IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 April 2023, accepted 5 May 2023, date of publication 9 May 2023, date of current version 15 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3274691

RESEARCH ARTICLE

Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption

MASAKI MIYAMOTO[1], (Graduate Student Member, IEEE), KAORU TERANISHI[1,2], (Graduate Student Member, IEEE), KEITA EMURA[3], AND KIMINAO KOGISO[1], (Member, IEEE)

[1]Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications (UEC), Chofu, Tokyo 1828585, Japan
[2]Japan Society for the Promotion of Science (JSPS), Chiyoda-ku, Tokyo 1020083, Japan
[3]Cybersecurity Research Institute, National Institute of Information and Communications Technology (NICT), Koganei, Tokyo 1848795, Japan

Corresponding author: Kiminao Kogiso (kogiso@uec.ac.jp)

This work was supported by the Japan Society for the Promotion of Science KAKENHI under Grant JP22H01509 and Grant JP21K11897.

ABSTRACT Encrypted control systems are secure control methods that use the cryptographic properties of a specific homomorphic encryption scheme. This study proposes a cyberattack-detectable encrypted control system and validates its effectiveness using a proportional integration derivative (PID) position-control system for an industrial motor. The proposed encrypted control system uses a keyed-homomorphic public-key encryption scheme for real-time detection of cyberattacks, such as signal and control parameter falsification. Additionally, a novel quantizer is presented to reduce the computation cost and quantization-error effects on control performance. The quantizer demonstrated a significant improvement, reducing the computation time by 47.3 % compared to using our previous quantizer, and decreasing the quantization-error effect by 30.6 % compared to a widely-used gain-multiplying quantizer. Moreover, this study establishes conditions through a theorem to avoid an overflow in the proposed control system. Experimental validation confirms that the proposed control system effectively conceals the control operation, and the presented theorem aids in designing the quantization gains to prevent overflows. Notably, the results of falsification attack tests highlight that the proposed control system enables real-time detection of attacked components within control parameters and signals, representing a significant advantage of this study.

INDEX TERMS Cybersecurity, encrypted control, keyed-homomorphic public key encryption, quantization, experimental validation.

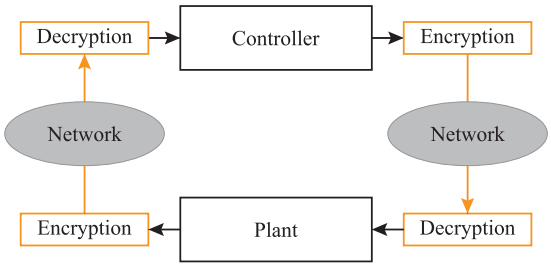
I. INTRODUCTION

Cybersecurity is important in networked control systems. Networked control systems are connected to information networks used in factory automation and power grids for supporting modern life. However, being connected to an information network entails the risk of a cyberattack on the control system. Furthermore, unlike in the case of conventional information technology systems, cyberattacks on control systems can cause physical damage. Stuxnet destroyed centrifuges at an Iranian nuclear facility [1], and Industroyer caused massive power outages in Ukraine [2].

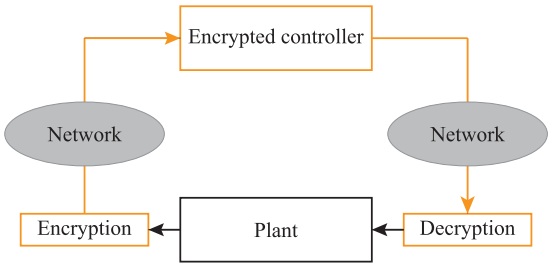
The associate editor coordinating the review of this manuscript and approving it for publication was Hosam El-Ocla.

Various techniques that are used to attack control systems and several main attacks [3], [4], [5], [6] are classified based on the impact and adversary's knowledge of the control system [7]. Eavesdropping attacks are the easiest to execute because they do not require any model knowledge of the target control system, but they lead to more sophisticated attacks [8]. However, cryptography can prevent eavesdropping attacks; thus, it increases the security of control systems.

From both control-theoretic and cryptographic viewpoints, a multidisciplinary method can develop a cyber-secure automatic control technology. Homomorphic encryption (HE) [9] enables arithmetic operations on encrypted data. The method of incorporating homomorphic encryption into a control system is known as encrypted control [10], [11],



(a) Traditional (unencrypted) control system.



(b) Encrypted control system.

FIGURE 1. Conceptual configuration of encrypted control systems.

[12], [13]. As shown in Fig. 1(a), networked control systems communicate control-system signals over a network. For cloud-based control systems, which have attracted attention in recent years, computations of the controller are performed in the cloud. In contrast, as shown in Fig. 1(b), an encrypted control system directly determines the control inputs in ciphertext without decrypting the signals. Hence, it has attracted considerable attention because it can reduce the risk of raw data leakage even if an attacker accesses the control network through cyberspace.

