Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption

Conference Paper · December 2015

DOI: 10.1109/CDC.2015.7403296

Kiminao Kogiso
The University of Electro-Communications

Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption

Kiminao Kogiso and Takahiro Fujita

Abstract— **This paper proposes a new concept of controller encryption for enhancement of the cyber-security of networked control systems and presents how to encrypt a linear controller using our modified homomorphic encryption schemes based on public-key RSA and ElGamal encryption systems. A remarkable advantage of the controller encryption is to be able to conceal several informations processed inside the controller device, such as controller parameters, references (recipes), measurements, control commands, and parameters of plant models in the internal model principal, maintaining an original function of the controller. Therefore, even if malicious users hacked the controller device by unauthorized accesses, it would take much time and cost to decipher and steal the control system's information. Finally, numerical examples confirm that only the scrambled parameters and signals can be seen in the controller device of the security-enhanced networked control system.**

I. Introduction

Cyber-security of the networked control system is one of the significantly important issues in the control engineering area because the networked control system is applied to the industrial and critical infrastructures such as water, transportation and electricity networks [1]. There are several approaches such as the model-based detections methods [2], [3], risk management for the threats [4], and protections of the signals transmitted over the communication channels [5], [6], in order to enhance the cyber-security against malicious users and adversaries. The authors are interested in how to prevent the malicious users and the adversaries from monitoring and stealing the information to operate the control system, in terms of a cryptography.

Cryptography is an important technology enabling to protect information against the third parity such as the malicious users and adversaries, and recently a public-key cryptography is in widespread use to cloud systems [7], [8]. For example, the RSA encryption system [9], named after its inventors Rivest, Shamir, and Adleman, is the first public-key encryption system in the widespread use and is still important to learn. The ElGamal encryption system [10] is the more secure public-key encryption system, and actually is used in the free GNU privacy guard, the digital signature algorithms. In such a public-key encryption scheme, the public key generated by some party severs as an encryption key; anyone who knows that public key can use it to encrypt messages and generate corresponding ciphertexts. The private key serves as a decryption key and is used by the party who knows it to recover the original message from any ciphertext generated using the matching public key. The secrecy of encrypted messages is preserved even against an adversary who knows the encryption key [11].

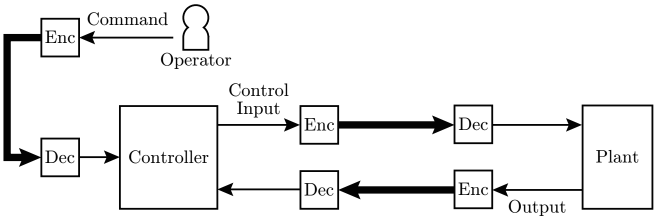


Fig. 1. A conventional configuration of secure networked control systems that the signals over communication links are encrypted.

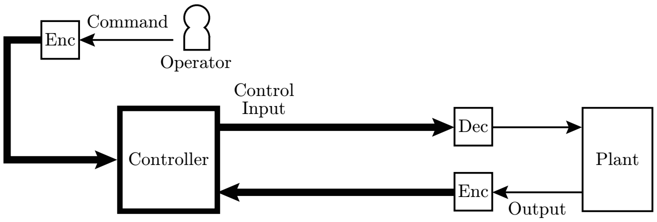


Fig. 2. The proposed configuration in this study that not only the signals over communication links but also parameters of the controller are encrypted and the controller has no decryption processes requiring a private key.

Cryptography-based protection of the transmission signals over the communication links, as illustrated in Fig. 1, is one of the effective approaches to make the networked control system secure. However, it requires to manage a number of the private keys simultaneously, used in the decryption process, and if the malicious users hacked the control device or the decryption device by the unauthorized accesses, they could record and steal the most important and secret informations to operate the system, such as controller parameters, references (recipes), measurements and control commands, as well as parameters of plant models in the internal model principal. Therefore, decreasing the number of sites of a private key as well as protecting the controller are meaningful for achieving the security-enhanced networked control system.

When considering the encryption of the controller, we need mathematical operations over the space of the ciphertexts, corresponding to a linear algebra over the real vector space. In the case of the RSA and ElGamal public-key encryptions, the ciphertexts space is a subset of whole integers and a homomorphism holds for modular multiplication.

K. Kogiso is with Faculty of Mechanical Engineering and Intelligent Systems, University of Electro-Communications, Chofu, Tokyo 182-8585, Japan kogiso@uec.ac.jp

T. Fujita is with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Nara, 630-0192 Japan

In [8] and [12], properties of the operation with regard to the homomorphism are discussed, assuming applications to cloud system and sensing system. In this study, actually, the homomorphism also plays a fundamental role of realizing algebraic operations of the ciphertexts used in the controller. However, as far as the authors know, there do not seem to be studies on the encryption of the controller for the cyber-security enhancement of the networked control system, especially in the control engineering area.

This paper aims at proposing a novel concept of encrypting a linear controller using the homomorphic encryptions, which are RSA and ElGamal schemes, and also at presenting how to realize the encrypted controller with our modified encryption schemes, as figured in Fig. 2. The most remarkable property of the concept is to encrypt the controller's parameters and the signals inside the controller device. Another property is also significant that the controller need not to keep any private keys for calculating the control input, which means that the decryption process is not required inside the controller. That is, in the encrypted controller, the encrypted output (the control input) is directly calculated from the encrypted input with the encrypted controller parameters, without any decryption processes. The resulting controller has only ciphertexts so that it will be possible to contribute to enhancing the cyber-security of the networked control system. Furthermore, the numerical examples illustrate how the encrypted controller works in the networked controls system and that the encrypted controller functions to enhance the cyber-security, comparing with the conventional secure networked control system. Moreover, this study demonstrates subspace identification [13] (`n4sid` in Matlab) using the encrypted reference and output on assumption that the malicious users successfully hacked the controller device without their knowledge that the control system is encrypted.

The structure of this remaining paper is as follows. Section II introduces essences of homomorphic encryptions. Section III proposes the novel concept about the encryption of the controller, states the controller encryption problem, and presents how to realize the encrypted controller based on the RSA and ElGamal encryption schemes, respectively. Section IV shows the numerical example with the demonstration results of the subspace identification. Finally, section V concludes this paper.

