2020 59th IEEE Conference on Decision and Control (CDC)
Jeju Island, Republic of Korea, December 14-18, 2020

Design Procedure for Dynamic Controllers based on LWE-based Homomorphic Encryption to Operate for Infinite Time Horizon

Junsoo Kim, Hyungbo Shim, and Kyoohyung Han

Abstract— **The design of encrypted controllers, which perform control operation directly over encrypted signals via homomorphic cryptosystems, should consider both security of the control data and performance of the controller. Considering the use of Learning With Errors (LWE) based cryptosystem, in this paper, we present a design procedure for encrypted linear dynamic controllers. Providing a guideline for choosing the parameters of the cryptosystem as well as quantization, the procedure guarantees both the desired level of security and performance. Receiving the encrypted signals of the plant input as well as the output, the proposed controller is able to perform the dynamic operation over encrypted data for infinite time horizon, without the use of decryption or reset of the state. Thanks to additively and multiplicatively homomorphic property of the LWE-based cryptosystem, information of both control signals and gain matrices is protected by encryption.**

I. Introduction

The development of network communication and the increase of computational power have made control systems more connected, and the threat of cyber-attacks has been a major problem. The most vulnerable part from the perspective of eavesdropping attacks, which targets to learn private data in the network layer, is computing devices in which the data are conventionally treated as un-encrypted for the computation. Against the unauthorized access, the notion of encrypted control based on homomorphic encryption techniques has been introduced [1]–[3], which aims for performing all the control operation over encrypted data without decryption, so that it keeps all the data in the controller from being exposed. The elimination of decryption key from the network layer is significant in terms of security as well, so the notion is being considered in more and more applications such as model predictive control [4], [5], average consensus [6], or reinforcement learning [7].

Implementing controllers to operate over encrypted data is to conduct the homomorphic cryptosystem algorithms to the control operations. In theory, the development of "bootstrapping techniques" of fully homomorphic cryptosystems [8] guarantees that any logical functions or arithmetic operations in a digital computer can be applied to an encrypted message, infinite number of times. Thus, it is clear that any operation for feedback control can be performed over encrypted signals and parameters for infinite time horizon, as introduced in [3]. However, it has been considered that the use of bootstrapping techniques requires substantial computational resources, so it may hinder them from being used for real-time process of feedback control, in practice.

Methods without the bootstrapping of fully homomorphic cryptosystems have been considered in literature, but due to the limitation on the sorts or the number of operations for encrypted messages, *implementing dynamic controllers to operate over encrypted data* has been a challenge. Typically, most homomorphic cryptosystems allow additions or multiplications over encrypted messages as integers, but with these properties only, it is generally impossible to perform division of numbers (multiplication of non-integer real numbers) for an encrypted message infinitely many times. Thereby, regarding the recursive state update of dynamic systems over non-integer real numbers, it leads to the fact that encrypted dynamic controllers implemented in the usual way may not be capable of operating for infinite time horizon. Consequently, it has been a common concern for the early studies on encrypted control, and most results in literature end up considering finite-time operation only as in [5], [6] or static operation only as in [2], [4], or assuming intermittent decryption or reset for the controller state as in [1], [10].

In this paper, we first revisit the method presented in [9], which implements dynamic controllers to operate over encrypted data for infinite time horizon. The proposed method in [9] converts the given controller to receive both the input and output of the plant as quantized signals and utilize only multiplications and additions over integers for computing the next state and the output of the controller. Then, employing a cryptosystem based on Learning With Errors (LWE) problem [11] presented in [12], which is both additively and multiplicatively homomorphic, the converted controller can be implemented to operate over encrypted signals and parameters for infinite time horizon, without the use of decryption, reset, or bootstrapping for the state.

And, as a follow-up result, in this paper, we provide a guideline for choosing both the parameters for the employed LWE-based cryptosystem and the parameters for quantization of the controller so that it guarantees both desired level of security and performance, at the same time. In general, these two objectives may conflict with each other;

- LWE-based cryptosystems necessarily inject errors for the messages being encrypted, for the purpose of security, where the injected errors may grow under recursive operations. To keep the messages from being damaged by the error growth, messages are usually scaled with a sufficiently large factor. However, increasing the scaling factor for the messages for the sake of controller performance will increase the size of space for encrypted data, and it may result in decrease of security level.

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. NRF-2017R1E1A1A03070342).

J. Kim and H. Shim are with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Korea. K. Han is with Samsung SDS. This work is done before K. Han joins to Samsung SDS.

978-1-7281-7446-4/20/$31.00 ©2020 IEEE

- with the same rationale, the finer quantization for the control signals or the more precise computation for the controllers will require the larger size for the space of encrypted messages, which may decrease the security level, as well.
- LWE-based cryptosystems utilize a vector of random numbers for the encryption, and a usual way for enhancing security is to increase the dimension of the random vector. However, increasing the dimension may encourage the growth of injected errors, so it may conflict with the performance of the controller.

Considering all these potential issues, the proposed procedure suggests that each parameter for the encrypted controller can be defined as a function of other parameters. By doing so, it will be seen that the choice of control parameters, which considers the performance only, automatically changes the parameters for the cryptosystem as well, so that it does not affect the desired level of security. Finally, given a dynamic controller over real-valued signals, the proposed procedure guarantees that the designed controller over encrypted data does not sacrifice the performance even when it performs the operation for infinite time horizon, while it guarantees the desired level of security for the whole time.

Notation: The set of natural numbers, integers, and real numbers are denoted by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$, respectively. We let $\lfloor\cdot\rfloor$, $\lceil\cdot\rfloor$, and $\lceil\cdot\rceil$ denote the floor, rounding, and ceiling function, respectively. The set of integers modulo $q\in\mathbb{N}$ is denoted by $\mathbb{Z}_q := \{0,1,\cdots,q-1\}$, and an integer $a\in\mathbb{Z}$ modulo q is defined as $a \mod q := a - \lfloor a/q\rfloor\cdot q \in \mathbb{Z}_q$. The zero-mean discrete Gaussian distribution with standard deviation $\sigma_0 > 0$ is simply denoted by $N(0,\sigma_0)$. For real numbers, $|\cdot|$ denotes the absolute value, and for vectors or matrices, $\|\cdot\|$ denotes the infinity norm. For a sequence $v_1,\cdots,v_p$ of column vectors or scalars, we define $\mathrm{col}\{v_i\}_{i=1}^p := [v_1^\top,\cdots,v_p^\top]^\top$. For $n\in\mathbb{N}$, the identity matrix is denoted as $I_n\in\mathbb{R}^{n\times n}$.

