Secure Networked Control of Large-Scale Cyberphysical Systems Using Cryptographic Techniques

Yamin Yan, Zhiyong Chen, and Vijay Varadharajan

Abstract—This paper aims to create a secure environment for networked control systems composed of multiple dynamic entities and computational control units via networking, in the presence of disclosure attacks. In particular, we consider the situation where some dynamic entities or control units are vulnerable to attacks and can become malicious. Our objective is to ensure that the input and output data of the benign entities are protected from the malicious entities as well as protected when they are transferred over the networks in a distributed environment. Both these security requirements are achieved using cryptographic techniques. However, the use of cryptographic mechanisms brings additional challenges to the design of controllers in the encrypted state space; the closed-loop system gains and states are required to match the specified cryptographic algorithms. In this paper, we propose a methodology for the design of secure networked control systems integrating the cryptographic mechanisms with the control algorithms. The approach is based on the separation principle, with the cryptographic techniques addressing the security requirements and the control algorithms satisfying their performance requirements. This paper presents the design of private controllers for two typical control problems, namely stabilization and consensus, as well as the discussion of numerical simulations and results.

Index Terms—Networked control systems, Large-scale systems, Cyberphysical security, Encryption, Quantization, Stabilization, Consensus

I. INTRODUCTION

Large-scale systems (LSSs) have been rapidly developed in interdisciplinary fields with the technological advances in computer science, software engineering, and systems engineering. The concept of LSS adopted in this paper involves dynamic systems involving a large number of states, control inputs, and parameters; see, e.g., [1, 2]. Such systems usually consist of a class of interconnected subsystems with physical coupling among them. It also includes the class of multi-agent systems (MASs) in [3, 4], and complex systems in [5–7]. In these systems, people are more interested in their collective phenomena and behaviors. A common feature of these LSSs is that they have multiple dynamic entities. Therefore, attacks can occur on a partial set of entities rather than the whole system, which necessitates the need to protect parts of the system even though some other parts are under attack.

For either a small-scale or a large-scale system, the controller may be implemented on a remote computing unit if the system itself does not have local computing facilities. Such an architecture is known as a networked control system (NCS) [8, 9]. It is also called a cyberphysical system especially as it involves physical dynamics and computer based algorithms via networking. The main challenges in studying NCSs lie in understanding the control principles with sampling, quantization, communication time-delay, packet dropout, etc. NCSs can find extensive applications in different fields, including smart grids [10], transportation [11], smart cities [12], healthcare [13], manufacturing [14], and so on.

The present research is on large-scale systems with networked control (LSS-NC), which is the synthesis of the aforementioned two concepts and involves all the associated research issues. It has become a class of representative complicated engineering systems involving various state-of-the-art technologies. For instance, controllers for a group of drones lacking onboard computing capacity are usually implemented on decentralized remote computing base stations [15, 16]. A railway system is a typical large-scale system with strong physical coupling among trains, whose dispatch planning and control is typically implemented in remote central stations through various network communication [17]. The main target of this research is not on the traditional control issues for LSSs and/or NCSs but on the need to develop a secure environment. LSS-NC is indeed a niche platform for the research from the security perspective because it allows us the possibility of protecting a whole system even when its partial dynamic entities or remote control units are subject to attack.

Security and privacy have become critical issues for modern industrial systems. Improperly addressing these issues could result in massive economic losses or even threats of human safety. Specifically, attack may occur ubiquitously and we consider the circumstance for LSS-NC that some dynamic entities or control units are hacked and can become malicious. The secure environment studied in this paper involves the system entities having mechanisms to protect their private input/output information from the malicious entities and controllers.

In the literature, the significance of addressing the cyberphysical security of NCSs has been widely recognized [18–20]. For example, cyberattacks such as Stuxnet malware [21] to typical NCSs operated through supervisory control and data acquisition (SCADA) systems have been well studied in, e.g., [22, 23]. Researchers are interested in knowing how much damage attacks can cause by injecting malicious signals or commands into an NCS and what can be done to mitigate that damage [24, 25]. The research in this paper is mainly concerned about data confidentiality violation by disclosure attacks. There has been an increasing interest for development of sophisticated control and estimation algorithms with encrypted data for defending disclosure attacks in [26, 27] among others.

Also, the research on secure LSSs has been attempted in recent literature, in particular, on consensus of MASs [28–30]. Privacy and security challenges associated with consensus protocol are of great practical and theoretical importance in a wide range of applications. An MAS requires information exchange via network to achieve consensus. Meanwhile, it is usually important to avoid information leakage during information exchange in a secure control environment. Apart from these cryptography based approaches, noise-based obfuscation approaches are also well studied that mask the true state values by adding or subtracting random noises to the control process. The research along this line has also been rapidly developed over the past years; see, e.g., [31, 32].

In the design of secure networked control systems, we consider two specific security requirements. The first requirement is concerned with the protection of information being transferred over the networks. For instance, the input and output data transferred between the system (plant) and the controller over untrusted networks. The second requirement is concerned with the protection of data between the components within a system. For instance, consider a system
consisting of say three sub components X, Y and Z. This requirement is concerned with securing the data generated by the component X from the data generated from components Y and Z. Similarly for data generated by components Y and Z. Such protection will be needed if there is mutual distrust between the various components within a system. Hence the first requirement addresses protection between systems, whereas the second requirement is concerned with protection within a system. To achieve both these security requirements, we have developed a double-layer security scheme using cryptographic mechanisms. One cryptographic layer offers protection against attacks on external networks, connecting the system plant(s) with the control units. The other layer provides cryptographic mechanisms offering protection of data from each of the components within the system.

Compared to the aforementioned literature on secure control of NCSs, our contribution proposes an approach to security that is more comprehensive. Often the works on NCSs have not differentiated the system entities, only considering the case when the remote controller is attacked, which is the first security objective. On the other hand, the works on the LSSs have mainly focused on the controller being synthesized within the entity, thereby not addressing separately attacks on the controller, which is only the second security objective.

When it comes to the implementation of the two security layers, in general, one has a choice of several cryptosystems to choose from. Many cryptosystems have been developed with different characteristics, which have been used in different applications [48]. Among them, RSA (Rivest-Shamir-Adleman) [49] is a widely used public-key cryptosystems in many different systems and applications. In such a cryptosystem, the encryption key is public and it is different from the decryption key, which is kept secret. The asymmetry in the RSA is based on the practical difficulty of factorizing a large number into its prime factors. Another asymmetric cryptosystem is the Paillier cryptosystem [50], which is a probabilistic semi-homomorphic algorithm. This scheme has an additive homomorphic property; this means that, given only the public-key and two encrypted messages, one can obtain the summation of the two messages by computing the multiplication of two encrypted messages. Such an additive property allows a remote system to operate on encrypted signals without requiring the access to the original signals (in plaintext form). From control systems perspective, one is more interested in how to achieve greater performance of control systems using these cryptosystems.

In this paper, we have used the RSA and Paillier cryptosystems to realize the two security layers, as both these systems are well known and have been used in many research works in control systems. In terms of formal security properties, though Paillier is semantically secure, algorithms such as RSA are not. The notion of semantic security implies that any information revealed cannot be feasibly extracted and is equivalent to the property of ciphertext indistinguishability under chosen-plaintext attack. However, algorithms such as RSA can be made to be semantically secure through the use of random encryption padding schemes such as Optimal Asymmetric Encryption Padding [51]. For the purposes of this paper, it is sufficient to argue that the schemes we have used are informally secure in that given a ciphertext and the public encryption key, a computationally bounded adversary will not be able to determine the actual plaintext or at least the probability of this happening can be made to be very low using well-constructed public key systems (e.g. for RSA, choosing suitable design parameters such as appropriate large primes and suitable exponents etc.).

The contributions of this paper are as follows:

First, we propose a novel double-layer security scheme using cryptographic mechanisms to satisfy both of our security objectives mentioned above. We have instantiated such a double-layer scheme by Paillier-RSA encryption techniques. First, the original signals coming from different components in a system are encrypted in an inner layer to protect the transfer of data over an insecure communication network. Then there is an outer-layer protecting the data between the components. The inner-layer offers protection against external attackers and the outer-layer offers protection between various system components. The combination of both these protection layers provides security of the overall networked control system.

Second, a systematic methodology is proposed for the design of a secure networked control system based on the principle of separation consisting of four procedures, namely, quantization, encryption, control, and decryption. This is being decomposed into two independent sub-problems, namely, a nonencrypted control problem and a quantization-encryption-decryption problem. Both sub-problems should be characterized in the same bounded space as described in Section IV to avoid computation overflow or underflow. We have provided a rigorous mathematical proof illustrating this. Another characteristic of this cryptographic design strategy is that it is independent of control problem. That is, we can separately handle different controller design problems to achieve different desired control objectives while simultaneously achieving the security objectives.

Third, we apply the proposed double-layer cryptographic mechanisms and the secure control approach to solve two classes of practical problems, namely, the encrypted centralized control problem for stabilization of multi-input multi-output (MIMO) systems, and the encrypted decentralized control problem for consensus of multiple agent systems (MASs). The effectiveness of the proposed design is illustrated theoretically and by numerical simulations for both these case studies.

The remainder of the paper is organized as follows. Section II presents preliminary concepts and algorithms. Section III gives the rigorous problem formulation. Section IV presents a general encrypted LSS-NC architecture followed by specific controller design. Two case studies are given in Sections V and VI where the stabilization problem of MIMO systems and the consensus problem of MASs are considered based on the proposed methodology, followed by numerical examples. Finally, we close the paper with some concluding remarks in Section VII.

Notation. The vector lumped by the vectors $c_1, \ldots, c_r$ is denoted by $\mathbf{c}(c_1, \ldots, c_r) = [c_1^T, \ldots, c_r^T]^T$. For a set $S$, its element $a$ is denoted by $a \in S$. For a vector $a = [a_1, \ldots, a_r]^T$, writing $a \in S$ means that $a_i \in S$, $i = 1, \ldots, r$. For a scalar variable and scalar valued function $\mathcal{E}$, element-wise operation is used throughout the paper, that is, $\mathcal{E}(a) = [\mathcal{E}(a_1), \ldots, \mathcal{E}(a_r)]^T$. For a vector $a$, its Euclidean norm is denoted by $\|a\|$ and its maximum norm by $\|a\|_{\infty}$. For a real matrix $A$, its induced 2-norm is denoted by $\|A\|_2$, and its element-wise absolute value by $|A|$. Let $1$ be a column vector whose elements are all 1 and dimension is from the context.