II. Essences of Homomorphic Encryption

A. Preliminaries

1) Notations: Through this paper, we use the following notations. $\mathbb{R}$ is the set of real numbers, $\mathbb{Z}^+$ is the set of nonnegative integers, $\mathbb{Z}_n$ is a reduced residue system modulo n, i.e., $\mathbb{Z}_n := \{0, 1, \cdots, n-1\}$, $\mathcal{M}$ is a message space, $\mathcal{C}$ is a ciphertext space, and $\mathbb{Z}_n^\times$ is the set of integers co-prime to n which belongs to $\mathbb{Z}_n$ (or is an multiplicative group of residues mudulo n), 1^k is a binary string of length k. For $n \in \mathbb{Z}^+$, Euler's phi function $\varphi(n)$ returns the order of the group $|\mathbb{Z}_n^\times|$. Euler's theorem is well known in number theory, which states that if n and a are co-prime positive integers, then

$$a^{\varphi(n)} = 1 \mod n, \; \forall n \in \mathbb{Z}^+, \; \forall a \in \mathbb{Z}_n^\times. \tag{1}$$

2) Public-key encryption scheme: The public-key encryption scheme consists of three algorithms: key generation (Gen), encryption (Enc), and decryption (Dec);

- Gen: on input 1^k generate the private key k_s and the public key k_p:
$$\mathsf{Gen}\left(1^k\right) = (k_p, k_s).$$
Determine the message space $\mathcal{M}$.
- Enc: on input the public key k_p and a plaintext $m \in \mathcal{M}$, compute the ciphertext c:
$$\mathsf{Enc}(k_p, m) = c.$$
- Dec: on input the private key k_s(or both of k_p and k_s) and the cihpertext $c \in \mathcal{C}$, compute the plaintext m':
$$\mathsf{Dec}(k_s, c) = m'.$$
Here, the cihpertext encrypted by Enc must be decrypted to be the same as the original plaintext.
$$m' = \mathsf{Dec}\left(k_s, \mathsf{Enc}(k_p, m)\right) = m, \; \forall m \in \mathcal{M}$$

As a public-key encryption system is defined as the algorithms Gen, Enc, and Dec, it is denoted as $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

B. Homomorphic encryption schemes

The homomorphism of the public-key encryption plays the significant role in this paper so its definition is shown below.

Definition 1: An encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *homomorphic* if the three following conditions are fulfilled.

1) the set $\mathcal{M}$ together with operation $\bullet$ and the set $\mathcal{C}$ together with operation $*$ form a group, respectively.
2) any plaintext m in $\mathcal{M}$ is mapped into $\mathcal{C}$, i.e.,
$$\mathsf{Enc}(k_p, m) \in \mathcal{C}, \; \forall m \in \mathcal{M}.$$
3) If for any plaintexts, m_1 and $m_2 \in \mathcal{M}$, the corresponding ciphertexts are written as
$$c_1 = \mathsf{Enc}(k_p, m_1) \in \mathcal{C} \;\text{ and }\; c_2 = \mathsf{Enc}(k_p, m_2) \in \mathcal{C},$$
then the following equation:
$$\mathsf{Enc}(k_p, m_1 \bullet m_2) = c_1 * c_2, \tag{2}$$
is held.

1) RSA encryption: The scheme of the RSA encryption [9] is defined in the form of the algorithms, $\mathcal{E}_R = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

- Gen: Generate the public key $k_p = (n, e)$ and the private key $k_s = d$, where k-bit binary $n = pq$ with different prime integers p and q, e is a positive integer co-prime to Euler's phi function $\varphi(n)$ and is less than $\varphi(n)$, and d is a modular multiplicative inverse of the integer e modulo $\varphi(n)$ such that
$$ed \mod \varphi(n) = 1$$

holds. Here, the message (plaintext) space is $\mathcal{M} = \mathbb{Z}_n$.

- Enc: Encrypt the plaintext $m \in \mathbb{Z}_n$ using the public key $k_p = (n, e)$ in order to compute the ciphertext c, i.e.,

$$\mathsf{Enc}(k_p, m) := m^e \mod n = c. \tag{3}$$

- Dec: Decrypt the cipher text c using the private key $k_s = d$ and the public key k_p in order to compute the plaintext m', i.e.,

$$\mathsf{Dec}(k_s, c) := c^d \mod n = m'. \tag{4}$$

If the ciphertext c is generated by (3), then from $ed \mod n = 1$,

$$\begin{aligned} m' &= c^d \mod n = m^{ed} \mod n \\ &= m^{(1+l\varphi(n))} \mod n \quad \exists\, l \in \mathbb{Z}^+, \end{aligned} \tag{5}$$

holds, the Euler's theorem (1) enables to hold $m' = m$.

The RSA encryption allows homomorphic computation of the multiplication on the ciphertexts [11]. With two plain texts m_1 and $m_2 \in \mathbb{Z}_n$ and the corresponding ciphertexts c_1 and c_2:

$$\begin{aligned} c_1 &= \mathsf{Enc}(k_p, m_1) = m_1^e \mod n \ \text{ and} \\ c_2 &= \mathsf{Enc}(k_p, m_2) = m_2^e \mod n, \end{aligned}$$

the ciphertext of $m_1 m_2$, multiplication of m_1 and m_2, results in,

$$\begin{aligned} \mathsf{Enc}(k_p, m_1 m_2) &= (m_1 m_2)^e \mod n \\ &= (m_1^e \mod n)(m_2^e \mod n) \mod n \\ &= \mathsf{Enc}(k_p, m_1)\,\mathsf{Enc}(k_p, m_2) \mod n \\ &= c_1 c_2 \mod n. \end{aligned} \tag{6}$$

This means that in (2), the operation $\bullet$ over the set $\mathcal{M}$ is multiplication and the operation $*$ over the set $\mathcal{C}$ is modular multiplication.