A. OUR CONTRIBUTIONS

The objective of this study is to propose an encrypted control system based on a keyed-homomorphic public-key encryption (KH-PKE) scheme that enables the detection of the malleability-based falsification of signals and control parameters. To enhance security, this study considers controller encryption using the KH-PKE scheme [14]. The falsification attack detection is inherited from the feature that allows the decryption and evaluation algorithms of the underlying KH-PKE scheme to output an error symbol when tampering occurs. The proposed encrypted control system benefits from the feature that enables the identification of attacked components within signals and control parameters, which constitutes a significant advantage over the conventional studies [10], [11], [12], [13], [15], [16], [17], [18], [19], [20], [21]. Moreover, a novel efficient quantizer is presented for constructing the encrypted control system, which is developed by modifying a conventional quantizer [16]. The efficient quantizer introduced in this study significantly improves the performance by reducing computation time, as compared to conventional quantizers [16]. Furthermore, this study investigates the conditions for avoiding overflows caused by quantization processes, which is summarized in a theorem. In addition, an experimental validation was conducted to confirm the effectiveness of the proposed encrypted control system using an industrial linear stage. First, this study evaluates three encrypted control systems with a modified quantizer and two conventional quantizers [10], [16] in terms of computation time and quantization-error effects on control performance, and the encryption scheme used is KH-PKE and common. Subsequently, this study verifies the theorem that provides a design policy for quantization gains, compared with the situation where quantization gains do not hold for the theorem. The final validation demonstrates that the proposed encrypted control system enables the real-time detection of falsification attacks. These experimental results indicate that the proposed encrypted control system is adequate and appropriate for developing secure control technologies.

The contributions of this study are threefold. i) This study developed a more secure encrypted control system that enables the real-time detection of cyberattacks compared with conventional encrypted control systems. This implies that there is expertise and knowledge in cryptography that helps enhance the security of control systems. ii) The developed linear-stage control system is a secure automatic control technology, and the proposed method can be implemented and can run in real-time with a certain key length. iii) This study provides the possibility and relevance of appropriate security concepts for real-time control systems in terms of provable and computational security. The findings of this study will lead to the creation of a new fusion area for cryptography and control engineering.

B. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows: Section II introduces the notations and syntax of the KH-PKE scheme. Section III presents the proposed encrypted control system that involves a novel quantizer. Section IV introduces a practical testbed control system and determines the parameters for implementing an encrypted controller. Section V validates the proposed encrypted control system in terms of the control performance effect, overflow avoidance, and cyberattack detection. Section VI discusses the security of the proposed encrypted control system. Finally, Section VII concludes the paper.

C. RELATED WORK

Encrypted control systems using Paillier encryption [22], which is an additive homomorphic encryption (AHE) that enables the addition of encrypted data, have been studied [11], [17], [18], [19]. Encrypted control systems using ElGamal encryption [23], which is a multiplicative homomorphic encryption (MHE) that enables the multiplication of encrypted data, have also been studied [10], [15], [16]. Furthermore, encrypted control systems using fully homomorphic encryption (FHE) [24], which can perform both addition and multiplication, have been proposed [12]. Some recent studies have considered encrypted control systems using AHE or leveled FHE based on learning with errors [20], [21]. Only the signal of the control system is encrypted when using AHE, whereas MHE and FHE enable the encryption of signals and controller parameters.

Countermeasures against cyberattacks such as tampering, are necessary to secure control systems. Although eavesdropping attacks can be prevented, the direct manipulation of signals or controller parameters enables the degradation of control performance or compromises it to break in the worst case. Encrypted control systems are vulnerable to attacks that use the malleability of the homomorphic encryption scheme [25], which means an attacker can manipulate encrypted signals and parameters to adjust controlled outputs without decrypting them. To reduce the vulnerability to attacks, there are related studies that consider countermeasures such as homomorphic authentication [26], obfuscation of controller parameters [25], and cancellation and detection by a modified somewhat homomorphic encryption [27], [28], which uses the malleability of a homomorphic encryption scheme. However, these studies could hardly identify an attacked component within signals and control parameters. The enhancement of cyberattack detection motivated us to develop a secure control technology for a quick response to cyberattack incidents.

The concept of KH-PKE, as proposed in [14] and [29], introduces another private key specifically dedicated to performing homomorphic operations. This approach aims to achieve indistinguishability under an adaptive chosen ciphertext attack (IND-CCA2) against adversaries who do not possess a homomorphic operation key. The IND-CCA2 security property enables the detection of attacks based on malleability, and various configurations of KH-PKE have been proposed in [14], [29], [30], [31], [32], [33], and [34]. Furthermore, a study has also proposed a KH-PKE scheme that supports multiplicative homomorphic operations [14]. Notably, the KH-PKE scheme is secure under the decisional Diffie-Hellman (DDH) assumption, which is commonly used to prove the security of ElGamal encryption. As a result, the use of DDH-based KH-PKE scheme is expected to enhance the security of encrypted control systems, making them more resillient against potentail cyberattacks.