II. Preliminaries

Using cryptographic algorithms to encrypt and decrypt messages during the control process provides the technical foundation for creating a secure environment. In this section, we first revisit some preliminaries of the two cryptosystems RSA [49] and Paillier [50]. Quantization of signals is also discussed in this section.

RSA is a well-known public-key cryptosystem, based on the computational difficulty of factorizing a large composite number. In RSA, the encryption key is public and it is different from the decryption key, which is kept secret (private). The encryption process can be denoted by a function $E_R: \mathbb{Z}_{n_R} \rightarrow \mathbb{Z}_{n_R}$ for a prescribed positive integer $n_R$ and the decryption process by its inverse $E_R^{-1}$.
Throughout the paper, we denote the set of integers modulo $n$ as $\mathbb{Z}_n = [0, 1, \ldots, n - 1]$. The detailed algorithm is as shown in Algorithm 1.

**Algorithm 1** RSA Cryptosystem: $\mathcal{E}_R : \mathbb{Z}_{nR} \mapsto \mathbb{Z}_{nR}$

### 1. Key Generation
Step 1: Generate two distinct large prime numbers $p_R, q_R$, such that $\gcd(p_Rq_R, (p_R - 1)(q_R - 1)) = 1$.
Step 2: Let $n_R = p_Rq_R, \phi(n_R) = (p_R - 1)(q_R - 1)$.
Step 3: Select randomly the encryption key $e_R$, where $1 < e_R < \phi(n_R), \gcd(e_R, \phi(n_R)) = 1$.
Step 4: Compute $d_R$ to satisfy the congruence relation $d_R e_R \equiv 1 \pmod{\phi(n_R)}$.
Step 5: The public key is $K_{pub} = (e_R, n_R)$ and the private key $K_{pri} = (d_R, p_R, q_R)$.

### 2. Encryption $\mathcal{E}_R$
$\mathcal{E}_R(m_R) = m_R^{e_R} \mod n_R, m_R \in \mathbb{Z}_{nR}$.

### 3. Decryption $\mathcal{E}_R^{-1}$
$\mathcal{E}_R^{-1}(m_R) = E_R(m_R)^{d_R} \mod n_R, m_R \in \mathbb{Z}_{nR}$.

The Pailletier cryptosystem, named after the inventor Pascal Paillier, is a probabilistic asymmetric algorithm for public key cryptography. It is based on the fact that computing $n$-th residue classes is computationally difficult. Also, in Paillier cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). The encryption process can be denoted by a function $\mathcal{E}_p : \mathbb{Z}_{n_P} \mapsto \mathbb{Z}_{n_P}^*$, for a prescribed positive integer $n_P$ and the decryption process by its inverse $\mathcal{E}_p^{-1}$. Here, $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. The Paillier cryptosystem has an additive homomorphic property $\mathcal{E}_P(m_1 + m_2) = \mathcal{E}_P(m_1) \mathcal{E}_P(m_2) \mod n_P$ for $m_1, m_2, m_1 + m_2 \in \mathbb{Z}_{n_P}$. This property means that, given only the public key and the encryption of $m_1$ and $m_2$, one can compute the encryption of $m_1 + m_2$. The detailed algorithm is as shown in Algorithm 2.

**Algorithm 2** Paillier Cryptosystem: $\mathcal{E}_P : \mathbb{Z}_{n_P} \mapsto \mathbb{Z}_{n_P}^*$

### 1. Key Generation
Step 1: Generate two distinct large prime numbers $p_P, q_P$, such that $\gcd(p_Pq_P, (p_P - 1)(q_P - 1)) = 1$.
Step 2: Let $n_P = p_Pq_P$ and $\lambda_P = \text{lcm}(p_P - 1, q_P - 1)$.
Step 3: Select a random integer $g_P \in \mathbb{Z}_{n_P}^*$ and ensure the existence of $\mu_P = (L(g_P)^{\lambda_P} \mod n_P)^{-1} \mod n_P$ where $L(x) = \frac{x - 1}{n_P}, x \in \{x \leq n_P, x \equiv 1 \pmod{n_P}\}$.
Step 4: The public key is $K_{pub} = (n_P, g_P)$ and the private key is $K_{pri} = (\lambda_P, \mu_P)$.

### 2. Encryption $\mathcal{E}_P$
Generate a random integer $h_P \in [0, n_P)$ and $h_P \in \mathbb{Z}_{n_P}^*$.
$\mathcal{E}_P(m_P) = g_P^{mp} h_P^{\mu_P} \mod n_P, m_P \in \mathbb{Z}_{n_P}$.

### 3. Decryption $\mathcal{E}_P^{-1}$
$\mathcal{E}_P^{-1}(m_P) = L(m_P^{\mu_P} \mod n_P^2) \mu_P \mod n_P, m_P \in \mathbb{Z}_{n_P}^*$.

The computation associated with encryption and decryption procedures in the aforementioned cryptosystems is performed on integers. To facilitate the procedures in control systems, we need to apply a function that converts an analogue signal into integers. For this purpose, we define a set of signed fixed-point rational numbers in base 2, $\mathbb{Q}_{(n,m)}$, that contains all rational numbers in $[-2^{n-m-1}, 2^{n-m-1} - 2^{-m}]$ separated from each other by $2^{-m}$, that is,

$$\mathbb{Q}_{(n,m)} := \{- b_n 2^{n-m-1} + \sum_{i=1}^{n-1} 2^{i-m-1} b_i \mid b_i \in \{0,1\}, \forall i \in \{1,\ldots,n\}\}.$$

The positive integers $n, m$ determine the length and the resolution of the fixed-point rationals. Moreover, a mapping $\mathcal{I}_{n,m} : \mathbb{Q}_{(n,m)} \mapsto \mathbb{Z}_{2^n}$ is defined to convert the rationals into integers, with $\mathcal{I}_{n,m}(a) = 2^m a \mod 2^n, \forall a \in \mathbb{Q}_{(n,m)}$. This mapping is bijective with the inverse mapping $\mathcal{I}_{n,m}^{-1} : \mathbb{Z}_{2^n} \mapsto \mathbb{Q}_{(n,m)}$ expressed as

$$\mathcal{I}_{n,m}^{-1}(a) = \begin{cases} \frac{(a - 2^n)}{2^m}, & a \geq 2^{n-1} \\ \frac{a}{2^m}, & \text{otherwise} \end{cases}, \forall a \in \mathbb{Z}_{2^n}.$$

**III. PROBLEM FORMULATION**

We consider a large-scale control system composed of $N \geq 1$ entities (components) whose dynamics are given as follows

$$x_i(k+1) = f_i(x_i(k), u_i(k))$$
$$y_i(k) = h_i(x_i(k), u_i(k)), \quad i = 1, \ldots, N,$$

where $x_i(k) \in \mathbb{R}^p$ is the state, $u_i(k) \in \mathbb{R}^p$ the input, and $y_i(k) \in \mathbb{R}^q$ the output, of the $i$-th entity. The functions $f_i$ and $h_i$ describe the entity’s evolution and measurement. The discrete time axis is labeled by the index $k = 0, 1, 2, \ldots$, in particular, with $k = 0$ being regarded as the initial time. The vector $x = \text{col}(x_1, \ldots, x_N)$ is the lumped state of the whole system. The dynamics governing $x$ generally represent $N$ coupled entities as $f_i(x_i, u_i)$ depends on $x_i$ only, explicitly rewritten as $f_i(x_i, u_i)$.

There are four elementary functions used in the problem formulation, representing rational-integer conversion and encryption, as follows:

$$\mathcal{I}_{n,m} : \mathbb{Q}_{(n,m)} \mapsto \mathbb{Z}_{2^n}$$
$$\mathcal{E}_P : \mathbb{Z}_{n_P} \mapsto \mathbb{Z}_{n_P}^*, \quad n_P > 2^n$$
$$\mathcal{E}_R, \mathcal{E}_R^{-1} : \mathbb{Z}_{n_R} \mapsto \mathbb{Z}_{n_R}^*, \quad n_R = n_P^2, \quad i = 1, \ldots, N.$$ (2)

The specific selections of these functions, including the encryption keys, will be elaborated in the next section. Based on these functions, we define the following composite functions, for the convenience of presentation:

$$\mathcal{E}_0(s) = \mathcal{E}_P(\mathcal{I}_{n,m}(s))$$
$$\mathcal{E}_1(s) = \mathcal{E}_R(\mathcal{E}_0(s))$$
$$\mathcal{D}_0(s) = \mathcal{I}_{n,m}^{-1}(\mathcal{E}_P^{-1}(s))$$
$$\mathcal{D}_1(s) = \mathcal{I}_{n,m}^{-1}(\mathcal{E}_R^{-1}(s))$$

The output signal $y_i(k), i = 1, \ldots, N$, is quantized as $y_i(k) \in \mathbb{Q}_{(n,m)}$, which is transformed into integer plaintext and hence encrypted before transmission over the network, resulting in the ciphertext $y_i(k)$. The postscript $q$ represents quantization of the signal, which rounds the elements of the signal to the nearest elements of $\mathbb{Q}_{(n,m)}$ less than or equal to the signal. A uniform quantization space $\mathcal{Q}_{(n,m)}$ is used for all entities $i = 1, \ldots, N$, with the specified integers $n$ and $m$ depending on the storage capacity. This process is represented by the mapping

$$y_i(k) = \mathcal{E}_q\left(\left[\begin{array}{c} y_i^q(k) \\ -y_i^q(k) \end{array}\right]\right)$$ (4)
where $E_i$ contains the double-layer encryption, composite of $E_i$ and $E_P$, as well as a rational-integer conversion $I_{mn}$. It is worth noting that both $y_i^v(k)$ and $-y_i^v(k)$ are encrypted when they are used in control design. By doing so, any linear operations on $y_i^v(k)$ can be regarded as pure summation (not involving subtraction) of $y_i^v(k)$ and $-y_i^v(k)$.