Properties of the RSA encryption are as follow:

- The encryption scheme $\mathcal{E}_R$ is deterministic, i.e., $\forall k_p$,

$$m_1 = m_2 \Leftrightarrow \mathsf{Enc}(k_p, m_1) = \mathsf{Enc}(k_p, m_2).$$

- For any public key k_p, integers 0 and 1 are invariant, i.e., $\forall e$, n,

$$\begin{aligned} \mathsf{Enc}(k_p, 1) &= 1^e \mod n = 1, \\ \mathsf{Enc}(k_p, 0) &= 0^e \mod n = 0. \end{aligned}$$

2) ElGamal encrpytion: The scheme of the ElGamal encryption [10] is defined in the form of the algorithms, $\mathcal{E}_E = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

- Gen: Generate the public key $k_p = (\mathbb{G}, q, g, h)$ and the private key $k_s = s$, where q is k-bit binary of a prime integer, $\mathbb{G} \subset \mathbb{Z}_p^\times$ is a cyclic group of the order q modulo prime p satisfying $p - 1 \mod q = 0$, $g \in \mathbb{G}$ is a generator of $\mathbb{G}$, s is a randomly chosen element of $\mathbb{Z}_q$ so that $h = g^s \mod p$, and the message space is $\mathcal{M} = \mathbb{G}$.
- Enc: Encrypt the plaintext $m \in \mathbb{G}$ using the public key $k_p = (\mathbb{G}, q, g, h)$ in order to compute the ciphertext C:

$$\begin{aligned} \mathsf{Enc}(k_p, m) &:= (g^r \mod p,\ m h^r \mod p) \\ &= (c_1, c_2) = C, \end{aligned} \tag{7}$$

where r is a random value uniformly chosen from $\mathbb{Z}_q$.

- Dec: Decrypt the ciphertext $C = (c_1, c_2)$ using the private key $k_s = s$ and the public key $k_p = (\mathbb{G}, q, g, h)$ in order to compute the plaintext m':

$$\mathsf{Dec}(k_s, C) := c_2 \left(c_1^s\right)^{-1} \mod p = m', \tag{8}$$

where $\left(c_1^s\right)^{-1}$ is a modular multiplicative inverse of the integer c_1^s modulo p. If the ciphertext C is encrypted by (7), then $m' = m$ holds because of the following;

$$\begin{aligned} m' &= c_2 \left(c_1^s\right)^{-1} \mod p \\ &= m h^r \left(g^{rs}\right)^{-1} \mod p \\ &= m g^{rs} g^{-rs} \mod p \\ &= m. \end{aligned}$$

The ElGamal encryption allows homomorphic computation of the multiplication on the ciphertexts as well. With two plain texts m_1 and $m_2 \in \mathbb{G}$ and the corresponding ciphertexts in (7):

$$\begin{aligned} C_1 &= \mathsf{Enc}(k_p, m_1) = \left(g^{r_1} \mod p,\ m_1 h^{r_1} \mod p\right), \\ C_2 &= \mathsf{Enc}(k_p, m_2) = \left(g^{r_2} \mod p,\ m_2 h^{r_2} \mod p\right), \end{aligned}$$

ciphertext of $m_1 m_2$, multiplication of m_1 and m_2, with a random value $r = r_1 + r_2$, results in

$$\begin{aligned} \mathsf{Enc}(k_p, m_1 m_2) &= (g^r \mod p,\ m_1 m_2 h^r \mod p) \\ &= (g^{r_1} g^{r_2} \mod p,\ m_1 h^{r_1} m_2 h^{r_2} \mod p) \\ &= C_1 \times_e C_2 \mod p, \end{aligned} \tag{9}$$

where the notation $\times_e$ in (9) denots an element-wise (Hadamard) product of C modulo p. This means that in (2), the operation $\bullet$ over the set $\mathcal{M}$ is the multiplication and the operation $*$ over the set $\mathcal{C}$ is the Hadamard product.

Properties of the ElGamal encryption are as follow:

- The encryption scheme $\mathcal{E}_E$ is not deterministic, that is, two ciphertexts computed by $m_1 = m_2$ are not always same because the random value r is used in Enc algorithm.
- The message space $\mathcal{M} = \mathbb{G}$ generated by the above algorithms is a proper subgroup of a group $\mathbb{Z}_p^\times$. Therefore, the message space includes only a part of elements of $\mathbb{Z}_p^\times$, and we cannot encrypt an arbitrary integers more than 1 and less than p.

III. Encryption of Controller

A. Controller encryption problem

In this study, we consider the situation in which for a plant, a discrete-time linear controller:

$$f : \left\{ \begin{array}{rcl} x(t+1) &=& Ax(t) + Bv(t) \\ u(t) &=& Cx(t) + Dv(t) \end{array} \right. \tag{10}$$

is designed to achieve appropriate and desired control specifications of the networked control system. t is a step, A, B, C, and D are parameters of the controller, $x \in \Re^{n_c}$ is a state of it, $v \in \Re^{m_c}$ is an input to the controller such as an output of the plant (measurements or feedback informations) and a command from an operator (references or recipe informations), and $u \in \Re^{l_c}$ is an output of the controller (a control input to the plant). The equation (10) is equivalently rewritten in the following;

$$\begin{bmatrix} x(t+1) \\ u(t) \end{bmatrix} = f(\Phi, \xi(t)) = \Phi\xi(t), \tag{11}$$

where the parameter Φ and the state and the input ξ are as follow;

$$\Phi := \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Re^{\alpha\times\beta}, \quad \xi := \begin{bmatrix} x \\ v \end{bmatrix} \in \Re^{\beta}.$$

with $\alpha := n_c + l_c$ and $\beta := n_c + m_c$.

The parameters and the signals, Φ and ξ, are processed inside a control device or a particular computer to yield the output, u. If someone performed unauthorized accesses to the control device, Φ and ξ should be monitored and recorded to inflict damage on the control system or to steal the information of the control operation (or the plant model via system identification) based on the recorded ξ and u for the purpose of revers engineering. From the engineering viewpoint, it is significant to discuss the control method possible to protect from recording and stealing the parameters and the signals by malicious users. Then, this motivates to consider the problem that the information appearing in the controller are concealed by an encryption appropriate for the control system. In other words, the problem of the controller encryption is that encrypting all of the information appearing in the controller, the encrypted output is directly calculated from the encrypted input with the encrypted controller parameters, without any decryption processes required inside the controller. The resulting controller has only ciphertexts so that it will be possible to contribute to enhancing the cyber-security of the networked control system.

The novel concept of an encryption of the controller, then, is introduced to state the controller encryption problem.