II. PRELIMINARIES

This section provides notations of variables and functions and introduces the KH-PKE as preliminaries for constructing encrypted control systems.

A. NOTATIONS

Sets of real numbers, integers, plaintext spaces, and ciphertext spaces are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathcal{M}$, $\mathcal{C}$, respectively. We define $\mathbb{R}^+ := \{x \in \mathbb{R} \mid 0 < x\}$, $\mathbb{Z}^+ := \{z \in \mathbb{Z} \mid 0 < z\}$, $\mathbb{Z}_n := \{z \in \mathbb{Z} \mid 0 \leq z < n\}$, $\mathbb{Z}_n^+ := \{z \in \mathbb{Z} \mid 0 < z < n\}$, and $\mathfrak{P}_a^b := \{a^i \bmod b \mid i \in \mathbb{Z}_b\}$. A set of vectors of size n is denoted by $\mathbb{R}^n$. The jth element of vector v is denoted by v_j. ℓ_2 norm and infinity norm v are denoted by $||v||$ and $||v||_\infty$, respectively. The set of matrices of size $m \times n$ is denoted by $\mathbb{R}^{m\times n}$. (i, j) entry of matrix M is denoted by M_{ij}. The induced 2-norm and maximum norm of M are denoted by $||M||$ and $||M||_{\max}$, respectively. The greatest common divisor of the two positive integers $a, b \in \mathbb{Z}^+$ is denoted by $\gcd(a, b)$.

Definition 2.1: The minimal residue of integer $a \in \mathbb{Z}$ modulo $m \in \mathbb{Z}^+$ is defined as

$$a \operatorname{Mod} m := \begin{cases} b & \text{if } b < |b - m|, \\ b - m & \text{otherwise,} \end{cases}$$

where $b = a \bmod m$. For example, let $m = 10$, $a_1 = 3$, and $a_2 = 7$, then $a_1 \operatorname{Mod} m = 3$ and $a_2 \operatorname{Mod} m = -3$, where $a_1 \bmod m = 3$ and $a_2 \bmod m = 7$.

Definition 2.2: Let p be an odd prime number and z be an integer satisfying $\gcd(z, p) = 1$. If there exists integer b such that $b^2 = z \bmod p$, then integer z is the quadratic residue of modulo p. If integer b does not exist, then integer z is a quadratic nonresidue of modulo p. This can be expressed using the Legendre symbol $(\cdot/\cdot)_L$ as follows:

$$\left(\frac{z}{p}\right)_L := z^{\frac{p-1}{2}} \operatorname{Mod} p = \begin{cases} 1 & \text{if } z \text{ is a quadratic residue,} \\ -1 & \text{if } z \text{ is a quadratic nonresidue.} \end{cases}$$

Definition 2.3: The rounding function $\lceil \cdot \rfloor$ of $\sigma \in \mathbb{R}^+$ to the nearest positive integer is defined as

$$\lceil \sigma \rfloor = \begin{cases} \lfloor \sigma + 0.5 \rfloor & \text{if } \sigma \geq 0.5, \\ 1 & \text{otherwise,} \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

B. KEYED-HOMOMORPHIC PUBLIC KEY ENCRYPTION

The syntax of KH-PKE for homomorphic operations [14] is introduced as follows:

Definition 2.4 (KH-PKE): Let $\odot$ be a binary operation over $\mathcal{M}$. The KH-PKE scheme $\mathcal{E} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}, \mathbf{Eval})$ for homomorphic operation $\odot$ consists of the following four algorithms:

- **Gen**: This key-generation algorithm takes a security parameter $\kappa \in \mathbb{R}^+$ as the input and returns public key $\mathbf{pk}$, private key $\mathbf{sk_d}$, and homomorphic operation key $\mathbf{sk_h}$;
- **Enc**: This encryption algorithm takes $\mathbf{pk}$ and plaintext $m \in \mathcal{M}$ as the input and returns ciphertext $c \in \mathcal{C}$;
- **Dec**: This decryption algorithm takes $\mathbf{sk_d}$ and c as inputs and returns m or $\perp$.
- **Eval**: This evaluation algorithm takes $\mathbf{sk_h}$, two ciphertexts c_1 and c_2 as inputs and returns ciphertexts c or $\perp$,

where $\perp$ denotes the error symbol.