A control algorithm implemented in the remote controller is of the following form

$$v_i(k) = \kappa_i(z_i(k), D_1(y_i(k)), \cdots, D_N(y_N(k)))$$

$$z_i(k+1) = \kappa_i(z_i(k), D_1(y_i(k)), \cdots, D_N(y_N(k)))$$

$$z_i(0) = E_o \left[ \begin{bmatrix} \zeta_i(0) \\ -\zeta_i(0) \end{bmatrix} \right]$$

where $v_i(k), z_i(k) \in \mathbb{Z}_{n_i}$, $\zeta_i(0) \in \mathbb{Z}_{(n,m)}$ and the control functions $\kappa_i$ and $\zeta_i$ rely on the received ciphertext $y_i(k)$ with a proper decryption, i.e., $D_1(y_i(k)), \cdots, D_N(y_N(k))$. Note that $D_i$ decrypts the outer-layer encryption $E_{R,i}$, that is,

$$D_i(y_i(k)) = E_o \left[ \begin{bmatrix} y_i^v(k) \\ -y_i^q(k) \end{bmatrix} \right].$$

Also, the functions $\kappa_i$ and $\zeta_i$ must be properly designed such that their values are always within the set $\mathbb{Z}_{n_i}$ to avoid a computation overflow; this is elaborated further later.

A general dynamic controller is used in the formulation, with $z_i(k)$ being the state of the dynamic compensator. In this paper, such a remote architecture is referred to as a networked control scheme. The architecture is centralized if each controller unit relies on the ciphertexts from all the entities. It also contains decentralized control scenario when the functions $\kappa_i$ and $\zeta_i$ rely on the ciphertexts from some (not all) entities, according to a specified communication network topology.

The designed control command $v_i(k)$ is again encrypted before transmission over network, resulting in a ciphertext $v_i(k)$, represented by the mapping

$$v_i(k) = \tilde{E}_i(v_i(k)).$$

Finally, the control command $u_i(k)$ is decrypted from $v_i(k)$ when it is received by the $i$-th entity, that is,

$$u_i(k) = \tilde{D}_i(v_i(k)),$$

where $\tilde{D}_i$ contains a double-layer decryption composite of $E_{i-1}$ and $E_P^{-1}$, as well as an integer-rational conversion $I_{n_i,m}$.

The networked control process for large-scale systems is explained above whose architecture is also illustrated in Figure 1. The overall controller is composed of $E_P$, $E_R, E_o$, and $E_{R,i}$, and the private control algorithm represented by the functions $\kappa_i$ and $\zeta_i$, for $i = 1, \cdots, N$, such that

P1: the closed-loop system composed of $\tilde{E}_i$, $\tilde{D}_i$, $E_P$, and $E_{R,i}$, has the desired control performance:

(Stabilization) there exist $\zeta_i(k) \in \mathbb{Z}_{(n,m)}$, $k \geq 0$ and a set $\mathcal{X}$, such that,

$$z_i(k) = E_o \left[ \begin{bmatrix} \zeta_i(k) \\ -\zeta_i(k) \end{bmatrix} \right]$$

and, with $x_c(k) = \text{col}(x(k), \zeta(k))$ and $\zeta = \text{col}(\zeta_1, \cdots, \zeta_N)$,

$$\|x_c(k)\| \leq \alpha \rho \|x_c(0)\| + \varsigma 2^{-m}, \forall x_c(0) \in \mathcal{X},$$

for some $\alpha, \varsigma > 0$ and $0 < \rho < 1$; or

(Consensus) there exist $x_{\infty}(k)$, $k \geq 0$ and a set $\mathcal{X}$, such that,

$$\|x(k) - 1 \otimes x_{\infty}(k)\| \leq \alpha \rho \|x(0)\| + \varsigma 2^{-m}, \forall x(0) \in \mathcal{X}$$

for some $\alpha, \varsigma > 0$ and $0 < \rho < 1$.

P2: the signals $y_i(k)$ and $u_i(k)$ are protected in the transmission of ciphertexts $y_i(k)$ and $v_i(k)$ to all entities and control units except the self-entity $i$.

P3: the signals $y_i(k)$ and $u_i(k)$ are protected in $D_i(y_i(k))$ and $v_i(k)$ to the control units.

Some remarks are listed below in order.

Remark 3.1: The property P1 describes the desired control performance in two classes of problems, stabilization and consensus, which are rigorously formulated here and will be explicitly investigated in Sections V and VI, respectively. The formulation includes a residual error $\varsigma 2^{-m}$ as the measurements are quantized for encryption, which will be further examined. It is worth mentioning that the proposed encryption architecture is separated from the desired control performance, and hence can be applied to tackle security in more control problems and applications.

Remark 3.2: The property P2 considers the protection of information transferred over untrusted networks, that is, the protection of entity $i$’s information $y_i(k)$ or $u_i(k)$ in the transmission ciphertexts $y_i(k)$ or $v_i(k)$. The information is protected from the controller and each of the entities within the system. The property P3 addresses the protection of information between the system and the controller, that is, the protection of entity $i$’s information $y_i(k)$ or $u_i(k)$ during operations within the controller.

Remark 3.3: A double-layer cryptographic approach is used in this paper to ensure both properties P2 and P3. With a single-layer cryptographic mechanism is applied, there can be two typical scenarios, neither of which can achieve these properties. (i) The decryption $D_i$ of the control unit is selected as the inverse function of $E_i$, that is, $D_i(y_i(k)) = D_i(E_i(col(y_i^v(k), y_i^q(k)))) = col(y_i^v(k), -y_i^q(k)).$

Then the measurement $y_i^v(k)$ can be directly used in the controller $\tilde{E}_i$, which much simplifies the controller design. However, in such a scenario, a malicious control unit would easily detect the output measurement $y_i^q(k)$ of the entity. So, P3 is thus violated. (ii) In the second case, no decryption is applied at the control unit. The ciphertext $y_i(k)$ must use the same cryptosystem for all entities to facilitate the design of an effective controller. As a result, P2 is violated, as the signal $y_i(k)$ does not remain secure with respect to other entities in the transmission ciphertext $y_i(k)$.

IV. A DOUBLE-LAYER CRYPTOGRAPHIC ARCHITECTURE

A general secure networked control design paradigm using cryptographic mechanisms is proposed in this section. In particular, the separation principle in this paradigm enables the quantization-encryption-decryption protocol to be separated from the control algorithm design. This principle is stated in the following theorem.

Theorem 4.1: Consider the system (1) with the private controller $E_P$, $E_{R,i}$, and $E_{R,R}$, satisfying the following three properties for two specified integers $n$ and $m$.

- (Controller subject to perturbation) There exists a controller

$$u_i(k) = \kappa_i(z_i(k), y_i(k) + \delta_1(k), \cdots, y_N(k) + \delta_N(k))$$

$$\zeta(k + 1) = \tilde{\kappa}_i(\zeta_i(k), y_i(k) + \delta_1(k), \cdots, y_N(k) + \delta_N(k))$$

and a set $\mathcal{X}$, such that the closed-loop system composed of $E_P$ and $E_{R,R}$ has the desired control performance $P_9$ or $P_{10}$ for

1 A signal $a(k)$ is protected or secure in a signal $b(k)$ to a party means that $a(k)$ or $a^p(k)$ cannot be obtained from $b(k)$ using the keys available to the party.
any $|\delta_i| < 2^{-m}$. Moreover, the signals $y_i(k), u_i(k), \zeta_i(k) \in [-2^{n-m-1}, 2^{n-m-1})$, $i = 1, \ldots, N$.

- **(Quantization property)** The output signal $y_i(k)$ can be quantized as

$$y_i^q(k) \in \mathcal{Q}_{i}(m), \quad \|y_i(k) - y_i^q(k)\|_{\infty} < 2^{-m},$$

and the functions $\hat{\kappa}_i, \tilde{\kappa}_i$ satisfy

$$\hat{\kappa}_i(c_o, c_1, \ldots, c_N), \tilde{\kappa}_i(c_o, c_1, \ldots, c_N) \in \mathcal{Q}_{i}(m)$$

for $\text{col}(c_o, c_1, \ldots, c_N) \in \mathcal{C}_{i,m}$ where the set $\mathcal{C}_{i,m}$ is defined as follows

$$\mathcal{C}_{i,m} := \{\text{col}(c_o, c_1, \ldots, c_N) \in \mathcal{Q}_{i}(m) \mid \hat{\kappa}_i(c_o, c_1, \ldots, c_N), \tilde{\kappa}_i(c_o, c_1, \ldots, c_N) \in [-2^{n-m-1}, 2^{n-m-1})\}.$$  

- **(Cryptographic property)** The functions $\kappa_i, \hat{\kappa}_i, \tilde{\kappa}_i$, and $\zeta_i$, satisfy

$$\mathcal{D}_{o}(\hat{\kappa}_i(\mathcal{E}_{o}(c_o, -c_o), \mathcal{E}_{o}(c_1, -c_1), \ldots, \mathcal{E}_{o}(c_N, -c_N)))$$

$$= \mathcal{E}_{o}\left(\begin{bmatrix} \zeta_i(c_o, c_1, \ldots, c_N) \\ \tilde{\kappa}_i(c_o, c_1, \ldots, c_N) \end{bmatrix} \right).$$

for $\text{col}(c_o, c_1, \ldots, c_N) \in \mathcal{C}_{i,m}$.

Then, the closed-loop system composed of [1, 4, 5, 7, and 8]. Let $\delta_i(k) = y_i^q(k) - y_i(k)$. From the quantization property, one has $\|\delta_i\|_{\infty} < 2^{-m}$.

Assume there exists a constant $\bar{k} \geq 0$ such that

$$z_i(k) = \mathcal{E}_{o}\left(\begin{bmatrix} \zeta_i(k) \\ -\zeta_i(k) \end{bmatrix} \right)$$

and

$$\text{col}(\zeta_i(k), y_i^q(k), \ldots, y_i^q(k)) \in \mathcal{C}_{i,m}, \quad k = 0, \ldots, \bar{k}.$$  

This statement is true with $k = 0$; see the initial condition in [5] and [15]. We will prove the statement for $k = k + 1$ and then apply mathematical induction.