Definition 2: Assumes that given a linear controller f in (10) for a networked control system, controller's input v and output u are encrypted by an encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. If there exists a map $f_{\mathcal{E}}$ such that an equation:

$$f_{\mathcal{E}}\left(\mathsf{Enc}(k_p, \overline{\Phi}), \mathsf{Enc}(k_p, \overline{\xi})\right) = \mathsf{Enc}(k_p, \overline{f}(\Phi, \xi)), \tag{12}$$

holds, then $f_{\mathcal{E}}$ is an *encrypted controller* to f. Here, $\overline{\Phi} \in \mathcal{M}^{\alpha\times\beta}$, $\overline{\xi} \in \mathcal{M}^{\beta}$, and $\overline{f}(\cdot) \in \mathcal{M}^{\alpha}$ are the plaintexts obtained from $\Phi \in \Re^{\alpha\times\beta}$, $\xi \in \Re^{\beta}$, and $f(\cdot) \in \Re^{\alpha}$, respectively.

The equation of (12) shows that the controller's encrypted output of the right hand side of it is equivalent to the output calculated by the controller's encrypted parameters and the controller's encrypted state and input through $f_{\mathcal{E}}$. Here, it should be noted that in calculating the encrypted output, any decryption processes are not performed. This is, the concept does not requires the control device to keep any private keys that are used to recover the encrypted signals. This is a main idea to be able to enhance the cyber-security of the networked control systems. Therfore, the problem considered in this paper is how to realize the encrypted controller $f_{\mathcal{E}}$ for the linear controller f and the encryption scheme $\mathcal{E}_R$ or $\mathcal{E}_E$, which will be stated in the section III-B. Moreover, since the plaintexts in (12), such as $\overline{\Phi}$ and $\overline{\xi}$, are whole numbers, this approach requires rounding the real number to the nearest integer in the plaintext space $\mathcal{M}$. In this process, a quantization error arises, which will be stated in the section III-C.

Additionally, it is assumed in this paper that signals over the communication links between the controller and the plant and between the controller and the operator are encrypted by the appropriate encryption scheme $\mathcal{E}_R$ or $\mathcal{E}_E$. It also assumes that there are no transmission delays and data losses over the communication links. This is because we want to focus on how to encrypt the controller.

B. Realization of the encrypted controller

In this study, the homomorphism, as stated in II-B, is used to realize the encrypted controller $f_{\mathcal{E}}$. The homomorphism (2) of the RSA and ElGamal encryptions is held for the multiplication, while the operation of the controller (11) consists of the multiplication and the addition. Thereby, the operation f is considered to be a composition product of addition f^{+} and multiplication $f^{\times}$, i.e.,

$$f = f^{+} \circ f^{\times},$$

where the multiplication is defined as,

$$f^{\times}(\Phi, \xi) := \begin{bmatrix} \Phi_1\xi_1 & \Phi_2\xi_2 & \cdots & \Phi_\beta\xi_\beta \end{bmatrix} =: \Psi,$$

from a linear combination of the matrix Φ and the vector ξ:

$$\Phi\xi = \Phi_1\xi_1 + \Phi_2\xi_2 + \cdots + \Phi_\beta\xi_\beta = \sum_{l=1}^{\beta} \Phi_l\xi_l,$$

and the addition is defined as,

$$f^{+}(\Psi) := \sum_{l=1}^{\beta} \Psi_l,$$

where ξ_l denotes the l-th component of the column vector ξ, Φ_l does the l-th row vector of the matrix Φ, Ψ_l does the l-th row vector of the matrix Ψ, and β is the maximum row number. Therefore, the multiplication $f^{\times}$ can be replaced with the homomorphism (2) to be able to incorporate the RSA or the ElGamal encryption into calculation inside the controller device.

Our idea for realizing the encrypted controller is as follows; In the controller device, the multiplication $f^{\times}$ of the parameters Φ and the signals ξ, which can be concealed by the homomorphism, is processed and the controller device outputs the encrypted matrix Ψ to the plant. In the decryption device just before the plant, the decryption of Ψ as well as the addition f^{+} of the decrypted Ψ are processed. In this way, the addition is separated from the original linear controller

(10) and so we need to modify the decryption process Dec. Then, this study introduces the modified encrypted scheme $\mathcal{E}^+ = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}^+)$ below;

Gen : On input $1^k \rightarrow (k_p, k_s)$ generate a public key k_p and a private key k_s in the similar way of $\mathcal{E}$.

Enc : $\mathcal{M}^\alpha \rightarrow \mathcal{C}^\alpha$ This is the same as one in $\mathcal{E}$, and the plaintext (vector) $m = [m_1, m_2, \cdots, m_\alpha]^\top \in \mathcal{M}^\alpha$ is encrypted in the component wise to compute,

$$\mathsf{Enc}(k_p, m) = \begin{bmatrix} \mathsf{Enc}(k_p, m_1) \\ \mathsf{Enc}(k_p, m_2) \\ \vdots \\ \mathsf{Enc}(k_p, m_\alpha) \end{bmatrix}.$$

Here, a matrix version of $\mathsf{Enc}(\cdot, M)$ with $M \in \mathcal{M}^{\alpha\times\beta}$ that returns $C \in \mathcal{C}^{\alpha\times\beta}$ is also defined.

Dec$^+$: $\mathcal{C}^{\alpha\times\beta} \rightarrow \mathcal{M}^\alpha$ the ciphertext (matrix):

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1\beta} \\ c_{21} & c_{22} & \cdots & c_{2\beta} \\ \vdots & \vdots & & \vdots \\ c_{\alpha 1} & c_{\alpha 2} & \cdots & c_{\alpha\beta} \end{bmatrix},$$

is decrypted for each of the component by $\mathsf{Dec}(k_s, \cdot)$, and then sum each row vector:

$$\begin{aligned} \mathsf{Dec}^+(k_s, C) &= \sum_{i=1}^{\beta} \begin{bmatrix} \mathsf{Dec}(k_s, c_{1i}) \\ \mathsf{Dec}(k_s, c_{2i}) \\ \vdots \\ \mathsf{Dec}(k_s, c_{\alpha i}) \end{bmatrix} \\ &=: (f^+ \circ \mathsf{Dec})(k_s, C). \end{aligned}$$

where $\mathsf{Dec}(k_s, C)$ gives the plaintext so that the last term is not strictly accurate. Here, we assume that $M = \overline{M} (= \mathsf{Dec}(k_p, C))$ with a plaintext (matrix) $\overline{M}$ corresponding to a real matrix M. For more details, please see the section III-C.