II. Preliminaries and Problem Formulation

Design and execution of encrypted controllers, which perform control operation directly over encrypted data, is necessarily based on the use of homomorphic cryptosystems. The proposed design of encrypted controller to be seen is also applicable with any homomorphic encryption that allows addition over encrypted data. But, taking into account the benefits of recent cryptosystems based on Learning With Errors problem [11], we suppose the use of encryption scheme presented in [12], introduced in the following subsection.

A. Learning With Errors based Cryptosystems [11], [12]

With the modulus $q\in\mathbb{N}$, the space of plaintexts (unencrypted messages) is defined as $\mathbb{Z}_q=\{0,1,\cdots,q-1\}$. The LWE-based encryption maps a message in $\mathbb{Z}_q$ to a vector consisting of elements in $\mathbb{Z}_q$; with a parameter $n\in\mathbb{N}$, the space of ciphertexts (encrypted data) is defined as $\mathbb{Z}_q^{n+1}$.

Let $\mathsf{Enc}:\mathbb{Z}_q\to\mathbb{Z}_q^{n+1}$ and $\mathsf{Dec}:\mathbb{Z}_q^{n+1}\to\mathbb{Z}_q$ denote the encryption and decryption algorithm, respectively. LWE-based encryptions necessarily inject errors to the ciphertexts. The following algorithms describe the cryptosystem to be used throughout the paper, in which it can be seen that every encrypted message of $m\in\mathbb{Z}_q$ is perturbed to $m+\Delta$, with an error $\Delta\in\mathbb{Z}$ sampled from zero-mean discrete Gaussian distribution.

- $\mathsf{Setup}(1^\lambda)$. Choose the modulus $q\in\mathbb{N}$, the standard deviation $\sigma_0>0$, and the dimension $n\in\mathbb{N}$ such that
$$n\log q \geq (0.63\lambda-0.21)\cdot\log^2\left(\frac{\sqrt{2\pi}\sigma_0}{q}\right). \qquad (1)$$
Return $params=\{q,\sigma_0,n\}$.
- $\mathsf{KeyGen}(params)$. Generate the secret key $\mathsf{sk}\in\mathbb{Z}^n$ as a row vector such that each element is sampled from the distribution $N(0,\sigma_0)$. Return sk.
- $\mathsf{Enc}(m\in\mathbb{Z}_q,\mathsf{sk})$. Generate a random (column) vector $a\in\mathbb{Z}_q^n$ from the uniform distribution over $\mathbb{Z}_q$, and an error $\Delta\in\mathbb{Z}$ from the distribution $N(0,\sigma_0)$. Compute $b=-\mathsf{sk}\cdot a+m+\Delta \mod q$. Return $\mathrm{col}\{b,a\}\in\mathbb{Z}_q^{n+1}$.
- $\mathsf{Dec}(\mathbf{c}\in\mathbb{Z}_q^{n+1},\mathsf{sk})$. Let $\mathbf{c}=\mathrm{col}\{b,a\}$ where $b\in\mathbb{Z}_q$ and $a\in\mathbb{Z}_q^n$. Return $b+\mathsf{sk}\cdot a \mod q\in\mathbb{Z}_q$.

As the security level of the LWE cryptosystem is determined with the parameters $\{q,\sigma_0,n\}$, the dimension n for the ciphertext space should be chosen sufficiently large to satisfy (1), in order to achieve the desired λ-bit security. The inequality (1) is derived from linear regression of data obtained with recent parameter estimator available in [15]. An alternative for the relation can be found in [14], for example, which suggests $n\log q\geq\frac{\lambda+110}{7.2}\cdot\log^2(\frac{\sqrt{2\pi}\sigma_0}{q})$.

The estimation for the parameters assumes Gaussian distribution for the errors, though, for the sake of simplicity, we assume that every error $\Delta\in\mathbb{Z}$ sampled in the algorithm Enc is bounded by a constant $\Delta_{\mathsf{Enc}}=k\sigma_0$ with some $k\in\mathbb{N}$. In other words, we neglect the probability for the case $|\Delta|>\Delta_{\mathsf{Enc}}$ for every sampled error $\Delta\in\mathbb{Z}$.

With this premise, the additively homomorphic property of the described crytpsystem is stated as follows. For the rest of this paper, we omit the argument of secret key sk from the algorithms $\mathsf{Enc}(\,\cdot\,,\mathsf{sk})$ and $\mathsf{Dec}(\,\cdot\,,\mathsf{sk})$, for simplicity.

Proposition 1: Given the secret key sk, the algorithms Enc and Dec satisfy the following properties.

1) For every $m\in\mathbb{Z}_q$, it satisfies $\mathsf{Dec}(\mathsf{Enc}(m))=m+\Delta \mod q$ with some $\Delta\in\mathbb{Z}$ such that $|\Delta|\leq\Delta_{\mathsf{Enc}}$.
2) For every $\mathbf{c}_1\in\mathbb{Z}_q^{n+1}$ and $\mathbf{c}_2\in\mathbb{Z}_q^{n+1}$, they satisfy[1] $\mathsf{Dec}(\mathbf{c}_1+\mathbf{c}_2 \mod q)=\mathsf{Dec}(\mathbf{c}_1)+\mathsf{Dec}(\mathbf{c}_2) \mod q$.
3) For every $k\in\mathbb{Z}$ and $\mathbf{c}\in\mathbb{Z}_q^{n+1}$, they satisfy $\mathsf{Dec}(k\cdot\mathbf{c} \mod q)=k\cdot\mathsf{Dec}(\mathbf{c}) \mod q$. □

Proof: It can be easily proven from the definition. ■

Proposition 1.3 shows that the additively homomorphic property allows multiplication over encrypted data as well, but the information of "multiplier" $k\in\mathbb{Z}$ is not protected by encryption, yet. To this end, we introduce further algorithms presented in [12], on top of the described cryptosystem. In order to exploit the multiplicatively homomorphic property of the cryptosystem as well, it considers a separate algorithm for encrypting the multipliers, as follows.

