techniques of fully homomorphic encryption has been developed in [15], it has been known that any sort of arithmetic or logical functions can be implemented and applied to encrypted variables, an unlimited number of times. Nonetheless, as it may require a substantial amount of computational resource, the use of bootstrapping has not been widely considered for real-time control operation. Instead, only the abilities of performing addition and multiplication over encrypted data have been exploited.

But then, the sort of operations or the number of operations that is allowed for encrypted messages becomes limited, and it makes the implemented systems or circuits over encrypted data incapable of operating for an infinite time horizon. The most representative case would be running a linear dynamic system, in which recursive multiplication by non-integer numbers as well as rounding operation for discarding least significant digits is required in most cases, so that it is also incapable of operating over encrypted data, as it is. For more details, see [16, Section II-D] or [17, Section III].

This problem has been a common concern in the initial studies on encrypted control, and most results that consider dynamic operation over encrypted data have admitted assumptions for "refreshing the state". More specifically, re-encryption of the state (as in [2]), reset of the state (as in [12]), or use of the bootstrapping (as in [4]) has been assumed, where each of them causes shortcomings of requiring additional communication resources, causing performance degradation, and requiring substantial computational resources, respectively. In [16], a method making use of re-encryption of system output is proposed instead of the whole system state, which re-encrypts a smaller portion of data, but it still relies on the presence of decryption key to have the system operate for an infinite time horizon.

In this paper, we propose a method for dynamic systems to operate over encrypted data for an infinite time horizon, which does not assume the use of reset, re-encryption, or bootstrapping for any portion of encrypted messages. The given system is first decomposed into the stable part and the anti-stable part. Motivated from the observation made in [16] and [17] that linear systems whose state matrix consisting of integers can be implemented to operate for an infinite time horizon without re-encryption, the stable part of system is approximated to have finite impulse response so that the state matrix becomes a nilpotent matrix consisting of zeros and ones. And, we propose a novel method for the anti-stable part of system, which first approximates the eigenvalues of state matrix to algebraic integers[1] and then converts the system to a periodically time-varying system which has the state matrices consisting of integers. Then, we show that the converted system can be implemented using only addition

This work was supported in part by the National Research Foundation of Korea(NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. NRF-2017R1E1A1A03070342), 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, H. Sandberg, and K. H. Johansson are with the Division of Decision and Control System, KTH Royal Institute of Technology, Sweden. They are also affiliated with Digital Futures.

H. Shim is with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Korea.

[1] An algebraic integer is a complex number which is a root of a monic polynomical having the coefficients as integer.

and multiplication over integers (quantized numbers), so that it can operate over encrypted data for an infinite time horizon without re-encryption or bootstrapping. Finally, it will be seen that the performance error due to the approximations as well as quantization can be made arbitrarily small, by appropriate choice of parameters.

The rest of this paper is organized as follows. Section II begins with preliminaries and problem formulation. Section III presents the main result on running dynamic systems over encrypted data. Finally, Section IV concludes the paper.

Notation: The set of integers, positive integers, non-negative integers, real numbers, and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{R}$, and $\mathbb{C}$, respectively. The floor function, rounding function, and ceiling function are denoted by $\lfloor\cdot\rfloor$, $\lceil\cdot\rfloor$, and $\lceil\cdot\rceil$, respectively. We define $a \mod q := a - \lfloor \frac{a}{q} \rfloor q$ for $a \in \mathbb{Z}$ and $q \in \mathbb{N}$, and the set of integers modulo q is denoted by $\mathbb{Z}_q := \{0, 1, \cdots, q-1\}$. We make use of the functions, such as $\lceil\cdot\rfloor$ or $(\cdot \mod q)$, defined for scalars, as component-wise functions for vectors and matrices, as well. We let $|\cdot|$ denote the absolute value of a complex number, let $\angle(\cdot)$ denote the angle of a non-zero complex number, and let $\|\cdot\|$ denote the infinity norm of a vector or a matrix. For a sequence $u_1, \cdots, u_m$ of column vectors or scalars, we define $\mathrm{col}\{u_i\}_{i=1}^m := [u_1; u_2; \cdots; u_m] := [u_1^\top, \cdots, u_m^\top]^\top$. For $m \in \mathbb{N}$ and $n \in \mathbb{N}$, we let $0_{m\times n} \in \mathbb{R}^{m\times n}$ denote the zero matrix, and $I_n \in \mathbb{R}^{n\times n}$ denote the identity matrix.

II. Preliminaries and Problem Formulation

A. Homomorphic Encryption

Consider a cryptosystem denoted by $(\mathbb{Z}_q, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec})$, where $\mathbb{Z}_q$ is the space of plaintexts (unencrypted data) with modulus $q \in \mathbb{N}$, $\mathcal{C}$ is the space of ciphertexts (encrypted data), and $\mathsf{Enc} : \mathbb{Z}_q \to \mathcal{C}$ and $\mathsf{Dec} : \mathcal{C} \to \mathbb{Z}_q$ are the encryption and decryption algorithms[2], respectively. We abuse notation and let $\mathsf{Enc} : \mathbb{Z}_q^n \to \mathcal{C}^n$ and $\mathsf{Dec} : \mathcal{C}^n \to \mathbb{Z}_q^n$, $n \in \mathbb{N}$, be regarded component-wise algorithms for vectors.

Throughout the paper, the cryptosystem is assumed to be additively homomorphic; i.e., to satisfy 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 property H2 means that the cryptosystem can perform addition directly over encrypted messages, and H3 means the ability of performing constant multiplication over ciphertexts, where the multiplier is unencrypted. We abuse notation and use $\mathbf{c}_1 + \mathbf{c}_2 := \mathsf{Add}_n(\mathbf{c}_1, \mathbf{c}_2)$ for $\mathbf{c}_1 \in \mathcal{C}^n$ and $\mathbf{c}_2 \in \mathcal{C}^n$, and $K \cdot \mathbf{c} := \mathsf{IntMult}_{m,n}(K, \mathbf{c})$ for $K \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{c} \in \mathcal{C}^n$.