Consequently, the modified encryption scheme $\mathcal{E}^+$ enables to realize the encrypted controller to the linear controller (10).

Theorem 1: Assume that the quantization errors between Φ and $\overline{\Phi}$ and between ξ and $\overline{\xi}$, are approximately zeros. For the linear controller f in (11), an encrypted controller $f^\times_{\mathcal{E}^+} : \mathcal{C}^{\alpha\times\beta} \times \mathcal{C}^\beta \rightarrow \mathcal{C}^{\alpha\times\beta}$ by the encryption scheme $\mathcal{E}^+ = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}^+)$ is formulated as,

$$\begin{aligned} &f^\times_{\mathcal{E}^+}(\mathsf{Enc}(k_p, \overline{\Phi}), \mathsf{Enc}(k_p, \overline{\xi})) \qquad (13) \\ &= \begin{bmatrix} \mathsf{Enc}(k_p, \overline{\Phi}_{11}) * \mathsf{Enc}(k_p, \overline{\xi}_1) & \cdots & \mathsf{Enc}(k_p, \overline{\Phi}_{1\beta}) * \mathsf{Enc}(k_p, \overline{\xi}_\beta) \\ \mathsf{Enc}(k_p, \overline{\Phi}_{21}) * \mathsf{Enc}(k_p, \overline{\xi}_1) & \cdots & \mathsf{Enc}(k_p, \overline{\Phi}_{2\beta}) * \mathsf{Enc}(k_p, \overline{\xi}_\beta) \\ \vdots & & \vdots \\ \mathsf{Enc}(k_p, \overline{\Phi}_{\alpha 1}) * \mathsf{Enc}(k_p, \overline{\xi}_1) & \cdots & \mathsf{Enc}(k_p, \overline{\Phi}_{\alpha\beta}) * \mathsf{Enc}(k_p, \overline{\xi}_\beta) \end{bmatrix}, \end{aligned}$$

where $\overline{\Phi} \in \mathcal{M}^{\alpha\times\beta}$ and $\overline{\xi} \in \mathcal{M}^\beta$ are respectively a plaintext matrix and vector corresponding to $\Phi \in \Re^{\alpha\times\beta}$ and $\xi \in \Re^\beta$, and $\overline{\Phi}_{ij}$ denotes the ij-th component of the matrix $\overline{\Phi}$. Particularly, the case of $f^\times_{\mathcal{E}^+} = f^\times_{\mathcal{E}^+_R}$ or $f^\times_{\mathcal{E}^+} = f^\times_{\mathcal{E}^+_E}$ respectively indicate that the encrypted controller is based on the modified scheme of the RSA or ElGamal encryption.

Proof: The multiplicative homomorphism in $\mathcal{E}^+$, the l-th row vector of (13) can be rewritten below;

$$\begin{bmatrix} \mathsf{Enc}(k_p, \overline{\Phi}_{1l}) * \mathsf{Enc}(k_p, \overline{\xi}_l) \\ \mathsf{Enc}(k_p, \overline{\Phi}_{2l}) * \mathsf{Enc}(k_p, \overline{\xi}_l) \\ \vdots \\ \mathsf{Enc}(k_p, \overline{\Phi}_{\alpha l}) * \mathsf{Enc}(k_p, \overline{\xi}_l) \end{bmatrix} = \begin{bmatrix} \mathsf{Enc}(k_p, \overline{\Phi}_{1l}\overline{\xi}_l) \\ \mathsf{Enc}(k_p, \overline{\Phi}_{2l}\overline{\xi}_l) \\ \vdots \\ \mathsf{Enc}(k_p, \overline{\Phi}_{\alpha l}\overline{\xi}_l) \end{bmatrix}.$$

Therefore, the left hand side of the above equation is equivalent to what is resulted from the encryption of the components of the multiplication $f^\times(\Phi, \xi)$ by $\mathsf{Enc}(k_p, \cdot)$. From the definition of Dec$^+$ and the assumption that the quantization errors are approximately zeros,

$$\begin{aligned} \mathsf{Dec}^+(k_s, f^\times_{\mathcal{E}^+}(\mathsf{Enc}(k_p, \overline{\Phi}), \mathsf{Enc}(k_p, \overline{\xi}))) &= (f^+ \circ f^\times_{\mathcal{E}^+})(\overline{\Phi}, \overline{\xi}) \\ &= f(\Phi, \xi), \\ \Leftrightarrow f^\times_{\mathcal{E}^+}(\mathsf{Enc}(k_p, \overline{\Phi}), \mathsf{Enc}(k_p, \overline{\xi})) &= \mathsf{Enc}(k_p, \overline{f}(\Phi, \xi)) \end{aligned}$$

is held. At the same time, the operation of (13) does not require the private key k_s so that the $\mathcal{E}^+$-encrypted controller $f^\times_{\mathcal{E}^+}$ satisfies the definition of the encrypted controller. ∎

As stated in *Theorem 1*, with the modified encryption scheme, we can realize the encrypted controller to a general class of linear controllers. It should be noted that the proposed scheme does not allow to operate the addition for the state transition inside the controller device so that the updated state of the controller, $x(t+1)$ in (10), can be seen the first time just after the decryption process in front of the plant. The state, therefore, needs to be fed back to the controller device in order to update the controller's state.

C. Encryption-induced quantization error

The issue of the quantization error arises in changing from the real values inside the controller to the plaintexts, for example, a real value $w = \pi (= 3.141592\cdots)$ is represented by an integer 314 and a gain 10^{-2}, i.e., $w \approx 314 \times 10^{-2}$. In the proposed approach, the real value is represented by the nearest integer in $\mathbb{Z}_n$ in the case of $\mathcal{E}_R$ or $\mathbb{G}$ in the case of $\mathcal{E}_E$ so that the quantization errors would lead the performance degradation. This is worth investigating how the errors caused by quantization with $\mathbb{Z}_n$ or $\mathbb{G}$ degrade performance of the networked control system, and it seems to be still open. Especially in the case of $n = p$, the set $\mathbb{Z}_n$ is denser than $\mathbb{G} \subset \mathbb{Z}_p^\times$ so that the ElGamal encryption would degrade the performance more than the RSA one. In this section, we discuss how the quantization errors happen in the both cases of RSA and ElGamal encryption schemes.