- $\mathsf{Setup}'(1^\lambda)$. Choose $\nu\in\mathbb{N}$ and $d\in\mathbb{N}$ such that $\nu^{d-1}<q\leq\nu^d$. Define $n'=d(n+1)$. Return $params'=(\nu,d,n')$.

[1] The functions defined in this paper for scalars, such as $(\,\cdot \mod q)$ or $\lfloor\cdot\rceil$, are also used for vectors as component-wise functions.

- $\mathsf{Enc}'(k \in \mathbb{Z}_q, \mathsf{sk})$. Generate a random matrix $A \in \mathbb{Z}_q^{n\times n'}$ from the uniform distribution over $\mathbb{Z}_q$, and a row vector $E \in \mathbb{Z}^{n'}$ with each element sampled from $N(0,\sigma_0)$. Compute $B = -\mathsf{sk}\cdot A + E$. Return $k\cdot[I_{n+1}, \nu\cdot I_{n+1}, \cdots, \nu^{d-1}\cdot I_{n+1}] + [B^\top, A^\top]^\top \bmod q \in \mathbb{Z}_q^{(n+1)\times n'}$.

Note that a message encrypted with the algorithm Enc' is an $(n+1)$ by n' matrix over $\mathbb{Z}_q$, which is different from the space $\mathbb{Z}_q^{n+1}$ with respect to the algorithm Enc. For the sake of multiplication, let us define a decomposition $D : \mathbb{Z}_q^{n+1} \to \mathbb{Z}_\nu^{d(n+1)}$ for the ciphertexts with respect to Enc, as

$$D(\mathbf{c}) := \mathrm{col}\left\{\mathbf{c}_i\right\}_{i=0}^{d-1}, \quad \text{where} \quad \mathbf{c}_i = \left\lfloor \frac{\mathbf{c}}{\nu^i} \right\rfloor \mod \nu$$

so that it satisfies $\mathbf{c} = \sum_{i=0}^{d-1} \mathbf{c}_i \nu^i$. Then, the decomposed ciphertext in $\mathbb{Z}_\nu^{d(n+1)} = \mathbb{Z}_\nu^{n'}$ can be multiplied with the ciphertexts in $\mathbb{Z}_q^{(n+1)\times n'}$ with respect to Enc', which results in the following proposition of the multiplicatively homomorphic property.

Proposition 2: For every $k \in \mathbb{Z}_q$ and $\mathbf{c} \in \mathbb{Z}_q^{n+1}$, they satisfy $\mathsf{Dec}(\mathsf{Enc}'(k)\cdot D(\mathbf{c}) \mod q) = k\cdot\mathsf{Dec}(\mathbf{c}) + \Delta \mod q$, with some $\Delta \in \mathbb{Z}$ such that $|\Delta| \le n'\nu\Delta_{\mathsf{Enc}}$. □

Proof: The proof is analogous to [9, Proposition 4] so omitted, in which it deals with a general case when the modulus q is a multiple of the modulus for the plaintexts. ■

For vectors of messages, as long as there is no ambiguity, we abuse notation and use Enc, Dec, D, and Enc', as component-wise algorithms; we define

$$\mathsf{Enc}(v) := \mathrm{col}\{\mathsf{Enc}(v_i)\}_{i=1}^{\mathsf{p}} \quad \text{for } v = \mathrm{col}\{v_i\}_{i=1}^{\mathsf{n}} \in \mathbb{Z}_q^{\mathsf{p}},$$

for vector of messages so that the result $\mathsf{Enc}(v) \in \mathbb{Z}_q^{\mathsf{p}(n+1)}$ is a column vector. And, the decryption or the decomposition for a vector $\mathbf{c} = \mathrm{col}\{\mathbf{c}_i\}_{i=1}^{\mathsf{p}} \in \mathbb{Z}_q^{\mathsf{p}(n+1)}$ of encrypted messages, where $\mathbf{c}_i \in \mathbb{Z}_q^{n+1}$ for each i, is defined as

$$\mathsf{Dec}(\mathbf{c}) := \mathrm{col}\{\mathsf{Dec}(\mathbf{c}_i)\}_{i=1}^{\mathsf{p}} \in \mathbb{Z}_q^{\mathsf{p}},$$
$$D(\mathbf{c}) := \mathrm{col}\{D(\mathbf{c}_i)\}_{i=1}^{\mathsf{p}} \in \mathbb{Z}_\nu^{\mathsf{p}\cdot n'},$$

respectively. Finally, component-wise encryption for a matrix $K = [k_{ij}] \in \mathbb{Z}_q^{\mathsf{p}\times\mathsf{m}}$ as multiplier is defined as

$$\mathsf{Enc}'(K) := \begin{bmatrix} \mathsf{Enc}'(k_{1,1}) & \cdots & \mathsf{Enc}'(k_{1,\mathsf{m}}) \\ \vdots & \ddots & \vdots \\ \mathsf{Enc}'(k_{\mathsf{p},1}) & \cdots & \mathsf{Enc}'(k_{\mathsf{p},\mathsf{m}}) \end{bmatrix} \in \mathbb{Z}_q^{\mathsf{p}(n+1)\times\mathsf{m}n'},$$

which yields a matrix having $\mathsf{p}(n+1)$-rows and $\mathsf{m}n'$-columns. The following proposition states the homomorphic property for vectors and matrices of encrypted messages.