$^2$To simplify the notation, we use $\mathcal{E}_{o}(c, -c)$ for $\mathcal{E}_{o}(\text{col}(c, -c))$.

From [6], the first two equations in [5] become

$$v_i(k) = \kappa_i(z_i(k), \mathcal{E}_{o}(y_i^q(k), -y_i^q(k)), \ldots, \mathcal{E}_{o}(y_N^q(k), -y_N^q(k)))$$

$$z_i(k + 1) = \mathcal{E}_{o}(z_i(k), \kappa_i(y_i^q(k), -y_i^q(k)), \ldots, \mathcal{E}_{o}(y_N^q(k), -y_N^q(k))).$$

The second equation further implies that, using the cryptographic property, and noting [16], we have

$$z_i(k + 1) = \mathcal{E}_{o}(\zeta_i(k), \mathcal{E}_{o}(y_i^q(k), -y_i^q(k)), \ldots, \mathcal{E}_{o}(y_N^q(k), -y_N^q(k)))$$

$$= \mathcal{E}_{o}\left(\begin{bmatrix} \zeta_i(k) \\ \zeta_i(y_i^q(k), -y_i^q(k)) \end{bmatrix} \right)$$

$$= \mathcal{E}_{o}\left(\begin{bmatrix} \zeta_i(k + 1) \\ -\zeta_i(k + 1) \end{bmatrix} \right)$$

for

$$\zeta_i(k + 1) = \tilde{\kappa}_i(z_i(k), y_i^q(k), \ldots, y_N^q(k)).$$

From the cryptographic property again, one has the following equation, noting [16],

$$\mathcal{D}_{o}(v_i(k)) = \tilde{\kappa}_i(\zeta_i(k), y_i^q(k), \ldots, y_N^q(k))$$

It is noted that $u_i(k) = \mathcal{D}_{o}(\tilde{\kappa}(v_i(k))) = \mathcal{D}_{o}(v_i(k))$. As a result,

$$u_i(k) = \kappa_i(\zeta_i(k), y_i^q(k), \ldots, y_N^q(k)).$$

The set of equations [17]-[18] is equivalent to [11], for $k = 0, \ldots, \bar{k}$. As a result, $y_i(k + 1)$ and $\zeta_i(k + 1)$ are determined by the closed-loop system composed of [1] and [11].

By mathematical induction, one has [16] for all $k = 0, 1, 2, \ldots, \bar{k}$. Therefore, the closed-loop system under consideration is always equivalent to the one composed of [1] and [11]. Hence, the desired control performance, that is, the property P1, is achieved.

**Remark 4.1:** To guarantee the control performance in a secure control environment, the prerequisite is the existence of the...
controller with the same performance. Additional conditions must also be satisfied to avoid a computation overflow or underflow when cryptographic mechanisms are applied. Firstly, the signals \( y_i(k), u_i(k), \zeta_i(k) \) must be within the range \([-2^{m-1}, 2^{m-1}]\) such that it can be quantized with the error up to \(2^{-m}\) in the space \(Q_{(b,m)}\) without overflow. Secondly, the functions \( \hat{\kappa_i} \) and \( \hat{\zeta_i} \) must satisfy (13), such that their values are rational numbers in base 2 without causing an underflow. For this purpose, these functions take the linear form of integer coefficients, which are explicitly constructed later. The third condition (14) shows that the required functions \( \hat{\kappa_i} \) and \( \hat{\zeta_i} \) can be equivalently realized by the functions \( \tilde{\kappa_i} \) and \( \tilde{\zeta_i} \) applied on the ciphertexts, provided that the cryptosystem has a certain homomorphous property and the aforementioned overflow or underflow issues are avoided. Satisfaction of these conditions create additional challenges on the design of the controller, which will be explicitly analyzed in the subsequent sections.

**Remark 4.2:** In a centralized control scenario, one common controller dynamics is typically used for all \( v_i(k) \). In this case, the proposed paradigm still applies with \( z_i(k) = z(k) \) and \( \kappa_i = \kappa \), \( i = 1, \ldots, N \), and the controller (11) reduces to

\[
v_i(k) = \kappa_i(z(k), D_1(y_1(k)), \ldots, D_N(y_N(k)))
\]

\[
z(k) = \kappa(z(k), D_1(y_1(k)), \ldots, D_N(y_N(k)))
\]

\[
z(0) = E_o \begin{bmatrix} \zeta(0) \\ -\zeta(0) \end{bmatrix}.
\]

(20)

Also, the controller (11) in Theorem 4.1 becomes

\[
u_i(k) = \kappa_i(\zeta(k), y_i(k) + \delta_i(k), \ldots, y_N(k) + \delta_N(k))
\]

\[
\zeta(k+1) = \kappa(\zeta(k), y_i(k) + \delta_i(k), \ldots, y_N(k) + \delta_N(k)).
\]

(21)

Next, the specific encryption-decryption protocols are designed in the following theorem, which guarantees the cryptographic property in Theorem 4.1, as well as the properties P2 and P3. In the following, \( \sum \) and \( \prod \) represent the normal summation and (element-wise) multiplication respectively. Also, for a real matrix \( A = [a_{ij}] \in \mathbb{R}^{r \times s} \) with \( a_{ij} \) being the \((i,j)\)th entry, and a vector \( b = [b_1, \ldots, b_s]^T \), let the following vectors be

\[
\prod E_o^{[A]}(\text{sgn}(A)b) = \begin{bmatrix}
\prod_{i=1}^{r} E_o^{[a_{1i}]}(\text{sgn}(a_{1i})b_1) \\
\vdots \\
\prod_{i=1}^{r} E_o^{[a_{ri}]}(\text{sgn}(a_{ri})b_r)
\end{bmatrix}
\]

\[
\prod b^{[A]} = \begin{bmatrix}
\prod_{i=1}^{r} b_{1i}^{[a_{1i}]} \\
\vdots \\
\prod_{i=1}^{r} b_{ri}^{[a_{ri}]}
\end{bmatrix}.
\]

**Theorem 4.2:** In Theorem 4.1, suppose the control functions \( \hat{\kappa_i} \) and \( \hat{\zeta_i} \) are linear with integer coefficients, that is,

\[
\hat{\kappa_i}(c_0, c_1, \ldots, c_N) = \sum_{j=0}^{N} \phi_{ij} c_j,
\]

\[
\hat{\zeta_i}(c_0, c_1, \ldots, c_N) = \sum_{j=0}^{N} \varphi_{ij} c_j
\]

(22)

for integer matrices \( \phi_{ij} \) and \( \varphi_{ij} \). If \( E_P, \tilde{E}_R, \) and \( \tilde{E}_R \) are designed as follows:

- \( E_P : \mathbb{Z}_{n_P} \rightarrow \mathbb{Z}_{n_P} \) is a Paillier encryption with

\[
n_P > \max\{2^p \sum_{j=0}^{N} |\phi_{ij}|, 2^p \sum_{j=0}^{N} |\varphi_{ij}| \}
\]

and the private key only available to all entities.

- \( \tilde{E}_{R,i} : \mathbb{Z}_{n_R} \rightarrow \mathbb{Z}_{n_R} \) is an RSA encryption with \( n_R = n_P^2 \) and the private key only available to the \( i \)-th controller.

- \( \tilde{E}_{R,i} : \mathbb{Z}_{n_R} \rightarrow \mathbb{Z}_{n_R} \) is an RSA encryption with the private key only available to the \( i \)-th entity.

Then, the cryptographic property in Theorem 4.1 is automatically satisfied for

\[
\kappa_i(E_o(c_0, -c_0), E_o(c_1, -c_1), \ldots, E_o(c_N, -c_N)) = \prod_{j=0}^{N} E_o^{[\phi_{ij}]}(\text{sgn}(\varphi_{ij}) c_j) \mod n_P^2,
\]

\[
\kappa_i(E_o(c_0, -c_0), E_o(c_1, -c_1), \ldots, E_o(c_N, -c_N)) = \prod_{j=0}^{N} E_o^{[\phi_{ij}]}(\text{sgn}(\varphi_{ij}) c_j) \mod n_P^2.
\]

(23)

Also the properties P2 and P3 are achieved.

**Proof:** We first prove the cryptographic property in Theorem 4.1. First, one has

\[
I_{n,m}(\hat{\kappa}_i(c_0, c_1, \ldots, c_N)) = 2^n \sum_{j=0}^{N} \phi_{ij} c_j \mod 2^n
\]

\[
= 2^n \sum_{j=0}^{N} |\phi_{ij}| \text{sgn}(\varphi_{ij}) c_j \mod 2^n
\]

\[
= \sum_{j=0}^{N} |\phi_{ij}| I_{n,m}(\text{sgn}(\varphi_{ij}) c_j) \mod 2^n.
\]

As \( E_P \) is a Paillier encryption, one has

\[
\prod_{j=0}^{N} E_P^{[\phi_{ij}]}(I_{n,m}(\text{sgn}(\varphi_{ij}) c_j)) \mod n_P^2 = \prod_{j=0}^{N} E_P(\sum_{j=0}^{N} |\phi_{ij}| I_{n,m}(\text{sgn}(\varphi_{ij}) c_j))
\]

noting \( 0 \leq I_{n,m}(\text{sgn}(\varphi_{ij}) c_j) < 2^n < n_P \) and \( 0 \leq \sum_{j=0}^{N} |\phi_{ij}| I_{n,m}(\text{sgn}(\varphi_{ij}) c_j) < 2^n \sum_{j=0}^{N} |\phi_{ij}| 1 < n_P \). Then,

\[
E_P^{-1}(\prod_{j=0}^{N} E_P^{[\phi_{ij}]}(I_{n,m}(\text{sgn}(\varphi_{ij}) c_j)) \mod n_P^2) \mod 2^n
\]

\[
= \sum_{j=0}^{N} \phi_{ij} I_{n,m}(\text{sgn}(\varphi_{ij}) c_j) \mod 2^n
\]

\[
= I_{n,m}(\hat{\kappa}_i(c_0, c_1, \ldots, c_N))
\]

and hence

\[
I_{n,m}(E_P^{-1}(\prod_{j=0}^{N} E_P^{[\phi_{ij}]}(\text{sgn}(\varphi_{ij}) c_j) \mod n_P^2) \mod 2^n)
\]

\[
= \hat{\kappa}_i(c_0, c_1, \ldots, c_N).
\]

As a result,

\[
D_o(\prod_{j=0}^{N} E_P^{[\phi_{ij}]}(\text{sgn}(\varphi_{ij}) c_j) \mod n_P^2) = \hat{\kappa}_i(c_0, c_1, \ldots, c_N).
\]

So, the first equation of (14) is proved noting (23). The second equation of (14) can be proved using similar arguments.