As typical examples of additively homomorphic encryption, Paillier cryptosystem [18] or cryptosystems based on the Learning With Errors (LWE) problem, such as [19] or [20], can be considered. Regarding the latter, the case of using LWE-based cryptosystems, the presence of "injected errors" should be considered in practice, as they satisfy H1–H3 with small errors (see [16] or [21] for details). But in this paper, we omit the argument of error effect, for simplicity.

[2]We omit the arguments of encryption and decryption key, for simplicity.

B. Problem Formulation

Consider a linear time-invariant system, given as

$$\begin{aligned} x(t+1) &= Fx(t) + Gy(t) + e_x(t), \quad x(0) = x_0 + e_{x,0}, \\ u(t) &= Hx(t) + Jy(t) + e_u(t), \quad t = 0, 1, 2, \cdots, \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^{\mathsf{n}}$ is the state, $y(t) \in \mathbb{R}^{\mathsf{p}}$ is the input, and $u(t) \in \mathbb{R}^{\mathsf{m}}$ is the output of the system, respectively, and $x_0 \in \mathbb{R}^{\mathsf{n}}$ is the initial state, and $e_x(t) \in \mathbb{R}^{\mathsf{n}}$, $e_u(t) \in \mathbb{R}^{\mathsf{m}}$, and $e_{x,0} \in \mathbb{R}^{\mathsf{n}}$ denote perturbations. For the ideal case, i.e., the case that $e_x(t) \equiv 0$, $e_u(t) \equiv 0$, and $e_{x,0} = 0$, the input, state, and output are denoted as $\{y'(t), x'(t), u'(t)\}$, respectively.

Assuming that the system (1) is a part of stable closed-loop system, we make two mild assumptions, as follows[3]:

A1: The input, state, and output of (1) for the ideal case are bounded; there exists $M > 0$, which is known, such that $\|[y'(t); x'(t); u'(t)]\| \le M$, for all $t \in \mathbb{N}_0$. Especially for the output $u'(t) =: \mathrm{col}\{u'_i(t)\}_{i=1}^{\mathsf{m}}$, we let

$$u_i^{\min} \le u'_i(t) \le u_i^{\max}, \quad \forall t \in \mathbb{N}_0,\ \forall i = 1, \cdots, \mathsf{m}, \tag{2}$$

with some real numbers $\{u_i^{\min}\}_{i=1}^{\mathsf{m}}$ and $\{u_i^{\max}\}_{i=1}^{\mathsf{m}}$.

A2: The trajectories $\{y'(t), x'(t), u'(t)\}$ of (1) are stable with respect to the perturbations $\{e_{x,0}, e_x(t), e_u(t)\}$; for any $\epsilon > 0$, there exists a constant $\eta_x > 0$ such that if $\sup_t(\|[e_x(t); e_u(t); e_{x,0}]\|) \le \eta_x$, then[4] $\|y(t) - y'(t)\| \le \epsilon$, $\|x(t) - x'(t)\| \le \epsilon$, and $\|u(t) - u'(t)\| \le \epsilon$, $\forall t \in \mathbb{N}_0$.

Given the system (1) with the real matrices $\{F, G, H, J\}$ and $x_0 \in \mathbb{R}^{\mathsf{n}}$, the objective of this paper is to implement (1) with a digital computer, to operate over encrypted data. Regarding quantization for digital implementation, let the input $y(t) \in \mathbb{R}^{\mathsf{p}}$ of (1) be quantized and encoded as

$$\overline{y}(t) := \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor \mod q, \tag{3}$$

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

$$\mathbf{y}(t) := \mathsf{Enc}(\overline{y}(t)) \in \mathcal{C}^{\mathsf{p}}. \tag{4}$$

Then, the problem is to construct a dynamic system defined over the space $\mathcal{C}$ which satisfies the followings:

- It receives the signal $\mathbf{y}(t) \in \mathcal{C}^{\mathsf{p}}$ as input, and computes its next state and its output $\mathbf{u}(t) \in \mathcal{C}^{\mathsf{m}}$, using only the operations Add_n and $\mathsf{IntMult}_{m,n}$ of H2 and H3.
- The performance of the constructed system is equivalent to that of (1); for any $\epsilon > 0$, the parameters of the system can be chosen so that it guarantees $\|g(\mathsf{Dec}(\mathbf{u}(t))) - u'(t)\| \le \epsilon$ for all $t \in \mathbb{N}_0$, with some function $g : \mathbb{Z}_q^{\mathsf{m}} \to \mathbb{R}^{\mathsf{m}}$ for the decrypted output.

[3]Note that we do not assume that the system (1) itself is a stable system.

[4]The perturbations $\{e_x(t), e_u(t), e_{x,0}\}$ may affect the value of the input $y(t)$ of (1) as well, in case the system (1) is a part of closed-loop system.

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

III. Main Result

It has been observed, as in [17], that linear systems having the state matrix as integers can be implemented to operate over ciphertexts, for an infinite time horizon. Motivated from this idea, the approach of this paper is *to convert the given linear time-invariant system* (1) *to a linear time-varying system having the state matrices consisting of integers*, which has practically the same input-output relation, and then implement the converted system to operate over ciphertexts.

Consider a linear time-varying system of the form

$$v(t+1) = F_v(t)v(t) + G_v(t)y(t) + e_v(t), \tag{5a}$$
$$u_v(t) = H_v(t)v(t) + J_v(t)y(t) + e_u(t), \tag{5b}$$
$$v(0) = v_0 + e_{v,0}$$

where $v(t) \in \mathbb{R}^{\mathsf{n}_v}$, $\mathsf{n}_v \in \mathbb{N}$, is the state with the initial value $v_0 \in \mathbb{R}^{\mathsf{n}_v}$, $y(t) \in \mathbb{R}^{\mathsf{p}}$ is the same input with (1), $u_v(t) \in \mathbb{R}^{\mathsf{m}}$ is the output, $\{e_v(t), e_u(t), e_{v,0}\}$ are the perturbations, and $\{F_v(t), G_v(t), H_v(t), J_v(t)\}_{t=1}^{\infty}$ are time-varying matrices which consist of a finite set of matrices.