Definition 2.5 (Correctness): A KH-PKE scheme for homomorphic operation $\odot$ is correct if, for all $(\mathbf{pk}, \mathbf{sk_d}, \mathbf{sk_h}) \leftarrow \mathbf{Gen}(\mathbf{1}^\kappa)$, the following two conditions are satisfied:

1) For all $m \in \mathcal{M}$ and $c \in \mathcal{C}_{\mathbf{pk},m}$, it holds that $\mathbf{Dec}(\mathbf{sk_d}, c) = m$;
2) For all $m_1, m_2 \in \mathcal{M}$, $c_1 \in \mathcal{C}_{\mathbf{pk},m_1}$, and $c_2 \in \mathcal{C}_{\mathbf{pk},m_2}$, it holds that $\mathbf{Eval}(\mathbf{sk_h}, c_1, c_2) \in \mathcal{C}_{\mathbf{pk},m_1 \odot m_2}$,

where $\mathcal{C}_{\mathbf{pk},m}$ denotes the set of all ciphertexts of $m \in \mathcal{M}$ under the public key $\mathbf{pk}$. For simplicity, the arguments $\mathbf{pk}$, $\mathbf{sk_d}$, and $\mathbf{sk_h}$ will be omitted henceforth.

In this study, the multiplicative KH-PKE scheme proposed in [14] is used to encrypt communication signals and

control parameters. This security is provided by the DDH assumption. In the case of multiplicative DDH-based KH-PKE, $\odot$ is replaced with a multiplicative homomorphic operation, and the plaintext space is a multiplicative cyclic group, defined as $\mathbb{G} := \{g^i \bmod p \mid i \in \mathbb{Z}_q\}$ such that $g^q \bmod p = 1$ and $p-1 \bmod q = 0$ with generator g of cyclic group $\mathbb{G}$, which is a set of positive integers with discrete values. The four algorithms can be specified as **Appendix A**. Moreover, the DDH-based KH-PKE scheme enables the error symbol to be returned when processing ill-formed ciphertexts in the **Dec** and **Eval** algorithms. Therefore, the DDH-based KH-PKE scheme helps us realize encrypted control systems with real-time detection of tampered communication signals and/or control parameters.

Remark 2.6: The original definition of the KH-PKE scheme states that if tampering occurs, then the error symbol is output to terminate the algorithm. However, because control systems require availability, this study modifies the algorithm such that it outputs the corresponding signals and never terminates them even if tampering occurs.

III. ENCRYPTED CONTROL SYSTEM

This section presents an appropriate quantizer for the proposed encrypted control systems, introduces the controller encryption technique, and explains the quantizer design policy to avoid overflows.

A. QUANTIZER

A quantizer is required to construct the encryption control system because the plaintexts and ciphertexts in the encryption scheme are integers, and the processes at the controller are reconstructed using the encryption scheme. Hence, this study presents a novel quantizer that maps $x \in \mathbb{R}$ onto $\bar{x} := (\bar{x}^1, \bar{x}^2) \in \mathbb{G}^2$, an encoding map $\mathsf{Ecd}_\gamma := \mathscr{C} \circ \mathscr{A}_\gamma$, and a decoding map $\mathsf{Dcd}_\gamma := \mathscr{B}_\gamma \circ \mathscr{D}$ with

$$
\begin{aligned}
\mathscr{A}_\gamma &: \mathbb{R} \to \mathfrak{P}_2^q \times \mathbb{Z}_q^+, \\
&: x \mapsto \begin{cases} (1, \lceil \gamma |x| \rfloor \bmod q) & \text{if } x \geq 0, \\ (2, \lceil \gamma |x| \rfloor \bmod q) & \text{if } x < 0, \end{cases} \\
\mathscr{B}_\gamma &: \mathfrak{P}_2^q \times \mathbb{Z}_q^+ \to \mathbb{R}, \\
&: (\zeta, z) \mapsto \left(\frac{\zeta}{3}\right)_L \frac{z}{\gamma} := \check{x}, \\
\mathscr{C} &: \mathfrak{P}_2^q \times \mathbb{Z}_q^+ \to \mathbb{G}^2, \\
&: (\zeta, z) \mapsto \left(\left(\frac{\zeta}{p}\right)_L \zeta, \left(\frac{z}{p}\right)_L z\right) \bmod p := (\bar{x}^1, \bar{x}^2), \\
\mathscr{D} &: \mathbb{G}^2 \to \mathfrak{P}_2^q \times \mathbb{Z}_q^+, \\
&: (\bar{x}^1, \bar{x}^2) \mapsto (|\bar{x}^1 \operatorname{Mod} p|, |\bar{x}^2 \operatorname{Mod} p|),
\end{aligned}
$$

where $\gamma \in \mathbb{R}^+$ is the quantization gain, $\zeta \in \{1, 2\}$, and $z := \lceil \gamma |x| \rfloor \bmod q$. The relationship between the maps is shown in Fig. 2.