Proposition 3: For every $K \in \mathbb{Z}_q^{\mathsf{p}\times\mathsf{m}}$ and $\mathbf{c} \in \mathbb{Z}_q^{\mathsf{m}(n+1)}$, they satisfy $\mathsf{Dec}(\mathsf{Enc}'(K)\cdot D(\mathbf{c}) \mod q) = K\cdot\mathsf{Dec}(\mathbf{c}) + \Delta \mod q$, with some $\Delta \in \mathbb{Z}^{\mathsf{p}}$ such that $\|\Delta\| \le \mathsf{m}n'\nu\Delta_{\mathsf{Enc}}$. □

Proof: It directly follows from Propositions 1.2 and 2. ■

B. Problem Formulation

Consider a discrete-time controller written by

$$x(t+1) = Fx(t) + Gy(t) + e_x(t), \tag{2a}$$
$$u(t) = Hx(t) + Jy(t) + e_u(t), \tag{2b}$$
$$x(0) = x_0 + e_0, \quad t = 0,1,2,\cdots,$$

where $x \in \mathbb{R}^{\mathsf{n}}$ is the state with the initial value $x_0 \in \mathbb{R}^{\mathsf{n}}$, $y \in \mathbb{R}^{\mathsf{p}}$ is the input, $u \in \mathbb{R}^{\mathsf{m}}$ is the output, and e_x, e_u, e_0 are perturbations or disturbances. Considering that the controller (2) would be designed to control a system called plant, the input y may consist of the output of the plant or reference signals, and the output u may be considered as the input of the plant, in practice.

For the perturbation-free case, i.e., for the case $e_x(t) \equiv 0$, $e_u(t) \equiv 0$, and $e_0 = 0$, the trajectories of the state and the output with the input $\{y(t)\}_{t=0}^{\infty}$ are written as $\{x'(t)\}_{t=0}^{\infty}$ and $\{u'(t)\}_{t=0}^{\infty}$, respectively. From the rationale that the design of the controller (2) should stabilize the closed-loop system so that (2) is a part of stable system, we assume in this paper that the signals $y(t)$, $x'(t)$, and $u'(t)$ are bounded. Especially for the signal $u'(t) = \mathrm{col}\{u_i'(t)\}_{i=1}^{\mathsf{m}}$, we let the i-th component $u_i'(t)$ is bounded as $u_i^{\min} \le u_i'(t) \le u_i^{\max}$ for all $t \ge 0$, with some $u_i^{\min} \in \mathbb{R}$ and $u_i^{\max} \in \mathbb{R}$, respectively.

And, the trajectories $\{x'(t)\}_{t=0}^{\infty}$ and $\{u'(t)\}_{t=0}^{\infty}$ are assumed to be stable with respect to perturbations, as follows.

Assumption 1: Given $\epsilon > 0$, there exists $\eta(\epsilon)$ such that $\sup_t(\|e_x(t)\|) \le \eta(\epsilon)$, $\sup_t(\|e_u(t)\|) \le \eta(\epsilon)$, and $\|e_0\| \le \eta(\epsilon)$ implies that $\|x(t) - x'(t)\| \le \epsilon$ and $\|u(t) - u'(t)\| \le \epsilon$ for all $t \ge 0$. □

Now, the problem of this paper is stated. Given the controller (2), the objective is to construct a dynamic system over encrypted data, which satisfies the following properties:

- The constructed system operates over encrypted data. Receiving an encrypted signal that contains the value of the input $y(t)$, the next state and the output of the system are computed without decryption, with the use of homomorphic properties of the LWE-based cryptosystem. Both the state and the output are obtained as ciphertexts, where the output contains the value of the signal $u(t)$.
- Given the parameters ϵ for the performance and λ for the security, all the parameters for the constructed system, including the parameters $\{q, \sigma_0, n\}$ for the cryptosystem, are determined a priori, so that they guarantee both the desired levels of performance and security. That is, the performance error for the output $u(t)$ is not larger than ϵ, and all the information of the signals $\{x, y, u\}$ and the parameters $\{F, G, H, J\}$ are protected by encryption, with the desired λ-bit security.
- The constructed system can operate for infinite time horizon, without decryption or reset for the state.

III. Encrypting Dynamic Controllers

In this section, we provide a simplified version of the method proposed in [9], for implementing dynamic controllers to operate over encrypted signals and parameters.

A. Conversion of State Matrix

We first briefly recall the necessity of converting the state matrix F of (2) to integers without scaling of components.

A typical way of implementing the controller (2) over integers (or floating-point numbers) is to consider quantization as well as the use of scale factors. To see the detail, we consider the part (2a) represented to operate over quantized signals; let $\mathsf{r} > 0$ denote the quantization step size for the input $y(t) \in \mathbb{R}^{\mathsf{p}}$ so that the controller receives $\overline{y}(t) = \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor \in \mathbb{Z}^{\mathsf{p}}$

as integers. And, for simplicity, suppose that precision of the matrices F and G in (2a) can be preserved with a scale factor $1/\mathsf{s}_1 \in \mathbb{N}$, i.e., suppose that $\overline{F} := F/\mathsf{s}_1 \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$ and $\overline{G} := G/\mathsf{s}_1 \in \mathbb{Z}^{\mathsf{n}\times\mathsf{p}}$ with some $1/\mathsf{s}_1 \in \mathbb{N}$ larger than 1. Then, the part (2a) can be easily implemented over integers as

$$\overline{x}(t+1) = \lceil \mathsf{s}_1 \overline{F}\overline{x}(t) \rfloor + \overline{G}\overline{y}(t), \tag{3}$$

with $\overline{x}(0) = \lceil x_0/(\mathsf{rs}_1) \rfloor \in \mathbb{Z}^{\mathsf{n}}$. It can be seen that the state $\overline{x}(t) \in \mathbb{Z}^{\mathsf{n}}$ has its values as integers for the whole time, while it has the value of $x(t)/(\mathsf{rs})$; if we let $e_x(t) = \mathsf{r}\cdot G(\lceil y(t)/\mathsf{r} \rfloor - y(t)/\mathsf{r})$ for (2a), it follows that $\mathsf{rs}_1 \overline{x}(t) = x(t)$ for all $t \geq 0$, where the quantization error $\|e_x(t)\|$ can be made arbitrarily small, by choosing $1/\mathsf{r}$ sufficiently large.