In Section III-A, we first propose a method for converting the given system (1) to the form (5), which has practically the same input-output relation with that of (1), subject to the constraint that the converted system (5) should have the state matrix as integers, i.e., have $F_v(t) \in \mathbb{Z}^{\mathsf{n}_v \times \mathsf{n}_v}$ for all $t \in \mathbb{N}_0$. Then, we demonstrate the validity of the proposed approach; it will be seen in Section III-B that the converted system (5) with the condition $F_v(t) \in \mathbb{Z}^{\mathsf{n}_v \times \mathsf{n}_v}$ can be implemented to operate over encrypted data for the infinite time horizon.

A. Conversion to System having State Matrix as Integers

We consider decomposition of the system (1) to stable part and anti-stable part, by a transformation to the real Jordan form; with an invertible matrix $W = [W_1^\top, W_2^\top]^\top \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$ such that $z_1(t) = W_1 x(t) \in \mathbb{R}^{\mathsf{n}_1}$ and $z_2(t) = W_2 x(t) \in \mathbb{R}^{\mathsf{n}_2}$ where $\mathsf{n}_1 + \mathsf{n}_2 = \mathsf{n}$, the system (1) is transformed as the form

$$z_1(t+1) = F_1 z_1(t) + G_1 y(t) + e_{z_1}(t), \tag{6a}$$
$$z_2(t+1) = F_2 z_2(t) + G_2 y(t) + e_{z_2}(t), \tag{6b}$$
$$u(t) = H_1 z_1(t) + H_2 z_2(t) + J y(t) + e_u(t), \tag{6c}$$
$$z_1(0) = W_1 x_0 + e_{z_1,0}, \quad z_2(0) = W_2 x_0 + e_{z_2,0},$$

where we let the matrix $F_1 \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$ be anti-stable, i.e., every eigenvalue $\lambda_1 \in \mathbb{C}$ of F_1 is such that $|\lambda_1| \geq 1$, and let the matrix $F_2 \in \mathbb{R}^{\mathsf{n}_2\times\mathsf{n}_2}$ be strictly stable, i.e., every eigenvalue $\lambda_2 \in \mathbb{C}$ of F_2 is such that $|\lambda_2| < 1$, and $\{e_{z_1}(t), e_{z_2}(t), e_{z_1,0}, e_{z_2,0}\}$ are the perturbations with respect to the states $z_1(t)$ and $z_2(t)$.

In this section, we present a scheme for converting the system (6) to the form (5) having the state matrices consisting of integers, in which the conversion for the part (6a) is based on a novel approximation method for the eigenvalues of the matrix F_1, and the part (6b) is proposed to be approximated to have finite impulse response.

First, we make use the following lemma to convert the part (6a), which implies that an anti-stable matrix can be slightly perturbed by a small error, so that one of its powers can be transformed to a matrix consisting of integers.

Lemma 1: For any $\alpha > 0$ and an anti-stable matrix $F_1 \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$, there exist $F_p \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$, $T \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$, and $k_1 \in \mathbb{N}$ such that $\|F_1 - F_p\| \leq \alpha$ and $TF_p^{k_1}T^{-1} \in \mathbb{Z}^{\mathsf{n}_1\times\mathsf{n}_1}$. □

Sketch of Proof: For a complex number $\lambda = \sigma + i\omega \in \mathbb{C}$ with $\sigma \in \mathbb{R}$, $\omega \in \mathbb{R}$, and $i^2 = -1$, define $\lceil\lambda\rfloor := \lceil\sigma\rfloor + i\lceil\omega\rfloor$. We claim that, for any $\lambda \in \mathbb{C}$ such that $|\lambda| \geq 1$, there exists a sequence $\{\lambda'_k\}_{k=1}^{\infty} \subset \mathbb{C}$, such that $\lim_{k\to\infty}\lambda'_k = \lambda$ and $(\lambda'_k)^k = \lceil\lambda^k\rfloor$. For each $k \in \mathbb{N}$, since $\lceil\lambda^k\rfloor \neq 0$, we can let $\beta_k := \angle\lceil\lambda^k\rfloor - \angle(\lambda^k)$. Define $\lambda'_k := \sqrt[k]{|\lceil\lambda^k\rfloor|}\cdot e^{i(\angle\lambda+\beta_k/k)}$. It follows that $(\lambda'_k)^k = \big|\lceil\lambda^k\rfloor\big| e^{i(\angle(\lambda^k)+\beta_k)} = \lceil\lambda^k\rfloor$, and

$$\lim_{k\to\infty}\lambda'_k = \lim_{k\to\infty}|\lambda|\cdot\sqrt[k]{1+\frac{|\lceil\lambda^k\rfloor| - |\lambda^k|}{|\lambda^k|}}\cdot e^{i\angle\lambda} = \lambda,$$