The presented quantizer comprising Ecd_γ and Dec_γ is a modified version of the conventional quantizer [16] and has the advantage of reducing computation time and resource consumption compared to the conventional quantizer. The conventional quantizer uses plaintext space $\mathbb{G}^3$ that assigns

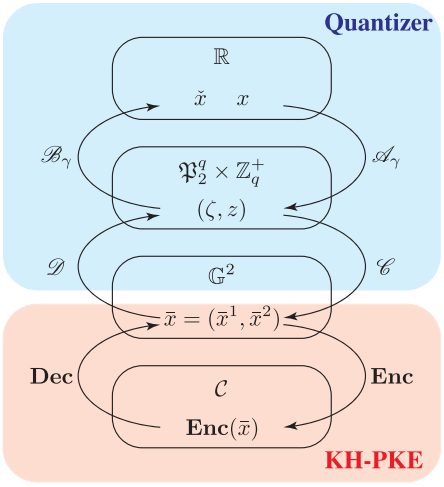


FIGURE 2. Relationship of the maps between the real and ciphertext spaces, realized by the presented $\mathbb{G}^2$-based quantizer.

$\mathbb{G}$ to a zero component. The assignment is inefficient in computing; therefore, the presented quantizer removes the zero component to obtain the plaintext space $\mathbb{G}^2$. In this study, the conventional quantizer is called a $\mathbb{G}^3$-based quantizer. In addition, the effects of the presented quantizer on the computation time are presented in Section IV-B. The proposed encrypted control system requires the plaintext space $\mathbb{G}^2$; therefore, the KH-PKE scheme must be conducted twice to encrypt data, as indicated in Fig. 2.

Remark 3.1: IND-CCA2 security holds against a KH-PKE ciphertext, and it does not imply IND-CCA2 security against two ciphertexts in a strict manner. In other words, the ciphertexts of $\bar{x}^1$ and $\bar{x}^2$ are non-malleable. However, if we consider that $(\mathbf{Enc}(\bar{x}^1), \mathbf{Enc}(\bar{x}^2))$ is a ciphertext, then it is malleable; for example, one can replace a component $\mathbf{Enc}(\bar{x}^1)$ (or $\mathbf{Enc}(\bar{x}^2)$) with other KH-PKE ciphertexts. In our system, this study does not consider such a replacement as tampering but considers element-wise tampering.

B. CONTROLLER ENCRYPTION

Let us consider a linear controller in a discrete-time state-space representation $f : \mathbb{R}^n \times \mathbb{R}^l \to \mathbb{R}^n \times \mathbb{R}^m$,

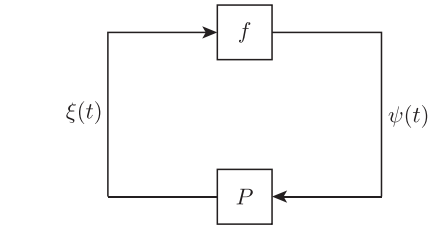
$$
f : \begin{cases} x_c(t+1) = A_c x_c(t) + B_c v_c(t), \\ u(t) = C_c x_c(t) + D_c v_c(t), \end{cases} \tag{1}
$$

where $t \in \mathbb{Z}^+$ is the time step, $u \in \mathbb{R}^m$ is the control input, $v_c \in \mathbb{R}^l$ is the measured output, $x_c \in \mathbb{R}^n$ is a controller state, and A_c, B_c, C_c, and D_c are controller parameters. Controller (1) can be rewritten as follows:

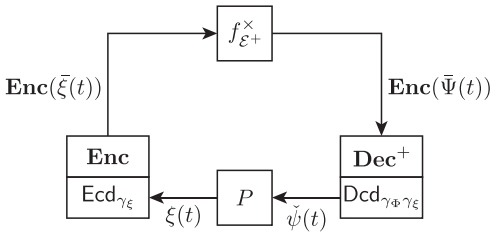
$$
\psi(t) = \Phi \xi(t) =: f(\Phi, \xi(t)), \tag{2}
$$

where $\Phi \in \mathbb{R}^{\alpha \times \beta}$ denotes a matrix that collects the control parameters, and $\psi \in \mathbb{R}^\alpha$ and $\xi \in \mathbb{R}^\beta$ denote a vector gathering the arguments and computed variables in the controller, respectively, which are written as follows:

$$
\Phi := \begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix}, \psi(t) := \begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix}, \xi(t) := \begin{bmatrix} x_c(t) \\ v_c(t) \end{bmatrix}, \tag{3}
$$



(a) Unencrypted control system.



(b) Encrypted control system using the KH-PKE scheme.

FIGURE 3. Block diagrams of feedback control systems before and after the controller encryption.

where $\alpha = n+m$ and $\beta = n+l$. The control system is shown in Fig. 3(a).