We can prove P2 noting that, in \( y_i(k) = E_{R,i}(E_P(I_{n,m}(y_i^0(k)), y_i^1(k))) \), the private key of \( E_{R,i} \) is unavailable to the entities and the private key of \( E_P \) is unavailable to the control units; and in \( u_i(k) = D_o(E_{r,i}^{-1}(v_i(k))) \), the private
Finally, we can prove P3 noticing that, in $D_i(y_i(k)) = E_P(T_{m,n}(y_i^0(k), -y_i^0(k)))$, the private key of $E_P$ is unavailable to the control units; and in $u_i(k) = T_{m,n}(E_P^{-1}(v_i(k)) \mod 2^n)$, the private key of $E_P$ is unavailable to the control units. \hfill $\square$

**Remark 4.3:** The importance of Theorem 4.2 is two-fold. On the one hand, it describes the specific cryptosystems $E_P$, $E_{R_i}$, and $\tilde{E}_{R,i}$ with their key generation rules; on the other hand, it also gives the explicit construction of the controller functions. It facilitates the practical implementation of the desired private controller.

**Remark 4.4:** The cryptographic techniques, especially the management of private keys in Theorem 4.2 guarantee the properties P2 and P3. If more than one entity is hacked and becomes malicious, they cannot eavesdrop and obtain the information of the remaining benign entities, as they cannot break the outer-layer RSA encryption. If all the controllers are under attack and the RSA private keys are disclosed, the information of the entity $i$ within the system still remains secure due to the inner-layer Paillier encryption. The secrecy of the entity $i$’s information is affected only when there is a malicious party who is able to obtain both the Paillier private key and the RSA private key.

**Remark 4.5:** Under Theorem 4.2, the controller (5) with (4) takes the following specific form

$$
v_i(k) = \prod(z^{sgn(\phi_o)}_{i}(k))^{\phi_{al}} \prod_{j=1}^{N} E^{(\phi_{ij})}_{o}(|sgn(\phi_{ij})|y^j_i(k)) \mod n^2_p.
$$

where $z^{sgn(\phi_o)}_{i} = z^+_{i}$ or $z^-_{i}$ for $sgn(\phi_o) = +1$ or $-1$, respectively, in the element-wise manner. When $\phi_o = 0$, $(z^{sgn(\phi_o)}_{i}(k))^{\phi_{al}} = 1$ vanishes in the product. When $sgn(\phi_o) = +1$ and $sgn(\phi_o) = +1$, the controller reduces to

$$
v_i(k) = \prod(z^{+}_{i}(k))^{\phi_{al}} \prod_{j=1}^{N} E^{(\phi_{ij})}_{o}(|sgn(\phi_{ij})|y^j_i(k)) \mod n^2_p.
$$

with the $z^+_{i}$-dynamics vanished. For the same reason, when $sgn(\phi_o) = -1$ and $sgn(\phi_o) = -1$, the controller reduces similarly with the $z^-_{i}$-dynamics vanished.

**V. CASE 1: CENTRALIZED STABILIZATION PROBLEM**

The plant (1) takes the following linear form, with $u_i(k) = col(u_i^0(k), u_i^1(k))$ and $y_i(k) = col(y_i^0(k), y_i^1(k))$,

$$
x_i(k + 1) = \sum_{j=1}^{N} A_{ij}x_i(k) + B_iu_i^1(k)
$$

$$
y_i^0(k) = \gamma_1 C_i x_i(k)
$$

$$
y_i^1(k) = \gamma_2 u_i^0(k), \ i = 1, \ldots, N,
$$

where all the matrices $A_{ij}$, $B_i$, and $C_i$ are rational matrices whose elements are rational numbers and $\gamma_1, \gamma_2 > 0$ are two parameters. The plant essentially consists of the upper two equations from the input $u_i^0$ to the output $y_i^0$. The parameter $\gamma_1$ modifies the output to match the required resolution. The third equation deliberately introduces an additional communication channel between the plant and the remote controller such that the state of remote controller can be sent back to the plant and processed by the gain $\gamma_2$, also to match the required resolution. The so-called resolution has to be matched through $\gamma_1$ and $\gamma_2$, because only the integer gains can be applied in the controller design, as elaborated in Lemma 5.1.

As this scenario considers a centralized stabilizer, from Remark 4.2, the controller used in Theorem 4.1 takes the form (21) with the linear functions $\kappa_i$ and $\zeta_i$ given as follows:

$$
u_i^0(k) = \phi_o[y_i^0(k) + \delta_i^0(k)]
$$

$$
u_i^1(k) = \zeta_i(k)
$$

$$
\zeta(k+1) = \varphi_o[y_i^1(k) + \delta_i^1(k)] + \sum_{j=1}^{N} \varphi_j[y_j^0(k) + \delta_j^0(k)]
$$

for integer matrices $\varphi_0, \phi_i, \varphi_i, i = 1, \ldots, N$, where $y_i^0(k) = \gamma_2 \zeta(k)$ and $\delta_i^0(k) = \delta_i^1(k) = \zeta_1 \zeta_2$. Let $\delta_i(k) = \text{col}(\delta_i^0(k), \delta_i^1(k))$. It is worth mentioning that the controller coefficients represented by the matrices $\varphi_0, \phi_i$ and $\varphi_i$ must be integers to avoid a computation underflow as explained in Remark 4.1. The need for controllers having integer coefficients has also been discussed in literature such as in [23] for PID controllers and FIR filters.

Representing the system and the controller in a compact form, let us denote $A = [A_{ij}]_{N \times N}$, $B = \text{block diag}(B_1, \ldots, B_N)$, $C = \text{block diag}(C_1, \ldots, C_N)$, $\phi = \text{col}(\phi_1, \ldots, \phi_N)$, $\varphi = [\varphi_1, \ldots, \varphi_N]$, and define two matrices

$$
A_c = \begin{bmatrix} A & \gamma_2 B \phi \\ \gamma_2 \varphi & C \end{bmatrix}, \quad B_c = \begin{bmatrix} 0 & B \phi \\ \varphi & \varphi \end{bmatrix}.
$$

We first give a technical lemma under the following assumption.

**Assumption 5.1:** The pairs $(A, B)$ and $(C, A)$ for the system (26) are controllable and observable.

**Lemma 5.1:** Under Assumption 5.1 there exist $\gamma_1, \gamma_2 > 0$ and integer matrices $\varphi_0, \phi_i$ and $\varphi_i, i = 1, \ldots, N$, such that the matrix $A_c$ defined in (28) is a Schur matrix.

**Proof:** Under Assumption 5.1 there exist two matrices $K$ and $L$ such that

$$
\begin{bmatrix} A & B K \\ -L C & A + B K + L C \end{bmatrix} = \begin{bmatrix} I & 0 \\ I & I \end{bmatrix} \begin{bmatrix} A + B K & B K \\ 0 & A + L C \end{bmatrix} \begin{bmatrix} I & 0 \\ -I & I \end{bmatrix}
$$

is a Schur matrix. As rational numbers are dense, the matrices $K$ and $L$ can be selected as rational matrices. Therefore, we can pick $\gamma_1, \gamma_2 > 0$ such that the following matrices

$$
\phi = K/\gamma_2, \quad \varphi = -L/\gamma_1, \quad \varphi_0 = (A + B K + L C)/\gamma_2
$$

are integer matrices. Also, it is easy to check that $A_c$ and $\tilde{A}_c$ are identical, which are Schur matrices.

Before we give the main result of this section, let us define some notations for the convenience of presentation. From Theorem 33 of Chapter 7 of [533], for the Schur matrix $A_c$ defined in (28), there exist $0 < \rho < 1$ and $M > 0$ such that $\|A_c^\rho\| \leq M \rho^\rho$. Let $\sigma = \|B_c\| d$, where $d$ is the dimension of $\delta(k) = \text{col}(\delta_i^0(k), \ldots, \delta_i^N(k), \delta_i(k))$. Let $x_c(k) = \text{col}(x(k), \zeta(k))$.

**Theorem 5.1:** Consider the closed-loop system composed of (26) and (27), under Assumption 5.1 with the parameters $\gamma_1, \gamma_2 > 0$ and
integer matrices $\varphi_0$, $\phi$, and $\varphi$, $i = 1, \cdots, N$, selected in Lemma 5.1. It has the desired control performance

$$\|x_c(k)\| \leq M\rho^k \|x_c(0)\| + \frac{M\sigma}{1 - \rho} 2^{-m}  \quad (29)$$

for $|\delta(k)| \leq 2^{-m}$. Moreover, the signals $y_i(k), u_i(k), \zeta(k) \in [-2^{m-1}, 2^{m-1}), i = 1, \cdots, N$, if the initial condition satisfies $\|x_c(0)\| \leq R_0$ for

$$R_0 = \frac{\beta}{M} - \frac{\sigma}{1 - \rho} 2^{-m}, \beta < 2^{m-1} \min\{1, \frac{1 - \|\phi\|2^{-n+1}}{\gamma_1\|C_i\|}, \frac{1}{\gamma_2}\}.  \quad (30)$$

**Proof:** Let $\tilde{y}_i(k) = C_i x_i(k) = y_i^e(k)/\gamma_1$. It is easy to check that the controller $y_i^e(k)$ is equivalent to

$$u_i^e(k) = \gamma_2\phi_i \zeta(k) + \phi_i \delta_i^e(k),$$

$$\zeta(k + 1) = \gamma_2\varphi_i \zeta(k) + \gamma_1 \sum_{j=1}^{N} \varphi_j \tilde{y}_j(k),$$

$$+ \sum_{j=1}^{N} \varphi_j \delta_j^e(k) + \varphi \varphi_i \zeta(k).  \quad (31)$$