since $\big|\big|\lceil\lambda^k\rfloor\big| - \big|\lambda^k\big|\big| \leq \sqrt{2}/2$. Thus, the claim holds. Now, let $\{\lambda_j\}_{j=1}^{\mathsf{n}_1} \subset \mathbb{C}$ be the eigenvalues of F_1. Given $\alpha > 0$, according to the claim, there exist $\{\lambda'_j\}_{j=1}^{\mathsf{n}_1} \subset \mathbb{C}$ and $k_1 \in \mathbb{N}$ such that $\big|\lambda_j - \lambda'_j\big| \leq \alpha/(2\|T_1\|\|T_1^{-1}\|)$ and $(\lambda'_j)^{k_1} = \lceil\lambda_j^{k_1}\rfloor$ hold, $\forall j = 1, \cdots, \mathsf{n}_1$, where $T_1 \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$ is the transformation matrix such that the matrix $J_1 := T_1 F_1 T_1^{-1} \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$ is of the real Jordan form of F_1. Let $J_p \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$ be the same matrix with J_1, where the real parts and the imaginary parts of the eigenvalues $\{\lambda_j\}_{j=1}^{\mathsf{n}_1}$ are replaced by those of $\{\lambda'_j\}_{j=1}^{\mathsf{n}_1}$. Define $F_p := T_1^{-1} J_p T_1$, which ensures $\|F_1 - F_p\| \leq \alpha$. Then, every eigenvalue $(\lambda'_j)^{k_1} = \lceil\lambda_j^{k_1}\rfloor$ of $F_p^{k_1}$ has the real and imaginary parts as integers, so a transformation $T \in \mathbb{R}^{\mathsf{n}_1\times\mathsf{n}_1}$ for $F_p^{k_1}$ to the real Jordan form yields $TF_p^{k_1}T^{-1} \in \mathbb{Z}^{\mathsf{n}_1\times\mathsf{n}_1}$. This completes the proof. ■

Remark 1: Note that the property $TF_p^{k_1}T^{-1} \in \mathbb{Z}^{\mathsf{n}_1\times\mathsf{n}_1}$ in Lemma 1 implies that the characteristic polynomial of $F_p^{k_1}$ is a monic polynomial having the coefficients as integers, which means, the eigenvalues of F_p are of algebraic integers. Indeed, an eigenvalue $\lambda \in \mathbb{C}$ of F_p is a root of $\det(s^{k_1}I_{\mathsf{n}_1} - F_p^{k_1}) = 0$. In this context, the meaning of Lemma 1 can be understood that the eigenvalues of the given matrix F_1 can be approximated to algebraic integers so that one of its powers can be transformed to a matrix of integers. □

With the perturbed state matrix F_p and transformation T obtained from Lemma 1, the anti-stable part (6a) of system is proposed to be converted as follows; we re-write (6a) as

$$\begin{aligned} z_1(t+1) &= F_p z_1(t) + G_1 y(t) + (F_1 z_1(t) - F_p z_1(t) + e_{z_1}(t)), \\ &=: F_p z_1(t) + G_1 y(t) + e'_{z_1}(t), \end{aligned} \tag{7}$$

and define a time-varying coordinate transformation as[5]

$$v_1(t) := TF_p^{-(t \bmod k_1)} z_1(t), \tag{8}$$

which varies with time, with period k_1. Then, by multiplying

[5]Since the matrix F_1 is anti-stable and hence invertible, the perturbed matrix F_p can be assumed to be invertible as well, thanks to Lemma 1.

both sides of (7) by $TF_p^{-(t+1 \bmod k_1)}$, it is transformed as

$$\begin{aligned} v_1(t+1) &= TF_p^{((t \bmod k_1)+1-(t+1 \bmod k_1))}T^{-1}v_1(t) \\ &\quad + TF_p^{-(t+1 \bmod k_1)}(G_1y(t)+e'_{z_1}(t)) \\ &=: F_{v_1}(t)v_1(t)+G_{v_1}(t)y(t)+e_{v_1}(t), \end{aligned} \tag{9}$$

with the initial state given by

$$v_1(0) = T(W_1x_0 + e_{z_1,0}) =: v_{1,0} + e_{v_1,0}.$$

Here, it can be clearly seen that the converted system (9) has the state matrix consisting of integers for all $t \in \mathbb{N}_0$, since

$$\begin{aligned} F_{v_1}(t) &= TF_p^{((t \bmod k_1)+1-(t+1 \bmod k_1))}T^{-1} \\ &= \begin{cases} TF_p^{k_1}T^{-1}, & \text{if } \ t \bmod k_1 = k_1-1, \\ I_{\mathsf{n}_1}, & \text{otherwise,} \end{cases} \end{aligned}$$

thanks to Lemma 1.

Next, for the stable part (6b) of the system, we use finite impulse response approximation, to convert the state matrix to integers; since the state $z_2(t)$ of (6b) can be computed as

$$z_2(t) \leftarrow F_2^tW_2x_0 + \sum_{\tau=0}^{t-1} F_2^{t-1-\tau}G_2y(\tau), \tag{10}$$

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

$$z_2(t) \leftarrow \sum_{\tau=t-k_2-1}^{t-1} F_2^{t-1-\tau}G_2y(\tau), \quad \text{for } t \geq k_2+1, \tag{11}$$

with $k_2 \in \mathbb{N}$ chosen sufficiently large, because the matrix F_2 is strictly stable. Thus, we convert the system (6b) as

$$\begin{aligned} v_2(t+1) &= \begin{bmatrix} 0_{k_2\mathsf{n}_2\times\mathsf{n}_2} & I_{k_2\mathsf{n}_2} \\ 0_{\mathsf{n}_2\times\mathsf{n}_2} & 0_{\mathsf{n}_2\times k_2\mathsf{n}_2} \end{bmatrix} v_2(t) + \begin{bmatrix} G_2 \\ F_2G_2 \\ \vdots \\ F_2^{k_2}G_2 \end{bmatrix} y(t) + e_{v_2}(t) \\ &=: F_{v_2}v_2(t) + G_{v_2}y(t) + e_{v_2}(t), \\ v_2(0) &= \left[W_2x_0; F_2W_2x_0; \cdots; F_2^{k_2}W_2x_0\right] + e_{v_2,0} \\ &=: v_{2,0} + e_{v_2,0}, \end{aligned} \tag{12}$$

where $v_2(t) \in \mathbb{R}^{(k_2+1)\mathsf{n}_2}$ is the state, with the parameter $k_2 \in \mathbb{N}$ for the dimension of (12), and $\{e_{v_2}(t), e_{v_2,0}\}$ are the perturbations with respect to the state $v_2(t)$. Note that the update rule for the first n_2-components of $v_2(t)$ corresponds to (10) for $0 \leq t \leq k_2$, and (11) for $t \geq k_2+1$. And, clearly, the state matrix F_{v_2} consists of integers, and it is nilpotent as $F_{v_2}^{k_2+1} = 0$, so the system (12) is of finite impulse response.