Because f is a composition product of multiplication $f^{\times}$ and addition f^{+}, the decryption algorithm is modified to yield $\mathbf{Dec}^{+} = f^{+} \circ \mathbf{Dec}$ [10]. Using the modified homomorphic encryption scheme $\mathcal{E}^{+} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}^{+}, \mathbf{Eval})$, the linear controller (1) can be encrypted, that is, it can be reconstructed into a different representation consisting of only encrypted parameters and signals. Then, the resulting encrypted controller when using $\mathcal{E}^{+}$ forms, $\forall t \in \mathbb{Z}^{+}$,

$$f^{\times}_{\mathcal{E}^+} : (\mathbf{Enc}(\bar{\Phi}), \mathbf{Enc}(\bar{\xi}(t))) \mapsto \mathbf{Enc}(\bar{\Psi}(t)), \tag{4}$$

where $\bar{\Phi} = \mathsf{Ecd}_{\gamma_\Phi}(\Phi)$, $\bar{\xi} = \mathsf{Ecd}_{\gamma_\xi}(\xi)$, $\bar{\Psi} = \mathsf{Ecd}_{\gamma_\Phi\gamma_\xi}(f^{\times}(\Phi, \xi))$, γ_Φ and γ_ξ are quantization gains regarding Φ and ξ, respectively, and $\mathbf{Enc}(\bar{\Psi}(t))$ is calculated using **Eval** as follows, $\forall t \in \mathbb{Z}^{+}$,

$$\mathbf{Enc}(\bar{\Psi}^{\theta}_{ij}(t)) = \mathbf{Eval}(\mathbf{Enc}(\bar{\Phi}^{\theta}_{ij}), \mathbf{Enc}(\bar{\xi}^{\theta}_{j}(t)), \\ \forall \theta \in \{1, 2\}, \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}.$$

The process (4) is a ciphertext version of (1); therefore, function f running in the controller is replaced by $f^{\times}_{\mathcal{E}^+}$, and the controller output $\mathbf{Enc}(\bar{\Psi}(t))$ is decrypted and decoded at the plant side to extract control input u via a signal $\check{\psi} = \mathsf{Dcd}_{\gamma_\Phi\gamma_\xi}(\mathbf{Dec}^{+}(\mathbf{Enc}(\bar{\Psi}(t))))$. The resulting encrypted control system is illustrated in Fig. 3(b).

The merits of using the KH-PKE scheme are as follows. The proposed encrypted control system can operate using encrypted Φ, ξ, and ψ. An index of vectors or matrices falsified by attackers can be identified because **Eval** and **Dec** are performed element-wise. Thus, controller encryption can protect the controller device and communication from cyberattacks, such as eavesdropping, and can also detect the falsification of signals and control parameters.

C. DESIGN POLICY OF QUANTIZATION GAIN

The plaintext space is finite; thus, overflows may occur with inappropriate gains. This study then provides the design policy of quantization gain as a theorem.

Definition 3.2: An overflow occurs when quantizing Φ, ξ, and a homomorphic operation if $\lceil \gamma_\Phi |\Phi_{ij}| \rfloor \geq q$, $\lceil \gamma_\xi |\xi_j| \rfloor \geq q$, and $\lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\Phi |\xi_j| \rfloor \geq q$ hold, respectively.

Theorem 3.3: Consider a discrete-time linear controller with input $\xi \in \mathbb{R}^{\beta}$ and coefficient matrix $\Phi \in \mathbb{R}^{\alpha \times \beta}$, where $\Phi_{\max} := ||\Phi||_{\max}$ is nonzero. For a given positive integer q, if there exists a quantization gain $\gamma_\Phi \in \mathbb{R}^{+}$ such that the following inequality condition:

$$\gamma_\Phi < \frac{1}{\Phi_{\max}} \left(q - \frac{1}{2} \right), \tag{5}$$

holds, and if there exists a quantization gain $\gamma_\xi \in \mathbb{R}^{+}$ and $||\xi(t)||_\infty < \infty, \forall t \in \mathbb{Z}^{+}$, such that the following inequality condition:

$$\gamma_\xi < \frac{1}{\gamma_\Phi \Phi_{\max} ||\xi(t)||_\infty} \left(q - \frac{1}{2} \right) \ \forall t \in \mathbb{Z}^{+}, \tag{6}$$

holds, then an overflow never occurs in the control operation using quantization gains γ_Φ and γ_ξ.

Proof: The inequality (5) is transformed into

$$q - \frac{1}{2} > \gamma_\Phi \Phi_{\max} \geq \gamma_\Phi |\Phi_{ij}|, \ \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}, \\ \Rightarrow \left\lceil q - \frac{1}{2} \right\rfloor = q > \lfloor \gamma_\Phi |\Phi_{ij}| \rfloor = \lceil \gamma_\Phi |\Phi_{ij}| \rfloor, \forall i, j, \tag{7}$$

which is the condition in which an overflow never occurs when quantizing Φ. Next, we define $\xi_{\max} := ||\xi(t)||_\infty$, $\forall t \in \mathbb{Z}^{+}$. The inequality (6) is transformed into

$$\begin{aligned} q - \frac{1}{2} &> \gamma_\Phi \Phi_{\max} \gamma_\xi \xi_{\max} \\ &\geq \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max}, \ \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}, \\ &\Rightarrow \left\lceil q - \frac{1}{2} \right\rfloor = q > \lfloor \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor \\ &= \lceil \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor, \forall i, j. \end{aligned} \tag{8}$$