Given the plantext space $\mathcal{M}$ and a real value $w = \zeta\gamma \in \Re$, the following map $\Gamma_{\mathcal{M}} : \Re \rightarrow \mathcal{M}$ is introduced,

$$\Gamma_{\mathcal{M}}(\zeta, \gamma) = \lceil (\zeta\gamma)^+ \rfloor_{\mathcal{M}},$$

where $\lceil \cdot \rfloor_{\mathcal{M}}$ is the nearest integer in $\mathcal{M}$ rounded from the representation. The notation of ζ^+ denotes a map from the real number ζ to nonnegative real number ζ^+, i.e.,

$$\zeta^+ = \begin{cases} \zeta & \text{if } \zeta \geq 0 \\ n + \zeta & \text{if } \zeta < 0 \end{cases},$$

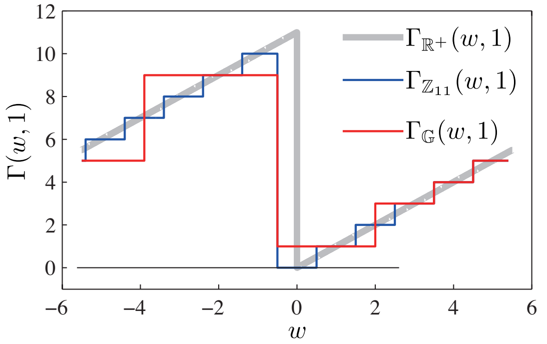


Fig. 3. Quantization errors appearing in the ElGamal encryption.

where $\zeta \in \Re$ and $\zeta^+ \in \Re^+$, and the above map guarantees that the following equation in (4),

$$\zeta + (-\zeta) \mod n = \zeta + (n - \zeta) \mod n = 0,$$

where $-\zeta$ is an addition inverse element and can be replaced with $n - \zeta$.

In the RSA encryption, the plaintext space is $\mathcal{M} = \mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, and setting γ to be sufficiently large could reduce the impact of the quantization errors on the performance degradation. On the other hand, in the ElGamal encryption, the plaintext space is $\mathcal{M} = \mathbb{G} \subset \mathbb{Z}_p^\times$, and the cyclic group $\mathbb{G}$ is intermittent more than $\mathbb{Z}_n$ under $p = n$. Therefore, we have to pay attention to choose γ when using the ElGamal encryption. Fig. 3 shows the errors that occur in quantizing a real value $w \in [-5,\ 5]$ with $\mathbb{G}$ (ElGamal) and $\mathbb{Z}_n$ (RSA) under $\gamma = 1$, $q = 5$, $n = p = 11$, and $g = 3$, where $\mathbb{G} = \{1, 3, 4, 5, 9\}$ and $\mathbb{Z}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. In the figure, the line in gray denotes an ideal change where no errors occur, and the lines in red and blue denote change by the quantization with $\mathbb{G}$ and $\mathbb{Z}_{11}$, respectively. The figure implies that the ElGamal encryption scheme gives impacts on the control performance more than the RSA one. Unfortunately, because the performance analysis for the control system involving the encryption-induced quantization is open, the analysis will be tackled as a future work.

IV. Numerical Example

A numerical example confirms that the encrypted controller can conceal the parameters and the signals inside the controller device, and demonstrates the cyber-security enhancement against the system identification.

A. Settings

In this example, a regulation problem of the networked control system shown in Fig. 4 is considered. The control system consists of the following discrete-time linear plant:

$$\begin{aligned} x_p(t+1) &= \begin{bmatrix} 9.9998 \times 10^{-1} & 1.9700 \times 10^{-2} \\ -1.970 \times 10^{-2} & 9.7025 \times 10^{-1} \end{bmatrix} x_p(t) \\ &\quad + \begin{bmatrix} 9.9900 \times 10^{-5} \\ 9.8508 \times 10^{-3} \end{bmatrix} u(t), \\ y(t) &= \begin{bmatrix} 1 & 0 \end{bmatrix} x_p(t). \end{aligned} \tag{14}$$

where $x_p \in \Re^2$ denotes a state of the plant and an initial state $x(0) = [1\ 0]^T$, and the following linear (PID type) controller in the form of (11):

$$\begin{aligned} \begin{bmatrix} x(t+1) \\ u(t) \end{bmatrix} &= f(\Phi, \xi) = \Phi\xi \\ &= \left[\begin{array}{cc|c} 1 & 0.0063 & 0 \\ 0 & 0.3678 & 0.0063 \\ \hline 10 & -99.90 & 3 \end{array}\right] \left[\begin{array}{c} x(t) \\ \hline -y(t) \end{array}\right], \end{aligned} \tag{15}$$

where $x \in \Re^2$ denote a controller state, and then $\alpha = 3$ and $\beta = 3$.

B. Numerical results

1) RSA encryption: With the keys $k_p = (n, e) = (94399927, 11)$ and $k_s = d = 85800451$ generated, the encrypted controller by the RSA-based encryption scheme $\mathcal{E}_R^+$ is given by,

$$\begin{aligned} &f^\times_{\mathcal{E}_R^+}(\mathsf{Enc}(k_p, \overline{\Phi}), \mathsf{Enc}(k_p, \overline{\xi})) \\ &= \begin{bmatrix} \mathsf{Enc}(\overline{\Phi}_{11})\,\mathsf{Enc}(\overline{\xi}_1) \mod n & \cdots & \mathsf{Enc}(\overline{\Phi}_{13})\,\mathsf{Enc}(\overline{\xi}_3) \mod n \\ \mathsf{Enc}(\overline{\Phi}_{21})\,\mathsf{Enc}(\overline{\xi}_1) \mod n & \cdots & \mathsf{Enc}(\overline{\Phi}_{22})\,\mathsf{Enc}(\overline{\xi}_3) \mod n \\ \mathsf{Enc}(\overline{\Phi}_{31})\,\mathsf{Enc}(\overline{\xi}_1) \mod n & \cdots & \mathsf{Enc}(\overline{\Phi}_{33})\,\mathsf{Enc}(\overline{\xi}_3) \mod n \end{bmatrix} \end{aligned}$$

with the encrypted parameters of the controller,

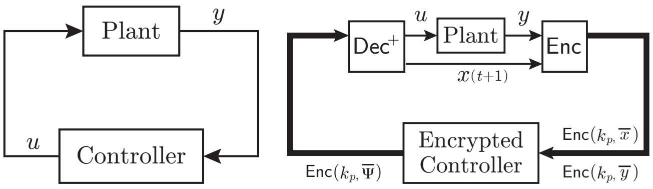
$$\mathsf{Enc}(k_p, \overline{\Phi}) = \begin{bmatrix} 15863779 & 0 & 20066117 \\ 82331095 & 89888050 & 82331095 \\ 0 & 89888050 & 13513040 \end{bmatrix},$$

that is implemented into the controller device, where it is noted that k_p is dropped due to the space.