As the result of the proposed conversion, the proposed form of converted system (5) is now determined; let the part (5a) be identified with the combination of (9) and (12), by

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

$$F_v(t) := \begin{bmatrix} F_{v_1}(t) & 0_{\mathsf{n}_1\times(k_2+1)\mathsf{n}_2} \\ 0_{(k_2+1)\mathsf{n}_2\times\mathsf{n}_1} & F_{v_2} \end{bmatrix},\ G_v(t) := \begin{bmatrix} G_{v_1}(t) \\ G_{v_2} \end{bmatrix}.$$

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

$$\begin{aligned} x_v(t) &:= W^{-1}\begin{bmatrix} F_p^{(t \bmod k_1)}T^{-1} & 0_{\mathsf{n}_1\times\mathsf{n}_2} & 0_{\mathsf{n}_1\times k_2\mathsf{n}_2} \\ 0_{\mathsf{n}_2\times\mathsf{n}_1} & I_{\mathsf{n}_2} & 0_{\mathsf{n}_2\times k_2\mathsf{n}_2} \end{bmatrix} v(t) \\ &= W^{-1}\left[F_p^{(t \bmod k_1)}T^{-1}v_1(t); [I_{\mathsf{n}_2}, 0_{\mathsf{n}_2\times k_2\mathsf{n}_2}]v_2(t)\right]. \end{aligned} \tag{13}$$

And, to obtain the output $u(t)$ from $v(t)$, by (5b), we define

$$H_v(t) := [H_1F_p^{(t \bmod k_1)}T^{-1}, H_2, 0_{\mathsf{m}\times k_2\mathsf{n}_2}], \quad J_v(t) := J.$$

Finally, the following theorem states that given any linear time-invariant system (1), it can be converted to the form (5) having the state matrix as integers, and it can have practically the same performance with that of (1), by appropriate choice of the parameters k_1 for the period of time-varying matrices for the part (9), and k_2 for the dimension of the part (12).

Theorem 1: Consider the converted system (5), designed as (9) and (12). For any $\epsilon > 0$, there exist $k_1 \in \mathbb{N}$, $k_2 \in \mathbb{N}$, and $\eta_v > 0$ such that $\sup_t(\|[e_v(t); e_u(t); e_{v,0}]\|) \leq \eta_v$ implies $\|x_v(t) - x'(t)\| \leq \epsilon$ and $\|u_v(t) - u'(t)\| \leq \epsilon$, $\forall t \in \mathbb{N}_0$. □

Sketch of Proof: We let $x_v(t)$ of (13) be identified with $x(t)$ of (1); let $e_x(t) := x_v(t+1) - Fx_v(t) - Gy(t)$, and $e_{x,0} := x_v(0) - x_0$, so that $x(t) = x_v(t)$, $\forall t \in \mathbb{N}_0$. Then,

$$\begin{aligned} e_{x,0} &= W^{-1}[T^{-1}e_{v_1,0}; I'_2e_{v_2,0}], \\ e_x(t) &= W^{-1}\begin{bmatrix} F_p^{(t+1 \bmod k_1)}T^{-1}e_{v_1}(t); \\ I'_2e_{v_2}(t) + F'_2(F_{v_2}^te_{v_2,0} \\ +\sum_{\tau=t-k_2-1}^{t-1} F_{v_2}^{t-1-\tau}e_{v_2}(\tau)) \end{bmatrix} \\ &\quad + W^{-1}\begin{bmatrix} (F_p - F_1)W_1x_v(t); \\ -F_2^{k_2+1}G_2y(t-k_2-1) \end{bmatrix} \\ &=: e_{x,1}(t) + e_{x,2}(t), \end{aligned}$$

where $F'_2 := [-F_2, I_{\mathsf{n}_2}, 0_{\mathsf{n}_2\times(k_2-1)\mathsf{n}_2}]$, $I'_2 := [I_{\mathsf{n}_2}, 0_{\mathsf{n}_2\times k_2\mathsf{n}_2}]$, and $y(t-k_2-1) := 0$ for $t < k_2+1$. Let $\epsilon > 0$ be given, and the constants $M > 0$ and η_x be given from the conditions A1 and A2. Thanks to Lemma 1, we choose $k_1 \in \mathbb{N}$ such that $\|F_p - F_1\| \leq \eta_x/(2\|W^{-1}\|\|W_1\|(M+\epsilon))$. And, since $\lim_{k\to\infty}\|F_2^k\| = 0$, we choose $k_2 \in \mathbb{N}$ such that $\|F_2^{k_2+1}\| \leq \eta_x/(2\|W^{-1}\|\|G_2\|(M+\epsilon))$. Then, it is clear that $\|[x_v(t); y(t-k_2-1)]\| \leq M+\epsilon$ implies $\|e_{x,2}(t)\| \leq \eta_x/2$. Next, since $\{F_p^{(t+1 \bmod k_1)}\}_{t=0}^{\infty}$ is a finite set, there exists a constant $C > 0$ such that $\|[e_{x,0}; e_{x,1}(t)]\| \leq C \cdot \max\{\|e_{v,0}\|, \{\|e_v(\tau)\|\}_{\tau=t-k_2-1}^{t}\}$. Now, we choose $\eta_v := \eta_x/(2C)$, and suppose that $\sup_t(\|[e_v(t); e_u(t); e_{v,0}]\|) \leq \eta_v$. Then, it directly implies $\|e_{x,0}\| \leq \eta_x/2$ and $\|e_{x,1}(t)\| \leq \eta_x/2$, $\forall t \in \mathbb{N}_0$. Based on the assumptions A1 and A2, it can be shown that $\|e_{x,2}(t)\| \leq \eta_x/2$, $\|x_v(t)\| \leq M+\epsilon$, and $\|y(t)\| \leq M+\epsilon$, $\forall t \in \mathbb{N}_0$, and hence $\|x_v(t) - x'(t)\| \leq \epsilon$ and $\|u_v(t) - u'(t)\| \leq \epsilon$, $\forall t \in \mathbb{N}_0$. This ends the proof. ■