However, following the usual way for implementing dynamic controllers over quantized signals, dynamic controllers may not be capable of operating over encrypted data for infinite time horizon; in (3), it is expected that the operations $\overline{F}\cdot\overline{x}$ or $\overline{G}\cdot\overline{y}$ consisting of additions and multiplication over integers can be performed over encrypted data, exploiting the homomorphic properties of homomorphic cryptosystem. But unfortunately, when it comes to the operation $\lceil \mathsf{s}_1(\cdot) \rfloor$, division of integers by $1/\mathsf{s}_1 \in \mathbb{N}$ and truncation of least significant bits, it is impossible for cryptosystems allowing only addition or multiplication to perform the division unlimited number of times. Since the operation $\lceil \mathsf{s}_1(\cdot) \rfloor$ is necessary for managing the size of data for $\overline{x}(t)$ with finite precision, that is, for keeping the scale of $\overline{x}(t)$ as $1/(\mathsf{rs}_1)$, it is concluded that encrypted controllers that utilize scaling of the state matrix F encounter overflow problems in finite time, so incapable of operating for infinite time horizon.

To overcome this problem, we follow the method in [9] to convert the state matrix F to integers, in which the decimal portion of F is kept without scaling. First, without loss of generality, we may assume that the pair (F, H) in (2) is observable[2]. Then, the system (2) is transformed as

$$\begin{aligned} z(t+1) &= T(F-RH)T^{-1}z(t) + T(G-RJ)y(t) \\ &\quad + TRu(t) + Te_x(t) - TRe_u(t) \qquad \text{(4a)} \\ u(t) &= HT^{-1}z(t) + Jy(t) + e_u(t), \qquad \text{(4b)} \end{aligned}$$

where an invertible matrix $T \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$ is used for the transformation $z(t) = Tx(t) \in \mathbb{R}^{\mathsf{n}}$, and the matrix $R \in \mathbb{R}^{\mathsf{n}\times\mathsf{m}}$ is used for changing the state matrix from TFT^{-1} to $T(F-RH)T^{-1}$, where the signal $u(t)$ in (4a) is regarded as an external input.

Then, the following lemma suggests that given any controller (2), it can be converted to the form (4), with the state matrix converted to integers without scaling.

Lemma 1: Given an observable pair $F \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$ and $H \in \mathbb{R}^{\mathsf{m}\times\mathsf{n}}$, there exist $T \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$ and $R \in \mathbb{R}^{\mathsf{n}\times\mathsf{m}}$ such that $T(F-RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$. □

Sketch of Proof: The matrix R can be designed with pole-placement techniques by which the eigenvalues of $F - RH$ are all integers, and the transformation T is found such that the matrix $T(F-RH)T^{-1}$ is of Jordan canonical form, so that it consists of integers. A formal proof for a general version of this lemma can be found in the proofs of Proposition 2 and Lemma 1 in [9]. ■

B. Conversion to System over $\mathbb{Z}_q$

The next procedure for encrypting controller is to convert the system (4) so that all matrices and signals are converted to the elements of the set $\mathbb{Z}_q$, the messages to be encrypted.

First, taking the benefit of state matrix consisting of integers, the system (4) is easily converted to a system that operates over integers, utilizing only addition and multiplication for the operation; let the matrices in (4), except the state matrix, be converted to integers, as

$$\overline{G} := \left\lceil \frac{T(G-RJ)}{\mathsf{s}_1} \right\rfloor, \quad \overline{R} := \left\lceil \frac{TR}{\mathsf{s}_1} \right\rfloor, \quad \overline{H} := \left\lceil \frac{HT^{-1}}{\mathsf{s}_2} \right\rfloor,$$

and $\overline{J} := \lceil \frac{J}{\mathsf{s}_1\mathsf{s}_2} \rfloor$, where $1/\mathsf{s}_1 \geq 1$ and $1/\mathsf{s}_2 \geq 1$ are scaling factors to keep the decimal portions from the rounding. Then, with $\overline{F} := T(F-RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$, the controller (4) is converted as

$$\begin{aligned} \overline{z}(t+1) &= \overline{F}\overline{z}(t) + \overline{G}\overline{y}(t) + \overline{R}\overline{u}'(t) + \Delta_x(t), \\ \overline{u}(t) &= \overline{H}\overline{z}(t) + \overline{J}\overline{y}(t) + \Delta_u(t), \\ \overline{z}(0) &= \frac{1}{\mathsf{L}}\left\lceil \frac{Tx_0}{\mathsf{rs}_1} \right\rfloor + \Delta_0, \end{aligned} \tag{5}$$

where $\overline{y}(t) := \lceil y(t)/\mathsf{r} \rfloor / \mathsf{L} \in \mathbb{Z}^{\mathsf{p}}$ is the quantized input scaled with an additional scale factor[3] $1/\mathsf{L} \in \mathbb{N}$, $\Delta_x(t) \in \mathbb{Z}^{\mathsf{n}}$, $\Delta_u(t) \in \mathbb{Z}^{\mathsf{m}}$, and Δ_0 are errors to be determined in the next section, and the signal $\overline{u}'(t) := \lceil \mathsf{s}_1\mathsf{s}_2\overline{u}(t) \rfloor \in \mathbb{Z}^{\mathsf{m}}$, which is in fact obtained from the output $\overline{u}(t) \in \mathbb{Z}^{\mathsf{m}}$, is regarded as external input of the controller. Operating over integers using multiplication and addition only, the following lemma suggests that the state $\overline{z}(t)$ and the output $\overline{u}(t)$ of (5) have the values of $z(t)/(\mathsf{Lrs}_1) = Tx(t)/(\mathsf{Lrs}_1)$ and $u(t)/(\mathsf{Lrs}_1\mathsf{s}_2)$, which corresponds to the state and output of (4) or (2), respectively, where the performance error can be made arbitrarily small with the choice of $\{\mathsf{L}, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2\}$.