When we choose $\xi_{\max}$ such that the following inequality $\lceil \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor \geq \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor$ is satisfied, the following inequality holds,

$$\begin{aligned} q &> \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor, \forall i, j, \\ &\Rightarrow q > \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor \geq \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi |\xi_j| \rfloor, \forall i, j, \\ &\Rightarrow q > \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi |\xi_j| \rfloor, \forall i, j, \end{aligned} \tag{9}$$

which implies that an overflow never occurs when quantizing the homomorphic operation. Furthermore, the inequalities (7) and (9) imply that an overflow never occurs when quantizing ξ. Therefore, the overflow avoidance conditions shown in **Definition 3.2** are derived. ■

Remark 3.4: The systematic computation of $\xi_{\max}$, which is needed to confirm the overflow avoidance conditions, is difficult. However, there is a situation where we can estimate it to some extent using the specifications of

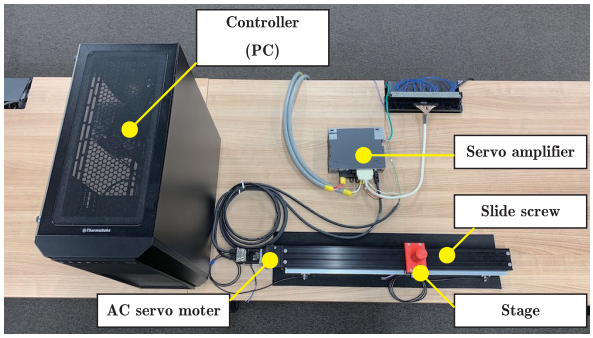


FIGURE 4. Experimental equipment.

TABLE 1. Experimental apparatus.

Servo amplifier	MITSUBISHI MR-J5-10A
Main circuit power supply	1/3-phase 200-240 VAC 50/60 Hz
AC servo motor	MITSUBISHI HK-KT13W
Rated power	0.1 kW
Rated torque	0.32 Nm
Rated speed	3000 rpm
Rated current	1.2 A
Pulse per rotation	67108864 ppr
Slide screw	MiSUMi LX3010CP-MX
Length	1250 mm
Lend	10 mm
PC	
CPU	Intel Core i7-10700K 3.80 GHz
Memory	64 GB
OS	CentOS Linux 8
Language	C++17
DA/AD board	Interface PEX-340216 (16-bit resolution)
Counter board	Interface PEX-632104 (32-bit resolution)

the control systems, such as the allowable position range of a linear stage. Section IV-B explains a method for estimating $\xi_{\max}$.

IV. IMPLEMENTATION

This section introduces a practical testbed control system and determines the parameters for implementing an encrypted controller in the control system.

A. PID POSITION CONTROL SYSTEM

We constructed a position-control system for the linear stage. Fig. 4 presents an overview of the stage position-control system. The actuator used to drive the stage via a slide screw (MiSUMi LX3010CP-MX) is an industrial AC servo motor (MITSUBISHI HK-KT13W) with a servo amplifier (MITSUBISHI MR-J5-10A). The controller device is a PC (Intel Core i7 and CentOS Linux 8), where a robot-control development tool, Advanced Robot Control System V6 (ARCS6) [35], was used for real-time control. The PC outputs a control input to the servo amplifier to actuate the AC servomotor. The position of the stage is measured by a rotary encoder installed in the motor unit and fed back to the PC via a counter board to update the control input. The processes run in the control algorithm are written as C++17. The apparatus and their specifications are listed in TABLE 1.

Throughout the experiments of the position control, we used a PID controller with proportional, integral, and derivative gains, K_p, K_i, and K_d, respectively. Defining the state and input of the controller as $x_c := \begin{bmatrix} e & w \end{bmatrix}^{\mathrm{T}}$ and $v_c := \begin{bmatrix} r & y \end{bmatrix}^{\mathrm{T}}$, respectively, the discrete-time state-space representation of the PID controller in (1) has the following matrices:

$$A_c = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, B_c = \begin{bmatrix} 1 & -1 \\ T_s & -T_s \end{bmatrix}, C_c = \begin{bmatrix} -\frac{K_d}{T_s} & K_i \end{bmatrix},$$
$$D_c = \begin{bmatrix} K_p + K_i T_s + \frac{K_d}{T_s} & -(K_p + K_i T_s + \frac{K_d}{T_s}) \end{bmatrix}, \quad (10)$$

where $r \in \mathbb{R}$ is a reference for the stage position, $y \in \mathbb{R}$ is the measured stage position, $e := r - y$ is the tracking error, and w is an integrated value defined as $w(t+1) := \sum_{\tau=0}^{t} e(\tau) T_s = w(t) + e(t) T_s$ with sampling period T_s. In this experiment, $K_p = 1.465 \times 10^{-2}$, $K_i = 6.000 \times 10^{-3}$, $K_d = 1.500 \times 10^{-4}$, and $T_s = 20$ ms. In this case, Φ is given as follows:

$$\Phi = \begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 1 & 0.02 & -0.02 \\ -0.0075 & 0.006 & 0.0223 & -0.0223 \end{bmatrix},$$