The meaning of Theorem 1 can be understood as follows. The difference between the trajectories $\{x_v(t), u_v(t)\}$ of the converted system (5) and those of $\{x'(t), u'(t)\}$ of the given system (1) for the ideal case is due to three things; the error $\|F_1 - F_p\|$ for approximation of the eigenvalues of the state matrix F_1 of (6a) to algebraic integers, the error due to finite impulse approximation for the part (6b), and the presence of the perturbations $\{e_v(t), e_u(t), e_{v,0}\}$ in (5). Since the two approximation errors can be made arbitrarily small by increasing the parameters $\{k_1, k_2\}$, it follows that the condition A2 for the system (1) also holds with respect to the converted system (5) and the perturbations $\{e_v(t), e_u(t), e_{v,0}\}$, with appropriate choice of $\{k_1, k_2\}$.

Remark 2: Since the transformation (8) for the state $v_1(t)$ is of periodically time-varying, and the part (12) for the

state $v_2(t)$ is of finite impulse response, it can be checked that the state $v(t)=[v_1(t);v_2(t)]$ is bounded. First, Theorem 1 with A1 and A2 ensures that $\|x_v(t)\| \le M+\epsilon$ and $\|y(t)\| \le M+\epsilon$ hold, for all $t \in \mathbb{N}_0$. Then, from (8), it is obvious that

$$\begin{aligned}\|v_1(t)\| &= \left\| TF_p^{-(t \bmod k_1)} W_1 x_v(t) \right\| \\ &\le \max_{i=0,\cdots,k_1-1} \{\|TF_p^{-i}W_1\|\}(M+\epsilon).\end{aligned}$$

And, since $F_{v_2}^{k_2+1}=0$ in (12), a bound for $v_2(t)$ is found as

$$\begin{aligned}\|v_2(t)\| &= \left\| F_{v_2}^t v_2(0) + \sum_{\tau=0}^{t-1} F_{v_2}^{t-1-\tau}(G_{v_2}y(\tau)+e_{v_2}(\tau)) \right\| \\ &\le \|v_{2,0}\| + \eta_v + (k_2+1)(\|G_{v_2}\|(M+\epsilon)+\eta_v).\end{aligned}$$

Thus, it is clear that the state $v(t)$ is bounded. □

In the next subsection, we show how to run the converted periodically time-varying system (5) over ciphertexts, where it will be seen that the conversion for the condition $F_v(t) \in \mathbb{Z}^{\mathsf{n}_v \times \mathsf{n}_v}$ allows the operation performed for an infinite time horizon without re-encryption, using only homomorphic property of cryptosystem. It can be seen as an extended version of the methods in [16] and [17], where time-invariant systems having the state matrix as integers are considered.

B. Implementation over Encryped Data

We first consider digital implementation for the converted system (5), to operate over the space $\mathbb{Z}_q=\{0,1,\cdots,q-1\}$, with some $q \in \mathbb{N}$. Let the matrices of (5) be stored as

$$\begin{aligned}&\overline{F}_t = F_v(t) \mod q, \quad \overline{G}_t := \left\lceil \frac{G_v(t)}{\mathsf{s}} \right\rfloor \mod q, \\ &\overline{H}_t := \left\lceil \frac{H_v(t)}{\mathsf{s}} \right\rfloor \mod q, \quad \overline{J} := \left\lceil \frac{J}{\mathsf{s}^2} \right\rfloor \mod q,\end{aligned} \tag{14}$$

with a scale factor $1/\mathsf{s} \ge 1$, as elements of $\mathbb{Z}_q$, which vary with time, with the period k_1. Note that, thanks to the conversion, the state matrices $F_v(t)$ are of integers, so it does not need scaling to keep the numbers down to decimal place.

Then, the system (5) is proposed to be implemented as

$$\begin{aligned}\overline{v}(t+1) &= \overline{F}_t\overline{v}(t) + \overline{G}_t\overline{y}(t) \bmod q, \ \overline{v}(0) = \left\lceil \frac{v_0}{\mathsf{rs}} \right\rfloor \bmod q, \\ \overline{u}(t) &= \overline{H}_t\overline{v}(t) + \overline{J}\overline{y}(t) \bmod q,\end{aligned} \tag{15}$$

where $\overline{v}(t) \in \mathbb{Z}_q^{\mathsf{n}_v}$ is the state, $\overline{u}(t) \in \mathbb{Z}_q^{\mathsf{m}}$ is the output, and $\overline{y}(t) \in \mathbb{Z}_q^{\mathsf{p}}$ is the input quantized as (3), so that it operates based on modular addition and multiplication over $\mathbb{Z}_q$. Here, we let the modulus $q \in \mathbb{N}$ be chosen to cover the range of the output $u(t)$ scaled by $1/(\mathsf{rs}^2)$; we let

$$q \ge \max_{i=1,\cdots,\mathsf{m}} \left\{ \left\lceil \frac{u_i^{\max}+\epsilon}{\mathsf{rs}^2} \right\rceil - \left\lfloor \frac{u_i^{\min}-\epsilon}{\mathsf{rs}^2} \right\rfloor + 1 \right\}, \tag{16}$$

where the constants $\{u_i^{\max}, u_i^{\min}\}_{i=1}^{\mathsf{m}}$ are from (2), and ϵ considers the error margin from the condition A2, respectively.