Lemma 2: Suppose that Assumption 1 hold, and that $\|\Delta_x(t)\| \leq \Delta_x'$, $\|\Delta_u(t)\| \leq \Delta_u'$, and $\|\Delta_0\| \leq \Delta_0'$ with some $\Delta_x' \geq 0$, $\Delta_u' \geq 0$, and $\Delta_0' \geq 0$. Then, there exists a function $\alpha : \mathbb{R}^7 \to \mathbb{R}^3$ of polynomials vanishing at the origin such that for every $\{\mathsf{L}, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2\}$ satisfying $\|\alpha(\mathsf{L}, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2, \Delta_x', \Delta_u', \Delta_0')\| \leq \eta(\epsilon)$, the controller (5) guarantees that $\|\mathsf{Lrs}_1 T^{-1}\cdot\overline{z}(t) - x'(t)\| \leq \epsilon$ and $\|\mathsf{Lrs}_1\mathsf{s}_2\overline{u}(t) - u'(t)\| \leq \epsilon$ hold, for all $t \geq 0$. □

Sketch of Proof: By $x(t) = \mathsf{Lrs}_1 \cdot T^{-1}\overline{z}(t)$ and $u(t) = \mathsf{Lrs}_1\mathsf{s}_2\cdot\overline{u}(t)$, the systems (2) and (5) can be seen as equivalent, where $\{e_x, e_u, e_0\}$ in (2) are bounded by a function, denoted as α, having the arguments of $\{\mathsf{L}, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2, \Delta_x', \Delta_u', \Delta_0'\}$. It can be verified that the function α vanishes when $(\mathsf{L}, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2) = (0, 0, 0, 0)$. Thus, we can have $\|\alpha\| \leq \eta(\epsilon)$ with sufficiently large $\{1/\mathsf{L}, 1/\mathsf{r}, 1/\mathsf{s}_1, 1/\mathsf{s}_2\}$, which ends the proof, by Assumption 1. ■

Next, it is addressed that the signals and matrices in (5) of integers can be treated as the elements of the set $\mathbb{Z}_q$ with modular addition and multiplication. Suppose that each component of the output $\overline{u}(t) = \mathrm{col}\{\overline{u}_i(t)\}_{i=1}^{\mathsf{m}} \in \mathbb{Z}^{\mathsf{m}}$ in (5)

[2] This is because, for general case, we can consider Kalman observable decomposition and obtain an observable subsystem. See [9, Section IV].

[3] In the next section, it will be seen that the use of $1/\mathsf{L} \in \mathbb{N}$ is in fact for suppressing the effect of injected errors during encryption.

is bounded as

$$\overline{u}_i^{\min} \leq \overline{u}_i(t) \leq \overline{u}_i^{\max}, \qquad \forall t \geq 0, \tag{6}$$

with some integers $\{\overline{u}_i^{\min}\}_{i=1}^{\mathsf{m}}$ and $\{\overline{u}_i^{\max}\}_{i=1}^{\mathsf{m}}$. Then, even though the signal $\overline{u}(t) \in \mathbb{Z}^{\mathsf{m}}$ is projected to the space $\mathbb{Z}_q^{\mathsf{m}}$ as $\overline{\mathsf{u}}(t) = \overline{u}(t) \mod q$, it can be recovered as

$$\mathrm{mod}(\overline{\mathsf{u}}(t), q, \overline{u}^{\min}) := \overline{\mathsf{u}}(t) - \left\lfloor \frac{\overline{\mathsf{u}}(t) - \overline{u}^{\min}}{q} \right\rfloor q = \overline{u}(t),$$

where $\overline{u}^{\min} := \mathrm{col}\{\overline{u}_i^{\min}\}_{i=1}^{\mathsf{m}}$, as long as the modulus q is sufficiently large to cover the range of $\overline{u}(t)$, as

$$q \geq \max_{i=1,\cdots,\mathsf{m}} \{\overline{u}_i^{\max} - \overline{u}_i^{\min} + 1\}. \tag{7}$$

Along this observation, we consider the following system

$$\begin{aligned} \overline{\mathsf{z}}(t+1) &= \overline{F}\overline{\mathsf{z}}(t) + \overline{G}\overline{y}(t) + \overline{R}\overline{\mathsf{u}}'(t) + \Delta_x(t) \mod q \\ \overline{\mathsf{u}}(t) &= \overline{H}\overline{\mathsf{z}}(t) + \overline{J}\overline{y}(t) + \Delta_u(t) \mod q \\ \overline{\mathsf{z}}(t) &= \frac{1}{\mathsf{L}} \left\lceil \frac{Tx_0}{\mathsf{rs}_1} \right\rfloor + \Delta_0 \mod q \end{aligned} \tag{8}$$

over $\mathbb{Z}_q$, where the signal $\overline{\mathsf{u}}'(t) \in \mathbb{Z}_q^{\mathsf{m}}$ defined as

$$\overline{\mathsf{u}}'(t) := \lceil \mathsf{s}_1\mathsf{s}_2 \cdot \mathrm{mod}(\overline{\mathsf{u}}(t), q, \overline{u}^{\min}) \rfloor \tag{9}$$

is regarded as an external input. Then, as the modulo operation is homomorphic with respect to addition and multiplication over integers, the following lemma states that the operations of (5) can be replaced with that of (8).

Lemma 3: If (6) and (7) hold, then the controller (8) over $\mathbb{Z}_q$ guarantees $\overline{u}(t) = \mathrm{mod}(\overline{\mathsf{u}}(t), q, \overline{u}^{\min})$, for all $t \geq 0$. □

Sketch of Proof: By construction, it satisfies $\overline{\mathsf{u}}(0) = \overline{u}(0) \mod q$. From the conditions (6) and (7), it can be seen that $\overline{u}(0) = \mathrm{mod}(\overline{\mathsf{u}}(0), q, \overline{u}^{\min})$, which leads to $\overline{\mathsf{u}}'(0) = \overline{u}'(0)$. Then, it follows that $\overline{\mathsf{u}}(1) = \overline{u}(1) \mod q$, and the proof is completed by induction principle. ■

Since the given controller (2) have been converted to a system over $\mathbb{Z}_q$ with modular arithmetic in which all the signals and matrices have been converted to integers as well, the construction of encrypted controller directly follows. Let the matrices and the input of (5) be encrypted as

$$\begin{aligned} &\mathbf{F} := \mathsf{Enc}'(\overline{F} \mod q), \qquad &&\mathbf{H} := \mathsf{Enc}'(\overline{H} \mod q), \\ &\mathbf{G} := \mathsf{Enc}'(\overline{G} \mod q), \qquad &&\mathbf{J} := \mathsf{Enc}'(\overline{J} \mod q), \\ &\mathbf{R} := \mathsf{Enc}'(\overline{R} \mod q), \qquad &&\mathbf{y}(t) := \mathsf{Enc}(\overline{y}(t) \mod q). \end{aligned}$$