The simulation result of time-responses of the output y and the control input u is shown in Fig. 5. Fig. 6 shows a time-response of the encrypted output $\overline{y}$. In this case, athough some quantization errors can be seen in the control input response of Fig. 5(b), the output signal monitored inside the controller device is scrambled, comparing with the output response of Fig. 5(a). However, the RSA encryption is deterministic so that the steady state can be identified.

2) ElGamal encryption: With the keys $k_p = (\mathbb{G}, q, g, h) = (\langle g \rangle, 67108913, 3, g^s)$ and $k_s = s$ (random), the encrypted controller by the ElGamal-based encryption scheme $\mathcal{E}_E^+$ is given by,

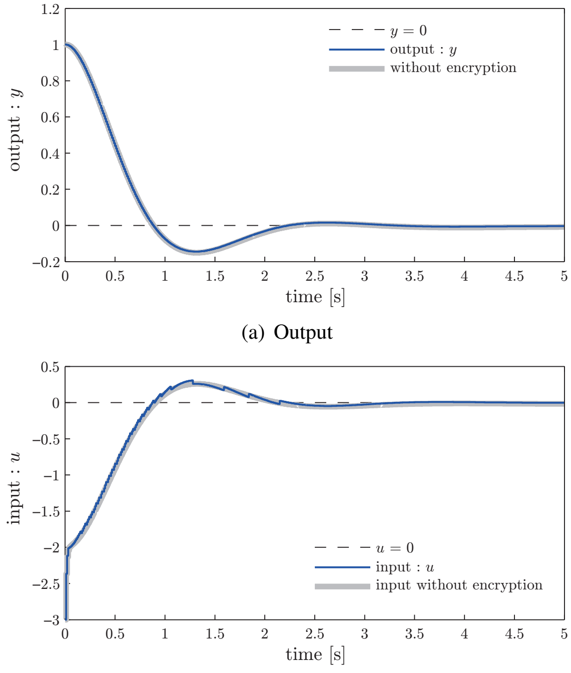
$$\begin{aligned} &f^\times_{\mathcal{E}_E^+}(\mathsf{Enc}(k_p, \overline{\Phi}_1), \mathsf{Enc}(k_p, \overline{\Phi}_2), \mathsf{Enc}(k_p, \overline{\Phi}_3), \mathsf{Enc}(k_p, \overline{\xi})) = \\ &\begin{bmatrix} \mathsf{Enc}(\overline{\Phi}_{11}) \times_e \mathsf{Enc}(\overline{\xi}_1) \mod p & \cdots & \mathsf{Enc}(\overline{\Phi}_{13}) \times_e \mathsf{Enc}(\overline{\xi}_3) \mod p \\ \mathsf{Enc}(\overline{\Phi}_{21}) \times_e \mathsf{Enc}(\overline{\xi}_1) \mod p & \cdots & \mathsf{Enc}(\overline{\Phi}_{23}) \times_e \mathsf{Enc}(\overline{\xi}_3) \mod p \\ \mathsf{Enc}(\overline{\Phi}_{31}) \times_e \mathsf{Enc}(\overline{\xi}_1) \mod p & \cdots & \mathsf{Enc}(\overline{\Phi}_{33}) \times_e \mathsf{Enc}(\overline{\xi}_3) \mod p \end{bmatrix} \end{aligned}$$


Plant
y
u
Controller
u
y
Dec$^+$
Plant
Enc
$x(t+1)$
Encrypted Controller
$\mathsf{Enc}(k_p, \overline{x})$
$\mathsf{Enc}(k_p, \overline{\Psi})$
$\mathsf{Enc}(k_p, \overline{y})$

(a) The normal NCS.

(b) The security-enhanced NCS.

Fig. 4. Feedback control system considered.



(a) Output

(b) Control

Fig. 5. Comparison of output $y(t)$ with and without the proposed cyber-security enhancement: RSA encryption.

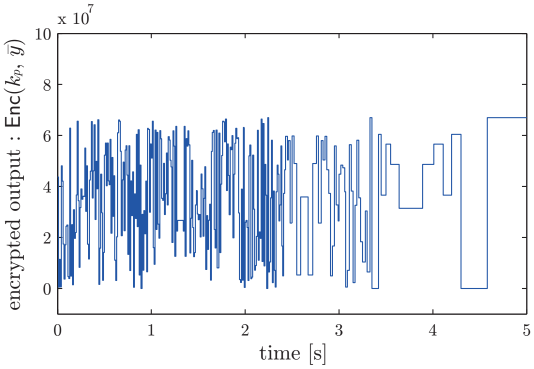


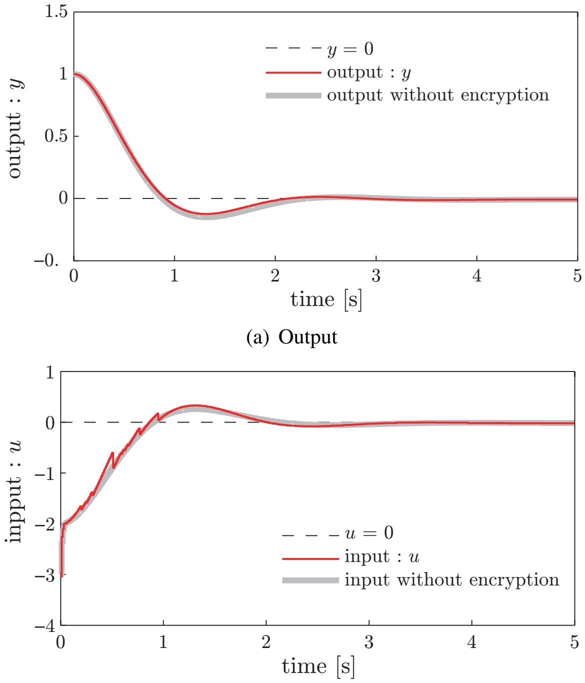
Fig. 6. A time-response of the controller's input encrypted by the RSA encryption, $\mathsf{Enc}\,(k_p, \overline{y}(t))$.

where $\mathbb{G}$ is the cyclic group in the order $q = 67108913$ with modulo $p = 134217827$.