Without considering the quantization errors, the closed-loop system composed of

$$x_i(k + 1) = \sum_{j=1}^{N} A_i x_j(k) + B_i u_i^o(k) + B_i u_i^e(k)$$

$$\tilde{y}_i(k) = C_i x_i(k), \quad i = 1, \cdots, N.  \quad (32)$$

and

$$u_i^o(k) = \gamma_2\phi_i \zeta(k)$$

$$\zeta(k + 1) = \gamma_2\varphi_i \zeta(k) + \gamma_1 \sum_{j=1}^{N} \varphi_j \tilde{y}_j(k)$$

(33)

can be proved to be stable. In fact, it can be put into the following compact form composed of

$$x(k + 1) = Ax(k) + Bu(k)$$

$$\bar{y}(k) = Cx(k)  \quad (34)$$

and

$$u(k) = \gamma_2\phi \zeta(k)$$

$$\zeta(k + 1) = \gamma_2\varphi \zeta(k) + \gamma_1 \varphi \bar{y}(k),$$

where $u(k) = \text{col}(u_1(k), \cdots, u_N(k)), \bar{y} = \text{col}(\tilde{y}_1, \cdots, \tilde{y}_N)$. The controller $y_i^e(k)$ is a typical Luenberger observer-based stabilizer. Furthermore, the closed-loop system composed of (34) and (35) takes the following form

$$x_c(k + 1) = A_c x_c(k)$$

for $A_c$ and $B_c$ defined in (28). From (38), we have

$$x_c(k) = A_c^k x_c(0) + \sum_{j=0}^{k-1} A_c^{k-j-1} B_c \delta_j.$$  \quad (39)

Noting $\|A_c^k\| \leq M\rho^k$ and $\sigma = \|B_c\|d$, the property (29) follows; see, e.g., [34].

From (29) and $\|x_c(0)\| \leq R_0$, one has

$$\|\zeta(k)\| \leq \|x_c(k)\| \leq MR_0 + \frac{M\sigma}{1 - \rho} 2^{-m}  = \beta < 2^{m-1}.$$  \quad (40)

More calculation shows

$$\|u_i^o(k)\| \leq \gamma_2\|\phi\|c_i\|z(k)\| + \|\phi\|2^{-m} < \frac{\gamma_2\|\phi\|c_i\|z(k)\| + \|\phi\|2^{-m}}{2^{m-1}}$$

$$\|u_i^o(k)\| \leq \gamma_1\|C_i\||x_i(k)|| \leq \gamma_1\|C_i\|^\beta < 2^{m-1}.$$  \quad (40)

It concludes that $y_i(k), u_i(k), \zeta(k) \in [-2^{m-1}, 2^{m-1}), i = 1, \cdots, N$. \hfill $\square$

**Remark 5.1:** In the desired performance (29), the term $M\rho^k \|x_c(0)\|$ vanishes as $k \to \infty$, so the closed-loop state $x_c(k)$ is asymptotically bounded by $\|M\sigma/(1 - \rho)\|2^{-m}$ where $2^{-m}$ is sufficiently small for a sufficiently large $M$. The initial states can be sufficiently large for a sufficiently large $R_0$, and hence $\beta$, at the cost of a sufficiently large $n$.

**Remark 5.2:** Based on (27), the implemented controller (31) has the following specific form

$$v_i(k) = \prod_{j=1}^{n} \mathcal{E}_{o|\varphi_j}(\text{sgn}(\varphi_j)y_j^o(k)) \mod n^p,$$

$$z(k + 1) = \prod_{j=1}^{n} \mathcal{E}_{o|\varphi_j}(\text{sgn}(\varphi_j)y_j^o(k)) \times \prod_{j=1}^{n} \mathcal{E}_{o|\varphi_j}(\text{sgn}(\varphi_j)y_j^o(k)) \mod n^p$$

$$z(0) = \mathcal{E}_o(\zeta(0)).$$

It is noted that $[y_i^o]^{[n]}(k)$ in the middle equation can be taken from any entity $i$, as they are identical with $y_i^e(k) = \gamma_2 \zeta(k)$.

By combining Theorems 4.1, 4.2, and 5.1 and noting that the quantization property is simply satisfied, one has the following result.

**Theorem 5.2:** Consider the system (20) with the private controller (34), (35), and (36) for two specified integers $n$ and $m$. Under Assumption 5.1, select the parameters $\gamma_1, \gamma_2 > 0$ and integer matrices $\varphi_0, \phi$, and $\varphi_i, i = 1, \cdots, N$, according to Lemma 5.1 and hence define the linear functions $\hat{\kappa}_i$ and $\hat{\varphi}$ as in (27). Let $\mathcal{E}_P, \mathcal{E}_{R_1}$, and $\mathcal{E}_{R_2}$ be designed in Theorem 4.2. Then, the controller (31) with (34), (35), and (36) is quantization-free. For any initial condition satisfying $\|x_c(0)\| \leq R_0$ with $R_0$ given in (30), the closed-loop system achieves the desired control performance $P1$ in the sense of (29) as well as $P2$ and $P3$.

**Example 1:** We consider the two-input two-output system (20) of the following specific form

$$x_1(k + 1) = x_1(k) + x_2(k) + 0.5u_1^e(k),$$

$$x_2(k + 1) = x_2(k) + u_2^e(k) + y_1^e(k) + \gamma_1 x_1(k)$$

$$y_2^e(k) = \gamma_1 x_2(k).$$

It can also be put in the form (34) with $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0.5 & 0 \\ 1 & 1 \end{bmatrix}$, and $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Obviously, Assumption 5.1 holds,
we can design the feedback gain and observer gain for the observer-based controller \( \hat{1} \), with the parameters \( \gamma_1 = 0.01, \gamma_2 = 0.01, \) and integer matrices \( \phi = \begin{bmatrix} -200 & -100 \\ -100 & -124 \end{bmatrix} \) and \( \varphi = \begin{bmatrix} -100 & 200 \\ 100 & 200 \end{bmatrix} \). We set the length and the resolution of the fixed-point rationals as \( n = 24 \) and \( m = 6 \). With the initial condition \( x_1(0) = 10 \) and \( x_2(0) = 20 \), setting the modular bits for generating keys of Paillier encryption to be 64, we conducted the numerical simulation and obtain the following results, illustrated in Fig. 2. The left graph shows that the states of the system approach zero as expected by the desired control performance. The observer is implemented in the encrypted space with the states plotted in the right graph. The presence of the observer states in wild disorder verifies that the privacy of the controller remain intact. The left graph of Fig. 3 zooms in on the trajectories of the system states and shows that the privacy of the controller remain intact. The observer is implemented in the encrypted space with the states plotted in the right graph. The presence of the observer states in wild disorder verifies that the privacy of the controller remain intact. The left graph of Fig. 3 zooms in on the trajectories of the system states and shows that the privacy of the controller remain intact.

**VI. CASE 2: DECENTRALIZED CONSSENSUS PROBLEM**

When the plant \( \{1\} \) composed of \( N \) isolated entities, it takes the following linear form,

\[
x_i(k+1) = Ax_i(k) + Bu_i(k) \\
y_i(k) = \gamma x_i(k), \quad i = 1, \ldots, N,
\]

for two real matrices \( A \) and \( B \) and a scalar \( \gamma > 0 \) whose role is the same as the parameters \( \gamma_1, \gamma_2 \) in Section V. A decentralized state feedback control law is considered in this scenario; hence the controller \( \{1\} \) used in Theorem 4.1 is with the linear function \( \hat{\gamma} \) vanished and \( \hat{8} \) given as follows

\[
u_i(k) = \Lambda \sum_{j=1}^{N} \nu_{ij} [y_i(k) + \delta_i(k)] - (y_j(k) + \delta_j(k)) \]

for an integer matrix \( \Lambda \) and integers \( \nu_{ij}, \) \( i, j = 1, \ldots, N, \) where \( \delta_i(k) \) is the quantization error of \( y_i(k) \). Denote \( \delta = \text{col}(\delta_1, \ldots, \delta_N) \). The communication graph \( \mathcal{G} = (V, E) \) associated with \( \nu_{ij} \) is defined as \( V = \{1, \ldots, N\} \) being the node set and \( E \) the edge set. The edge \( (i, j) \in E, i \neq j, i, j = 1, \ldots, N, \) if and only if \( \nu_{ij} \neq 0 \), that is, the control \( u_i \) has access to the output \( y_j \).

Define the Laplacian matrix \( L \) whose \((i,j)\)-th entry is \( l_{ij} = -\nu_{ij} \) for \( i \neq j, i, j = 1, \ldots, N, \) and diagonal entry is \( l_{ii} = \sum_{j=1, j \neq i}^{N} \nu_{ij} \).

Let \( r, 1 \in \mathbb{R}^{N}, \) satisfying \( r^{T} 1 = 1 \), be the left and right eigenvectors of \( L \) associated with the eigenvalue 0, that is, \( r^{T} L = 0 \) and \( L 1 = 0 \). A nonsingular matrix \( T \) exists such that

\[
T = [1 U], \quad T^{-1} = \begin{bmatrix} r^{T} \\ V \end{bmatrix}, \quad T^{-1}LT = \begin{bmatrix} 0 & 0^{T} \\ 0_{N-1} & H \end{bmatrix}
\]

for \( H = VLU \), called the \( H \)-matrix of the Laplacian \( L \).

We first give two technical lemmas under the following assumptions.

**Assumption 6.1:** The communication graph \( \mathcal{G} \) is a directed graph that contains a spanning tree.

**Assumption 6.2:** The pair \((A, B)\) is stabilizable and the matrix \( A \) is neutrally stable, i.e., all the eigenvalues of \( A \) are semi-simple with modulus 1.

**Lemma 6.1:** For a given communication graph \( \mathcal{G} \) satisfying Assumption 6.1 and two matrices \( A \) and \( B \) satisfying Assumption 6.2, there exist an integer matrix \( \Lambda \), integers \( \nu_{ij}, i, j = 1, \ldots, N, \) whose graph is \( \mathcal{G} \), and a scalar \( \gamma > 0 \), such that

\[
\hat{A}_c = I_{N-1} \otimes \Lambda + \gamma H \otimes (BA)
\]

is a Schur matrix.