Then, the given controller is finally encrypted as

$$\begin{aligned} \mathbf{z}(t+1) &= \mathbf{F}\cdot D(\mathbf{z}(t)) + \mathbf{G}\cdot D(\mathbf{y}(t)) + \mathbf{R}\cdot D(\mathbf{u}'(t)) \bmod q \\ \mathbf{u}(t) &= \mathbf{H} \cdot D(\mathbf{z}(t)) + \mathbf{J} \cdot D(\mathbf{y}(t)) \bmod q \\ \mathbf{z}(0) &= \mathsf{Enc}\left(\frac{1}{\mathsf{L}} \left\lceil \frac{Tx_0}{\mathsf{rs}_1} \right\rfloor \bmod q \right), \end{aligned} \tag{10}$$

in which $\mathbf{u}'(t) := \mathsf{Enc}(\lceil \mathsf{s}_1\mathsf{s}_2 \cdot \mathrm{mod}(\mathsf{Dec}(\mathbf{u}(t)), q, \overline{u}^{\min}) \rfloor)$ is defined as the same as in (9).

Assuming that the output $\mathbf{u}(t)$ be decrypted (at the plant side, e.g., at the actuator having decryption key), re-encrypted, and transmitted to the controller where it is regarded as an external input of encrypted system, it is clear that the constructed system performs dynamic operation over encrypted data without decryption of the state $\mathbf{z}(t)$. Most of all, the encrypted controller is able to operate for infinite time horizon, provided that its performance is (practically) equivalent to that of (2).

Finally, for the rest of this section, we suggest that the operation of (10) can be identified with that of (8). Indeed, by Propositions 1.1, 1.2, and 2 for the homomorphic properties of the cryptosystem, it can be easily verified that the messages $\mathsf{Dec}(\mathbf{z}(t))$ and $\mathsf{Dec}(\mathbf{u}(t))$ obeys the form (8), so that it can be defined as $\overline{\mathsf{z}}(t) := \mathsf{Dec}(\mathbf{z}(t))$ and $\overline{\mathsf{u}}(t) := \mathsf{Dec}(\mathbf{u}(t))$, where the perturbations $\{\Delta_x(t), \Delta_u(t), \Delta_0\}$ are regarded as effect of the injected errors, bounded as

$$\begin{aligned} \|\Delta_x(t)\| &\leq (\mathsf{n}+\mathsf{p}+\mathsf{m})n'\nu\Delta_{\mathsf{Enc}} + (\|\overline{G}\| + \|\overline{R}\|)\Delta_{\mathsf{Enc}}, \\ \|\Delta_u(t)\| &\leq (\mathsf{n}+\mathsf{p})n'\nu\Delta_{\mathsf{Enc}} + \|\overline{J}\|\Delta_{\mathsf{Enc}}, \end{aligned} \tag{11}$$

and $\|\Delta_0\| \leq \Delta_{\mathsf{Enc}}$. Hence, provided that the conditions in Lemma 2 and 3 hold, the operation of encrypted controller (10) can be seen as equivalent to the given controller (2), where the perturbations $\{e_x(t), e_u(t), e_0\}$ in (2) can be specified as the errors due to quantization error and effect of error injection.

Performance analysis of (10) with the choice of parameters $\{1/\mathsf{L}, 1/\mathsf{s}_1, 1/\mathsf{s}_2, 1/\mathsf{r}\}$ is to be deal with in the next section, together with the issue of the security of encrypted controller. It will be seen that the controller (10) is capable of operating for infinite time horizon, while it keeps the desired level of performance and security for the whole time.

IV. Parameter Design of Encrypted Controller

In this section, parameter design for the encrypted controller (10) is considered. Given $\epsilon > 0$ for the performance from Assumption 1 and the security parameter $\lambda > 0$ from the algorithm Setup of cryptosystem, the parameters to be determined are listed as follows;

- the matrices T and R for the conversion of state matrix,
- the scaling factors $\{1/\mathsf{L}, 1/\mathsf{s}_1, 1/\mathsf{s}_2, 1/\mathsf{r}\}$ for converting signals and the rest matrices to integers,
- the vector $\overline{u}^{\min}$ of lower bounds for the decrypted output, which defines the function $\mathrm{mod}(\,\cdot\,, q, \overline{u}^{\min})$.
- the parameters $\{q, \sigma_0, n, \nu, d, n'\}$ for the LWE-based cryptosystem.

Each set $\{1/\mathsf{L}, 1/\mathsf{s}_1, 1/\mathsf{s}_2, 1/\mathsf{r}\}$ and $\{q, \sigma_0, n, \nu, d, n'\}$ can be chosen to keep the desired level of either performance or security, respectively, but they may conflict with each other, in practice. For example;

- as proposed in the previous result [9], the performance of (10) is guaranteed as the parameters $\{1/\mathsf{L}, 1/\mathsf{s}_1, 1/\mathsf{s}_2, 1/\mathsf{r}\}$ increase. However, increasing these parameters for the sake of the performance may enlarge the size of modulus q and affect the security level of the cryptosystem. Indeed, as in (1), the increase of q may decrease the parameter λ for the security level. Thus, increasing the parameters $\{1/\mathsf{L}, 1/\mathsf{s}_1, 1/\mathsf{s}_2, 1/\mathsf{r}\}$ only, it may affect the security of encrypted controller.
- according to (1), the security parameter λ heavily depends on the parameter n for the dimension of ciphertexts. So, the desired security level is commonly achieved by enlarging the dimension n. However, the increase of n means the increase of the number of injected errors during encryption, so it increases the

effect of injected errors, and results in performance degradation. For example, in Proposition 2, it can be seen that the size of error Δ increases when the parameter $n' = n(d+1)$ increases.

To deal with these issues or trade-offs, we provide a guideline for choosing all the parameters so that it keeps both the performance and security of the proposed encrypted controller, as follows. Given $\lambda > 0$ and $\epsilon > 0$, we choose all the parameters so that the encrypted controller (10) achieves the λ-bit security of the controller while the performance error with respect to the model (2) should be less than ϵ.