Then, with the decoding function $g: \mathbb{Z}_q^{\mathsf{m}} \to \mathbb{R}^{\mathsf{m}}$ to recover the real output $u_v(t) \in \mathbb{R}^{\mathsf{m}}$ from $\overline{u}(t) \in \mathbb{Z}_q^{\mathsf{m}}$, defined as

$$g(\overline{u}(t)) := \mathsf{rs}^2 \cdot \left(\overline{u}(t) - \left\lfloor \frac{\overline{u}(t)-\overline{u}_0}{q} \right\rfloor q \right) \tag{17}$$

where $\overline{u}_0 := \operatorname{col}\left\{ \left\lfloor \frac{u_i^{\min}-\epsilon}{\mathsf{rs}^2} \right\rfloor \right\}_{i=1}^{\mathsf{m}} \in \mathbb{Z}^{\mathsf{m}}$, the following lemma states that operation of (15) is equivalent to that of (5).

Lemma 2: Consider the system (5) with $F_v(t) \in \mathbb{Z}^{\mathsf{n}_v \times \mathsf{n}_v}$, and the system (15) over $\mathbb{Z}_q$. For any $\eta_v > 0$, there exist $\mathsf{r}' > 0$ and $\mathsf{s}' > 0$ such that for every $\mathsf{r} < \mathsf{r}'$ and $\mathsf{s} < \mathsf{s}'$, it satisfies $g(\overline{u}(t)) = u_v(t)$, $\forall t \in \mathbb{N}_0$, with some $\{e_v(t), e_u(t), e_{v,0}\}_{t=0}^{\infty}$ such that $\sup_t(\|[e_v(t); e_u(t); e_{v,0}]\|) \le \eta_v$. □

Sketch of Proof: Consider an auxiliary system written as

$$\begin{aligned}\overline{v}'(t+1) &= \overline{F}_t\overline{v}'(t) + \overline{G}_t \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor, \quad \overline{v}'(0) = \left\lceil \frac{v_0}{\mathsf{rs}} \right\rfloor, \\ \overline{u}'(t) &= \overline{H}_t\overline{v}'(t) + \overline{J} \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor, \ \overline{v}'(t) \in \mathbb{Z}^{\mathsf{n}_v}, \ \overline{u}'(t) \in \mathbb{Z}^{\mathsf{m}}.\end{aligned} \tag{18}$$

It is obvious that $\overline{u}(t) = \overline{u}'(t) \mod q$, $\forall t \in \mathbb{N}_0$. Conversely, as the same as in [16, Lemma 2], it can be easily proven that

$$\overline{u}'(t) = \overline{u}(t) - \left\lfloor \frac{\overline{u}(t)-\overline{u}_0}{q} \right\rfloor q, \quad \forall t \in \mathbb{N}_0,$$

as long as (16) holds. Then, the system (18) is identified with (5); with the errors $\{e_{v,0}, e_v(t), e_u(t)\}$ of (5) given as

$$\begin{aligned}e_{v,0} &= \mathsf{rs}\left\lceil \frac{v_0}{\mathsf{rs}} \right\rfloor - v_0, \ e_v(t) = \mathsf{rs}\left\lceil \frac{G_v(t)}{\mathsf{s}} \right\rfloor \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor - G_v(t)y(t), \\ e_u(t) &= \left(\mathsf{s}\left\lceil \frac{H_v(t)}{\mathsf{s}} \right\rfloor - H_v(t) \right) v(t) + \mathsf{rs}^2 \left\lceil \frac{J}{\mathsf{s}^2} \right\rfloor \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor - Jy(t),\end{aligned}$$

it follows that $v(t) = \mathsf{rs} \cdot \overline{v}'(t)$ and $u_v(t) = \mathsf{rs}^2 \cdot \overline{u}'(t)$, $\forall t \in \mathbb{N}_0$. Note that the matrix $G_v(t)$ is of periodically time-varying so that bounded, and the signals $\{y(t), v(t)\}$ are also bounded as shown in Remark 2. Based on this boundedness, it can be shown that $\|e_{v,0}\|$, $\|e_v(t)\|$, and $\|e_u(t)\|$ tend to zero, as r and s go to zero; for any $\eta_v > 0$, there exist $\mathsf{r}' > 0$ and $\mathsf{s}' > 0$ such that for every $\mathsf{r} < \mathsf{r}'$ and $\mathsf{s} < \mathsf{s}'$, it satisfies $\|[e_{v,0}; e_v(t); e_u(t)]\| \le \eta_v$, $\forall t \in \mathbb{N}_0$. This ends the proof. ■

Remark 3: Note that the implementation of (15), using only modular addition and multiplication over integers for operation for the whole time, is attributable to the state matrix $\overline{F}_t$ consisting of integers, obtained with the proposed conversion. Indeed, if the matrix $F_v(t)$ were not of integers, so kept as $\overline{F}_t = \lceil F_v(t)/\mathsf{s} \rfloor$ with the scale factor $1/\mathsf{s} > 1$, the factor $1/\mathsf{s}$ as well as the matrix $F_v(t)$ would be recursively multiplied to the state $\overline{v}(t)$ of (15). Then, unless any operation other than addition and multiplication is allowed, there would be an overflow problem for the state $\overline{v}(t)$ so that it would be incapable of operating for an infinite time horizon, even if the real state $v(t)$ is bounded. See [16, Section II-D] or [17, Section III] for more details. □

So far, we have proposed a method for implementing the given system (1), as (15), using only modular addition and multiplication over the space $\mathbb{Z}_q$. As the end result, we now show that it is straightforward to implement the operation of (15) directly over ciphertexts, via additively homomorphic cryptosystems described in Section II-A; consider a dynamic system defined on the space $\mathcal{C}$ of ciphertexts, designed as

$$\begin{aligned}\mathbf{v}(t+1) &= \overline{F}_t \cdot \mathbf{v}(t) + \overline{G}_t \cdot \mathbf{y}(t), \mathbf{v}(0) = \mathsf{Enc}\left(\left\lceil \frac{v_0}{\mathsf{rs}} \bmod q \right\rfloor \right), \\ \mathbf{u}(t) &= \overline{H}_t \cdot \mathbf{v}(t) + \overline{J} \cdot \mathbf{y}(t),\end{aligned} \tag{19}$$

in which $\mathbf{v}(t) \in \mathcal{C}^{\mathsf{n}_v}$ is the state, $\mathbf{y}(t) \in \mathcal{C}^{\mathsf{p}}$ is the input encrypted as (4), and $\mathbf{u}(t) \in \mathcal{C}^{\mathsf{m}}$ is the output, and $+$ and $\cdot$ denote the operations Add_n and $\mathsf{IntMult}_{m,n}$ of the properties H2 and H3, respectively, with some dimensions $\{m, n\}$.