**Proof:** First, let us pick rational numbers \( a_{ij} \geq 0, \) \( i \neq j, i, j = 1, \ldots, N, \) whose associated graph is \( \mathcal{G} \). Define a row-stochastic rational matrix \( W \) whose \((i,j)\)-th entry is \( w_{ij} = \frac{a_{ij}}{1+\sum_{j=1, j \neq i}^{N} a_{ij}} \) for \( i \neq j, \) and \( w_{ii} = \frac{1}{1+\sum_{j=1, j \neq i}^{N} a_{ij}}. \) It is easy to see that the graph associated with \( w_{ij} \) is also \( \mathcal{G} \). Then \( \hat{L} = I_{N} - W \) is a Laplacian matrix and the \( H \)-matrix of \( \hat{L} \) is denoted as \( H \).
By Theorem 15 of [55], under Assumptions 6.1 and 6.2, there exists a matrix $\Gamma$ such that all the matrices $A + \lambda_i B^T$, $i = 2, \ldots, N$, are Schur stable, where $\lambda_i$, $i = 2, \ldots, N$, denote the eigenvalues of $\hat{H}$. As a result,

$$\tilde{A}_c = I_{N-1} \otimes A + \hat{H} \otimes B \Gamma,$$  (45)

is a Schur matrix. As rational numbers are dense, the matrix $\Gamma$ can be selected as a rational matrix.

There exist $\gamma_1, \gamma_2$ such that $\Lambda = \Gamma / \gamma_2$ is an integer matrix and $\nu_{ij} = w_{ij} / \gamma_1$ are integers. It is easy to see that the graph associated with $\nu_{ij}$ is also $G$. One has

$$\begin{align*}
\gamma_1(-\nu_{ij}) &= -w_{ij}, \\
\gamma_1\left(\sum_{j=1, j \neq i}^N \nu_{ij}\right) &= \sum_{j=1, j \neq i}^N w_{ij} = \frac{d_i}{1 + d_i} = 1 - w_{ii}.
\end{align*}$$

That is, $\gamma_1 L = I_N - W = \hat{L}$ and hence $\gamma_1 H = \hat{H}$. Letting $\gamma = \gamma_1 \gamma_2$ gives that $A_c = A_c$ is a Schur matrix. The proof is then completed. \hfill \square

**Lemma 6.2:** Under Assumptions 6.1, 6.2 for the $\gamma$, $\Lambda$, $\nu_{ij}$, $i, j = 1, \ldots, N$, given in Lemma 6.1 define the following two matrices

$$A_c = I_N \otimes A + \gamma L \otimes B A, \quad B_c = \gamma L \otimes B A.$$  (46)

There exist $0 < \rho < 1$ and $M, M_A, M_B > 0$ such that, for $k \geq 0$,

$$\begin{align*}
\|A_c^k - (1 \otimes I_s)A^k r^T \otimes I_s\| &\leq M \rho^k, \\
\|A^k r^T \otimes I_s\| &\leq M_A, \\
\sum_{j=0}^{k-1} \|A_{c}^{k-j-1} B_c\| N s &\leq M_B.
\end{align*}$$  (47)  (48)  (49)

**Proof:** A direct calculation shows that

$$A_c = (T \otimes I_s) \begin{bmatrix} A & 0 \\ 0 & \hat{A} \end{bmatrix} (T^{-1} \otimes I_s)$$

and hence

$$A_{c}^{k} = (T \otimes I_s) \begin{bmatrix} A^k & 0 \\ 0 & \hat{A}^k \end{bmatrix} (T^{-1} \otimes I_s)$$

$$= (1 \otimes I_s) A^k (T^T \otimes I_s) + (U \otimes I_s) \hat{A}^k (V \otimes I_s).$$

Then,

$$\|A_{c}^{k} - (1 \otimes I_s)A^k (T^T \otimes I_s)\| = \|(U \otimes I_s) \hat{A}^k (V \otimes I_s)\| \leq M \rho^k,$$

as $\hat{A}_c$ is a Schur matrix, which implies (47).

The assumption that $A$ is neutrally stable implies (48) in a straightforward manner.

Finally, another calculation shows that

$$A_c^k B_c = (T \otimes I_s) \begin{bmatrix} A^k & 0 \\ 0 & \hat{A}^k \end{bmatrix} (T^{-1} \otimes I_s) (\gamma L \otimes B A)$$

$$= \gamma(U \otimes I_s) \hat{A}^k [(V L) \otimes (B A)].$$

So (49) is true, because $A_c$ is a Schur matrix. \hfill \square

**Remark 6.1:** It is assumed that the matrix $A$ is neutrally stable in Assumption 6.2 for two reasons. On the one hand, the existence of the matrix $\Gamma$ in the proof of Lemma 6.1 is guaranteed under this assumption. On the other hand, the system trajectories are expected to be bounded in (48) under this assumption.

The main result can now be given as follows

**Theorem 6.1:** For a given communication graph $G$ satisfying Assumption 6.1 and two matrices $A$ and $B$ satisfying Assumption 6.2 there exist an integer matrix $\Lambda$, integers $\nu_{ij}$, $i, j = 1, \ldots, N$, whose graph is $G$, and a scalar $\gamma > 0$, such that the closed-loop system composed of (42) and (43) has the desired control performance,

$$\|x(k) - 1 \otimes x_{\infty}(k)\| \leq M \rho^k \|x(0)\| + M_B 2^{-m},$$  (50)

for $|\delta(k)| < 2^{-m}$, where $x(0) = A^k (r^T \otimes I_s)x(0)$ and $\rho, M, M_A, M_B$ are given in Lemma 6.2. Moreover, the signals $y_i(k), u_i(k) \in [-2^{-m}, 2^{-m} - 1], \quad i = 1, \ldots, N$, if the initial condition satisfies $\|x(0)\| \leq R_0$ for

$$R_0 = \beta - M_B 2^{-m} M + \sqrt{N} M_A,$$

$$\beta < 2^{-n-m-1} \min \left\{ \frac{1}{\gamma}, \frac{1}{\|A\|\|L\|} - N s 2^{-n+1} \right\}.$$  (51)

**Proof:** The controller (43) can be rewritten as

$$u(k) = \gamma \Lambda \sum_{j=1}^{N} \nu_{ij} [x_i(k) + \delta_i(k)] - (x_j(k) + \delta_j(k)).$$  (52)

Without considering the quantization errors, the closed-loop network dynamics composed of

$$x(k+1) = A x(k) + B u(k)$$  (53)

and the decentralized controller

$$u_i(k) = \gamma \Lambda \sum_{j=1}^{N} \nu_{ij} [x_i(k) - x_j(k)],$$  (54)

takes the following form

$$x(k+1) = A_c x(k)$$  (55)

where $A_c$ is the matrix given by (46). Therefore, the closed-loop system achieves consensus in the sense of

$$\|x(k) - 1 \otimes x_{\infty}(k)\| = \|A_c^k x(0) - (1 \otimes I_s)A^k (r^T \otimes I_s)x(0)\|$$

$$\leq M \rho^k \|x(0)\|$$  (56)

where (47) is used.

When the quantization errors are taken into consideration, the closed-loop system composed of (53) and (52) takes the following form

$$x(k+1) = A_c x(k) + B_c \delta(k)$$  (57)

where $A_c$ and $B_c$ are the matrices given by (46). Then, we have

$$x(k) = A_c^k x(0) + \sum_{j=0}^{k-1} A_c^{k-j-1} B_c \delta(j).$$  (58)

By (47) and (49), the property (50) follows.

From (50), it is easy to see that

$$\|x(k)\| \leq \sqrt{N} M_A \|x(0)\| + M \|x(0)\| + M_B 2^{-m} = \beta$$  (59)

and hence

$$\|y(k)\| = \|x(k)\| \leq \beta < 2^{-n-m-1}$$

$$\|u(k)\| \leq \|A\|\|L\|\|x(k)\| + \|\delta(k)\|$$

$$\leq \|A\|\|L\|([\beta + N s 2^{-n+1}] < 2^{-n-m-1}.$$  (51)

It concludes that $y_i(k), u_i(k) \in [-2^{-m}, 2^{-m} - 1], \quad i = 1, \ldots, N$, \hfill \square

**Remark 6.2:** Based on the controller (43), the implemented controller (24) has the following specific form

$$v_i(k) = \sum_{j=1}^{N} \bar{E}_0^{\nu_{ij}} (\text{sgn}(\nu_{ij})y_j^0(k))$$

$$\cdot \bar{E}_0^{\nu_{ij}} (-\text{sgn}(\nu_{ij})y_j^0(k)) \mod n_p^2.$$  (60)
By combining Theorems 4.1 and 6.1 and noting that the quantization property is simply satisfied, one has the following result.

**Theorem 6.2:** For a given communication graph $G$ satisfying Assumption 6.1 and two matrices $A$ and $B$ satisfying Assumption 6.2, consider the system (40) with the private controller (4), (5), and (6), for two specified integers $n$ and $m$. There exist an integer matrix $A_i$, integers $n_{ij}$, $i, j = 1, \ldots, N$, whose graph is $G$, and a scalar $\gamma > 0$, such that the linear function $\kappa_i$ is as in (43). Let $E_{D_i}$, $E_{R_i}$, and $F_{R_i}$ be designed in Theorem 4.2. Then, the controller (6) takes the specific form (60). For any initial condition satisfying $\|x(0)\| \leq R_0$ with $R_0$ given in (51), the closed-loop system achieves the desired control performance $P_1$ in the sense of (50), as well as $P_2$ and $P_3$.

**Example 2:** We consider the following three-agent system,

\[
\begin{align*}
x_i(k+1) &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} x_i(k) + \begin{bmatrix} 1 \\ 0 \end{bmatrix} u_i(k), \\
y_i(k) &= \gamma x_i(k), \quad i = 1, 2, 3.
\end{align*}
\]

It is a specific form of system (40) with $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and $N = 3$. Obviously, Assumption 6.2 holds.