1) The parameters $\sigma_0 > 0$ and $\nu \in \mathbb{N}$ are considered to be determined as constants first, where ν is determined as $\nu = 2^{\nu_0}$ with some $\nu_0 \in \mathbb{N}$. This determines the parameters d and n', as $d = \lceil \log_\nu q \rceil$ and $n' = d(n+1)$, as functions of q and n, respectively.
2) The parameters $\{T, R\}$ for the conversion of state matrix is determined, along the method in the proof of Lemma 1. Then, the parameters $\{\mathsf{r}, \mathsf{s}_1, \mathsf{s}_2\}$ for the converted controller (5) are chosen such that
$$\|\alpha(1, \mathsf{r}, \mathsf{s}_1, \mathsf{s}_2, 0, 0, 0)\| < \eta(\epsilon). \qquad (12)$$
3) The modulus q is defined as a function of $1/\mathsf{L}$, as
$$\log q := \left\lceil \log_2 \left(\frac{\max\{u_i^{\max} - u_i^{\min}\} + \mathsf{r} + 2\epsilon}{\mathsf{L}\mathsf{s}_1\mathsf{s}_2\mathsf{r}} \right) \right\rceil, \qquad (13)$$
and $\overline{u}^{\min} = \mathrm{col}\{\overline{u}_i^{\min}\}_{i=1}^{\mathsf{m}}$ for (9) is defined as
$$\overline{u}_i^{\min} := \left\lfloor \frac{u_i^{\min} - \frac{\mathsf{r}}{2} - \epsilon}{\mathsf{L}\mathsf{s}_1\mathsf{s}_2\mathsf{r}} \right\rfloor.$$
4) The ciphertext dimension n is determined from (1), as
$$n := \left\lceil \frac{0.63\lambda - 0.21}{\log q} \log^2 \left(\frac{\sqrt{2\pi}\sigma_0}{q} \right) + n_0 \right\rceil, \qquad (14)$$
with some $n_0 \geq 0$, so that it is a function of q.
5) Every parameter has been determined or is now a function of $1/\mathsf{L}$. The upper bounds Δ'_x, Δ'_u, and Δ'_0 in Lemma 2, computed as (11), are also functions of $1/\mathsf{L}$, which tend to zero as L tends to zero. Finally, choose $1/\mathsf{L} \in \mathbb{N}$ such that
$$\|\alpha(\mathsf{L}, \mathsf{s}_1, \mathsf{s}_2, \mathsf{r}, \Delta'_x, \Delta'_u, \Delta'_0)\| \leq \eta(\epsilon). \qquad (15)$$

As the end result, the following theorem states that the choice of parameters with the described algorithm is always feasible, so that it guarantees both the desired level of performance and security of the controller (10).

Theorem 1: Suppose that Assumption 1 hold. Then, given $\epsilon > 0$ and $\lambda > 0$, the encrypted controller (10) designed with (12)–(15) guarantees that (1) holds, and
$$\|\mathsf{L}\mathsf{r}\mathsf{s}_1\mathsf{s}_2 \cdot \mathrm{mod}(\mathsf{Dec}(\mathbf{u}(t)), q, \overline{u}^{\min}) - u'(t)\| \leq \epsilon \qquad (16)$$
hold, for all $t \geq 0$. □

Sketch of Proof: By Lemma 2 and 3, it is clear that (16) is satisfied if the condition (15) with respect to the controller (10) holds. At the stage of choosing the last parameter L such that (15) holds, it can be verified that α becomes a function of L such that $\|\alpha(\mathsf{L})\| \leq k_1 \mathsf{L} \cdot (k_2 + (\log \mathsf{L})^{k_2})$ with some constants $k_1 > 0$, $k_2 > 0$, and $k_3 > 0$. Thus, by enlarging $1/\mathsf{L}$, it is able to determine all the parameters to satisfy all conditions (12)–(15), which ends the proof. ■

Remark 1: The design method for (12) is understood as follows. Note that the function α in Lemma 2 in fact considers the size of error due to quantization and error injection, which corresponds to the upper-bound of the norm of $\{e_x, e_u, e_0\}$, with respect to the model (2). The design (12) first neglects the effect of Δ-terms, the effect of errors, in (5), so that it keeps the desired level of performance with respect to quantization errors. The rest parameters are next determined, so that the size of quantization error plus effect of injected errors is not larger than $\eta(\epsilon)$, so that it keeps the performance for the general setting. □

V. Conclusion

In this paper, we have proposed a design procedure for encrypting dynamic controllers based on LWE-based homomorphic encryption. The proposed design is based on the method for converting the state matrix of the controller without scaling. Taking the benefit of the conversion, the designed controller is capable of performing dynamic operation over encrypted data for infinite time horizon. The proposed design procedure includes an algorithm for choosing all the parameters for the cryptosystem as well as the parameters for digital implementation of the controller, in a constructive way. Given the desired level of performance and security, it has proven that the choice of parameters is always feasible so that the designed encrypted controller achieves both desired level performance and security.

References

[1] 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.

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

[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] 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, iss. 2, pp. 195–200, 2018.

[5] A.B. Alexandru, M. Morari, G.J. Pappas, “Cloud-based MPC with encrypted data,” in *Proc. 57th IEEE Conf. Decision and Control*, 2018, pp. 5014–5019.

[6] C.N. Hadjicostis and A.D. Domínguez-García, “Privacy-Preserving Distributed Averaging via Homomorphically Encrypted Ratio Consensus,” *IEEE Trans. Autom. Cont.*, vol. 65, no. 9, pp. 3887–3894, 2020.

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

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

[9] J. Kim, H. Shim, and K. Han, “Dynamic controller that operates over homomorphically encrypted data for infinite time horizon,” arXiv:1912.07362v1 [eess.SY], 2019.

[10] C. Murguia, F. Farokhi, and I. Shames, “Secure and private implementation of dynamic controllers using semi-homomorphic encryption,” *IEEE Trans. Autom. Cont.*, vol. 65, no. 9, pp. 3950–3957, 2020.

[11] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *Jortnal of the ACM*, vol. 56, no. 6, pp. 34, 2009.

[12] 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.

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

[14] R. Lindner and C. Peikert, “Better key sizes (and attacks) for LWE-based encryption,” in *Topics in Cryptology–CT–RSA*, Springer, Berlin, Heidelberg, 2011, pp. 319–339.

[15] Learning with Errors Estimator, `https://bitbucket.org/malb/lwe-estimator/src/master/`, commit a276755, 2020.