Finally, we have the following main theorem, which states that the operation of the given system (1) can be implemented only using addition and multiplication over encrypted data for an infinite time horizon, in which it does not re-encrypt or reset any portion of data for the whole time, and the performance error can be made arbitrarily small with the choice of the parameters $\{k_1, k_2, \mathsf{r}, \mathsf{s}\}$.

Theorem 2: Consider the system (19) over encrypted data. For any $\epsilon > 0$, there exist $k_1 \in \mathbb{N}$, $k_2 \in \mathbb{N}$, $\mathsf{r}' > 0$, and $\mathsf{s}' > 0$ such that for every $\mathsf{r} < \mathsf{r}'$ and $\mathsf{s} < \mathsf{s}'$, it guarantees that $\|g(\mathsf{Dec}(\mathbf{u}(t))) - u'(t)\| \leq \epsilon$ holds, for all $t \in \mathbb{N}_0$. □

Proof: Let $\mathsf{Dec}(\cdot)$ be taken for the both sides of (19). Then, by the properties H1–H3, it is clear that $\mathsf{Dec}(\mathbf{v}(t))$ obeys (15), i.e., $\mathsf{Dec}(\mathbf{v}(t)) = \overline{v}(t)$ and $\mathsf{Dec}(\mathbf{u}(t)) = \overline{u}(t)$, $\forall t \in \mathbb{N}_0$. Now, consider (5) as an auxiliary system, and let $\epsilon > 0$ be given. According to Theorem 1, there exist $k_1 \in \mathbb{N}$, $k_2 \in \mathbb{N}$, and $\eta_v > 0$ such that $\sup_t(\|[e_v(t); e_u(t); e_{v,0}]\|) \leq \eta_v$ implies $\|x_v(t) - x'(t)\| \leq \epsilon$ and $\|u_v(t) - u'(t)\| \leq \epsilon$, $\forall t \in \mathbb{N}_0$. Then, Lemma 2 completes the proof. ■

Remark 4: A remark is made to compare the proposed method of this paper, and the method presented in [16]. Both the methods consider converting the state matrix to integers for operation for an infinite time horizon. But, a significant difference is that the method in [16] assumes the existence of an external unit[6] having the decryption key, which can decrypt and re-encrypt the system output, and transmit it back to the system. In contrast, this assumption is not considered in this paper, as it is clear that the proposed system (19) does not utilize re-encryption of the output $\mathbf{u}(t)$. To sum up, a strong point of the method of this paper is that the proposed system (19) can operate solely, for the infinite time horizon, without relying on the presence of decryption key (without re-encrypting any portion of data). □

IV. Conclusion

In this paper, we have proposed a method for running linear time-invariant systems over encrypted data for an infinite time horizon, which does not make use of bootstrapping techniques, reset, or re-encryption of data, but exploiting the additively homomorphic property of the cryptosystem only.

The proposed method first consider the Jordan canonical decomposition of the given system, into stable part and anti-stable part, and convert each of them to have the state matrix as integers. To this end, finite impulse response approximation is used for the stable part, and a novel conversion scheme is presented for the anti-stable part, which first approximates the eigenvalues of the state matrix, and then transforms the system to a periodically time-varying system having the state matrices as integers. By doing so, it has been proven that the converted system can be implemented to operate using only modular addition and multiplication, that is, can be implemented over encrypted data without re-encryption. Moreover, it has been seen that the performance error, which is due to approximation errors during the conversion and quantization errors because of digital implementation, can be made arbitrarily small by appropriate choice of parameters.

The case of using LWE-based cryptosystems which can be both multiplicatively and additively homomorphic is not considered in this paper, and consideration of injected errors during encryption for such cases is omitted for simplicity, but they can be considered in the future work.

[6]For example, the actuator in the common configuration of encrypted control system can be considered as such external unit.

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 Conf. Decision and Control*, 2015, pp. 6836–6843.

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

[4] 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.

[5] M. Schulze Darup, "Encrypted model predictive control in the cloud," in *Privacy in Dynamical Systems*, Springer, Singapore, 2020, pp. 231–265.

[6] N. Schlüter and M. Schulze Darup, "Encrypted explicit MPC based on two-party computation and convex controller decomposition," in *Proc. 59th IEEE Conf. Decision and Control*, 2020, pp. 5469–5476.

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

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

[9] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.

[10] D. Lee, J. Kim, and H. Shim, "Distributed aggregation over homomorphically encrypted data under switching networks," in *Proc. 59th IEEE Conf. Decision and Control*, 2020, pp. 5495–5500.

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

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

[13] A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Towards private data-driven control," in *Proc. 59th IEEE Conf. Decision and Control*, 2020, pp. 5449–5456.

[14] J. Suh and T. Tanaka, "SARSA(0) reinforcement learning over fully homomorphic encryption," arXiv:2002.00506 [eess.SY], 2020.

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

[16] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," under review for *IEEE Trans. Automatic Control*.

[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 Conf. Decision and Control*, 2018, pp. 5020–5025.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. 17th Int. Conf. Theory Applicat. Crypto. Tech.*, 1999, pp. 223–238.

[19] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 34, 2009.

[20] G. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based," in *Advances in Cryptology–CRYPTO*, Springer, Berlin, Heidelberg, 2013, pp. 75–92.

[21] 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, Singapore, 2020, pp. 209–230.