The communication graph $G$ among the three agents satisfies Assumption 6.1 with

\[
E = \begin{bmatrix} 0 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}, \quad W = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.
\]

By Theorem 15 of [55], we can design $\Gamma = [0, -1]$. With the parameters $\gamma_1 = 0.1$, $\gamma_2 = 1$, and $\gamma = 0.1$, the implemented controller (60) is further designed with $\Delta = \Gamma/\gamma_2$ and $u_{ij} = v_{ij}/\gamma_i$, $i, j = 1, 2, 3$. We set the length and the resolution of the fixed-point rational as $n = 24$ and $m = 8$. With the initial conditions $x_1(0) = [1.12, 3.45]^T$, $x_2(0) = [4.33, 2.09]^T$, and $x_3(0) = [3.67, 2.43]^T$, setting the modular bits for generating keys of Paillier encryption to be 64, we conduct the numerical simulation and obtain the following results, illustrated in Figs. 2 and 3. Fig. 4 presents the first and second components of the agent states which achieve consensus. Specifically, the left graph of Fig. 4 shows that the consensus error for all the three agents practically approaches zero as expected by the desired control performance (50). Similar as Example 1, the consensus error can be reduced by using a higher resolution. At last, the right graph of Fig. 5 presents the control inputs generated by the remote decentralized controllers. Their wild disorderliness verifies that the privacy of each decentralized control input remains intact.

**VII. CONCLUSION**

In this paper, we have established a secure networked control system design approach for large-scale cyberphysical systems using a novel double-layer cryptographic scheme. The approach is based on a design separation principle and is supported by a rigorous analytical proof. Two case studies on secure stabilization of MIMO systems and secure decentralized consensus of MAS have been presented with numerical simulations. The double-layer cryptographic scheme used Paillier and RSA cryptosystems to provide protection of information of plant entities and control units from any malicious party. Even though the approach is general, due to the specific use of Paillier, one can only handle the control laws involving linear computations. In the future work, we are planning to investigate other homomorphic cryptosystems to cater for more complicated nonlinear control laws. The computational performances of the Paillier and RSA algorithms are typically of the order of tens to hundreds of milliseconds [56, 57], this in turn implies that these computations in private controllers do not cause any delay issue in the current discrete-time setting environment if they can be finished within one sampling period. Each cryptographic algorithm has its own advantages and it would be interesting to investigate different options for achieving greater efficiency in future research.

**REFERENCES**

[1] S. Mehrnaeen, S. Jagannathan, and M. L. Crow, “Decentralized dynamic surface control of large-scale interconnected systems in strict-feedback form using neural networks with asymptotic stabilization,” *IEEE Transactions on Neural Networks*, vol. 22, no. 11, pp. 1709–1722, 2011.

[2] T. X. Nghiem and G. J. Pappas, “Receding-horizon supervisory control of green buildings,” in *American Control Conference*. IEEE, 2011, pp. 4416–4421.

[3] S. Baldi, I. Michailidis, E. B. Kosmatopoulos, and P. A. Ioannou, “A “plug and play” computationally efficient approach for control design of large-scale nonlinear systems using cosimulation: a combination of two “ingredients”,” *IEEE Control Systems Magazine*, vol. 34, no. 5, pp. 56–71, 2014.

[4] H. Trentelman, K. Takaba, and N. Monshizadeh, “Robust synchronization of uncertain linear multi-agent systems,” *IEEE Transactions on Automatic Control*, vol. 58, no. 6, pp. 1511–1523, 2013.

[5] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative Control of Multi-agent Systems: Optimal and Adaptive Design Approaches*. Springer Science & Business Media, 2013.

[6] A. Isidori, L. Marconi, and G. Casadei, “Robust output synchronization of a network of heterogeneous nonlinear agents via nonlinear regulation theory,” *IEEE Transactions on Automatic Control*, vol. 59, no. 10, pp. 2680–2691, 2014.

[7] Z. Li, G. Wen, Z. Duan, and W. Ren, “Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs,” *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1152–1157, 2015.

[8] S. Knorn, Z. Chen, and R. H. Middleton, “Overview: Collective control of multiagent systems,” *IEEE Trans. Control of Network Systems*, vol. 3, no. 4, pp. 334–347, 2016.

[9] F. Dörfler and F. Bullo, “Synchronization in complex networks of phase oscillators: A survey,” *Automatica*, vol. 50, no. 6, pp. 1539–1564, 2014.

[10] X. Liu and T. Chen, “Synchronization of complex networks via aperiodically intermittent pinning control,” *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3316–3321, 2015.

[11] A. L. Fradkov, I. V. Miroshnik, and V. O. Nikiforov, *Nonlinear and Adaptive Control of Complex Systems*. Springer Science & Business Media, 2013, vol. 491.

[12] E. Estrada, *The Structure of Complex Networks: Theory and Applications*. Oxford University Press, 2012.

[13] D. Nesic and D. Liberzon, “A unified framework for design and analysis of networked and quantized control systems,” *IEEE Transactions on Automatic Control*, vol. 54, no. 4, pp. 732–747, 2009.

[14] G. C. Walsh, H. Ye, and L. G. Bushnell, “Stability analysis of networked control systems,” *IEEE Transactions on Control Systems Technology*, vol. 10, no. 3, pp. 438–446, 2002.

[15] H. Sandberg, S. Amin, and K. H. Johansson, “Cyberphysical security in networked control systems: An introduction to the issue,” *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.
Fig. 4. Left: profile of first components of agent states; right: profile of second components of agent states.

Fig. 5. Left: profile of consensus errors practically approaching 0; right: profile of control inputs computed by remote controller in the encrypted space.

[16] X. Ge, F. Yang, and Q.-L. Han, “Distributed networked control systems: A brief overview,” Information Sciences, vol. 380, pp. 117–131, 2017.
[17] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2013.
[18] P. Park, H. Khadilkar, H. Balakrishnan, and C. J. Tomlin, “High confidence networked control for next generation air transportation systems,” IEEE Transactions on Automatic Control, vol. 59, no. 12, pp. 3357–3372, 2014.
[19] S. P. Mohanty, U. Choppali, and E. Koungianos, “Everything you wanted to know about smart cities: The internet of things is the backbone,” IEEE Consumer Electronics Magazine, vol. 5, no. 3, pp. 60–70, 2016.
[20] S. A. Haque, S. M. Aziz, and M. Rahman, “Review of cyber-physical system in healthcare,” International Journal of Distributed Sensor Networks, vol. 10, no. 4, p. 217415, 2014.
[21] J. Lee, B. Bagheri, and H.-A. Kao, “A cyber-physical systems architecture for industry 4.0-based manufacturing systems,” Manufacturing Letters, vol. 3, pp. 18–23, 2015.
[22] A. Otto, N. Agatz, J. Campbell, B. Golden, and E. Pesch, “Optimization approaches for civil applications of unmanned aerial vehicles (UAVs) or aerial drones: A survey,” Networks, vol. 72, no. 4, pp. 411–458, 2018.
[23] M. Cummings, “Operator interaction with centralized versus decentralized uav architectures,” in Handbook of Unmanned Aerial Vehicles. Springer, 2015, pp. 977–992.
[24] F. Kiessling, R. Puschmann, A. Schmieder, and E. Schneider, Contact Lines for Electric Railways: Planning, Design, Implementation, Maintenance. John Wiley & Sons, 2018.
[25] A. A. Cárdenas, S. Amin, and S. Sastry, “Research challenges for the security of control systems,” in HotSec, 2008.
[26] R. S. Smith, “Covert misappropriation of networked control systems: Presenting a feedback structure,” IEEE Control Systems Magazine, vol. 35, no. 1, pp. 82–92, 2015.
[38] K. Kogiso and T. Fujita, “Cyber-security enhancement of networked control systems using homomorphic encryption,” in *54th IEEE Conference on Decision and Control*, 2015, pp. 6836–6843.

[39] F. Farokhi, I. Shames, and N. Batterham, “Secure and private cloud-based control using semi-homomorphic encryption,” *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.

[40] 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, no. 22, pp. 175–180, 2016.

[41] L. Sadeghikhorraram, M. Zamani, A. Safavi, and Z. Chen, “Secure control mechanism for network environments,” *IEEE Transactions on Cybernetics*, 2019, under review.

[42] W. Fang, M. Zamani, and Z. Chen, “Secure and privacy preserving consensus for second-order systems based on paillier encryption,” *Systems and Control Letters*, 2020, under review.

[43] X. Duan, J. He, P. Cheng, Y. Mo, and J. Chen, “Privacy preserving maximum consensus,” in *54th IEEE Conference on Decision and Control*, 2015, pp. 4517–4522.

[44] M. Ruan, M. Ahmad, and Y. Wang, “Secure and privacy-preserving average consensus,” in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. ACM, 2017, pp. 123–129.

[45] Y. Mo and R. M. Murray, “Privacy preserving average consensus,” *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2017.

[46] M. Kefayati, M. S. Talebi, B. H. Khalaj, and H. R. Rabiee, “Secure consensus averaging in sensor networks using random offsets,” in *IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 2007, pp. 556–560.

[47] E. Nozari, P. Tallapragada, and J. Cortes, “Differentially private average consensus with optimal noise selection,” *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[48] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, “Survey of various homomorphic encryption algorithms and schemes,” *International Journal of Computer Applications*, vol. 91, no. 8, 2014.

[49] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[50] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.

[51] M. Bellare and P. Rogaway, “Optimal asymmetric encryption,” in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1994, pp. 92–111.

[52] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, “Need for controllers having integer coefficients in homomorphically encrypted dynamic system,” in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 5020–5025.

[53] F. M. Callier and C. A. Desoer, *Linear System Theory*. Springer Science & Business Media, 2012.

[54] Z.-P. Jiang and Y. Wang, “Input-to-state stability for discrete-time nonlinear systems,” *Automatica*, vol. 37, no. 6, pp. 857–869, 2001.

[55] Z. Li and Z. Duan, *Cooperative Control of Multi-agent Systems: A Consensus Region Approach*. CRC Press, 2014.

[56] C. Jost, H. Lam, A. Maximov, and B. J. Smeets, “Encryption performance improvements of the paillier cryptosystem.” *IACR Cryptology ePrint Archive*, vol. 2015, p. 864, 2015.