The simulation result of time-responses of the output y and the control input u is shown in Fig. 7. Fig. 8 shows a time-response of the encrypted output $\overline{y}$. In this case, athough relatively large quantization errors can be seen in the control input response of Fig. 7(b), the output signal monitored inside the controller device is similarly scrambled, comparing with the output response of Fig. 7(a). Moreover, the ElGamal encryption is not deterministic so that the steady state looks hard to be identified.

Therefore, we can conclude that the encrypted controller proposed in this paper conceal the parameters and the signals processed inside the controller device.

3) Demonstration of confidence: In this section, we show that the encrypted controller is confidential and is able to prevent the malicious users, who performed the unauthorized access to the controller device, from stealing the information and dynamics in the control system. They are supposed to be able to record the encrypted signals, the encrypted reference $\mathsf{Enc}(k_p, \overline{0})$ and the encrypted output $\mathsf{Enc}(k_p, \overline{y})$, in order to get the dynamics by the subspace identification method, `n4sid` in Matlab. The result of the identification based on the encrypted signals available in the controller device is in Fig. 9. From the figure, in the both cases of RSA and ElGamal, the identified models are different from the true dynamics. Therefore, we can state that the proposed concept of the controller encryption is effective and useful for enhancing the cyber-security.



(a) Output

(b) Control

Fig. 7. Comparison of output $y(t)$ with and without the proposed cyber-security enhancement: ElGamal encryption.

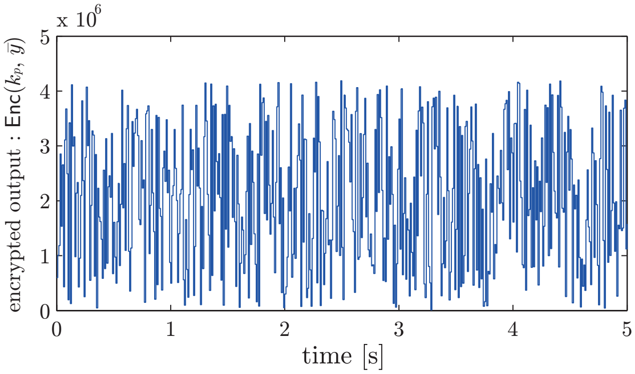


Fig. 8. A time-response of the controller's output encrypted by the ElGamal encryption, $\mathsf{Enc}\,(k_p, \overline{y}(t))$.

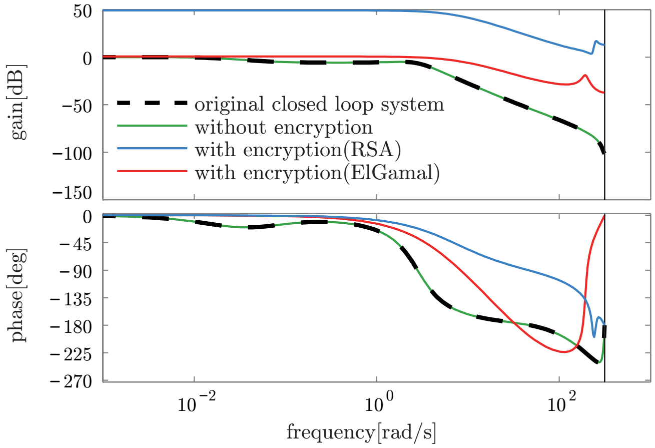


Fig. 9. Results of the subspace identification (`n4sid` in Matlab) using the normal or encrypted signals in the reference and the output.

V. Conclusion

In this paper, we proposed the novel concept of encrypting a linear controller using homomorphic encryptions of RSA and ElGamal schemes, and presented how to realize the encrypted controller with the modified encryption schemes. The most remarkable property of the concept is to encrypt the controller's parameters and the signals inside the controller device, and another property is also significant that the controller need not to keep any private keys for calculating the control input, which means that the decryption process is not required inside the controller. In the numerical example, furthermore, we showed that how the encrypted controller works in the networked controls system and that the encrypted controller functions to enhance the cyber-security, comparing with the conventional secure networked control system. Moreover, we found that the controller encryption problem is related to the quantized control problem with the cyclic group $\mathbb{G}$ that is an intermittent non-negative integer set. This motivates us to research a new quantized control problem as a future work. As well, we will perform experimental verification of the encrypted controller.

References

[1] H. Sandberg, S. Amin, and K. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.

[2] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 6294–6303, 2014.

[3] F. Pasqualetti and F. D. an F. Bullo, "Control-theoretic methods for cyberphysical security," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, 2015.

[4] A. Teixeira, K. Sou, H. Sandberg, and K. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, 2015.

[5] S. Amin, A. Cardenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control. Proc. 12th Intl. Conf., LNCS*, vol. 5469, 2009, pp. 31–45.

[6] Z. Pang, G. Zheng, G. Liu, and C. Luo, "Secure transmission mechanism for networked control systems under deception attacks," in *Proceedings of IEEE International Conference on Cyber Technology in Automation*, 2011, pp. 27–32.

[7] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947–1960, 2013.

[8] H. Zhou and G. Wornell, "Efficient homomorphic encryption on integer vectors and its applications," in *Proceedings of Information Theory and Applications*, 2014, pp. 1–9.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," *Communications of the ACM*, vol. 21, no. 2, Feb 1978.

[10] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO '84*, vol. 196, 1984, pp. 10–18.

[11] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2015.

[12] K. Huang and R. Tso, "A commutative encryption scheme based on elgamal encryption," in *Proceedings of International Conference on Information Security and Intelligence Control*, 2012, pp. 156–159.

[13] T. Katayama, *Subspace methods for system identification*. Springer, 2005.