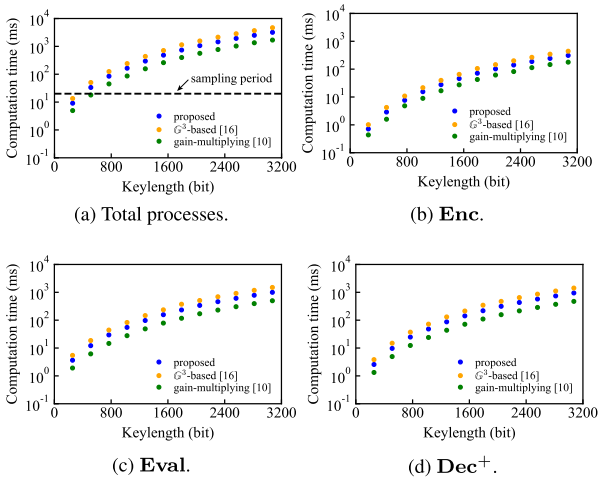
and ξ is defined by $\xi := \begin{bmatrix} e & w & r & y \end{bmatrix}^{\mathrm{T}}$, where $\alpha = 3$ and $\beta = 4$.

B. SECURE IMPLEMENTATION OF THE PID CONTROLLER

To encrypt the PID controller, we set the key length to 256 bits, which was determined by evaluating the computation time of the encrypted control processes, including **Enc**, **Eval**, and **Dec**$^+$ over key lengths. The averages of 100 computation times from 256 to 3072 bits for every 256 bits are shown in Fig. 5. Fig. 5(a) shows the total computation time of **Enc**, **Eval**, and **Dec**$^+$ of the encrypted controls using the proposed $\mathbb{G}^2$-based, $\mathbb{G}^3$-based [16], and gain-multiplying [10] quantizers, as shown in Figs. 5(b), (c), and (d), respectively. Table 2 presents the total computation time and its comparison to the proposed quantizer. The two conventional methods employed the DDH-based KH-PKE scheme, which is common in the method proposed in this study. The figure and table confirm that the computation time of the proposed encrypted control is 47.3 % lower than that of the control system with the $\mathbb{G}^3$-based quantizer, as mentioned in Section III-A. Although processing the control computation with the gain-multiplying quantizer is 45.6 % faster than with the proposed control, it tends to degrade the control performance, as shown in Section V-A. Furthermore, the computation at key length $\ell = 256$ must be completed within a sampling period of 20 ms; therefore, the presented faster quantizer is preferred to the $\mathbb{G}^3$-based quantizer.

We determine γ_Φ and γ_ξ using **Theorem 3.3**. First, we set γ_Φ to 1.0×10^{20} from the inequality (5) of $\gamma_\Phi < 4.3 \times 10^{76}$, with $||\Phi||_{\max} = 1$ and

$$q = 436330242283591462479179208760550548662 \times 291077161756781216195899944211526105 93,$$
$$\approx 4.3 \times 10^{76}.$$



(a) Total processes. (b) **Enc**. (c) **Eval**. (d) $\mathbf{Dec}^+$.

FIGURE 5. Computation time of each process over the key length.

Next, we estimate $||\xi(t)||_\infty$ over a step; that is, we estimate the maximum error e, state w, reference r, and output y. When the length of the linear stage is 1250 mm, the maximum error is 1250 mm because of $e = r - y = 625 - (-625)$. w is given by $w(t+1) := \sum_{\tau=0}^{t} e(\tau)T_s = w(t) + e(t)T_s$. If $T_s = 0.02$ and the duration of this experiment is 10 s, then the maximum state is 1250. Subsequently, $||\xi(t)||_\infty$ can be set to 1250. Therefore, we set γ_ξ to 1.0×10^{53} from inequality (6) of $\gamma_\xi < 3.44 \times 10^{53}$.

Using KH-PKE with the parameters above, the controller gains Φ are encrypted and implemented on the PC. For example, $\mathbf{Enc}(\bar{\Phi}^1_{11})$, $\mathbf{Enc}(\bar{\Phi}^2_{31})$, and $\mathbf{Enc}(\bar{\Phi}^2_{32})$ are (11), as shown at the bottom of the page.

V. EXPERIMENTAL VALIDATION

This section validates the three attributes of the proposed encrypted control system, namely, the control-performance effect, overflow avoidance, and cyberattack detection, compared with the unencrypted control (10) and the two conventional encrypted controls with a $\mathbb{G}^3$-based quantizer [16] and gain-multiplying quantizer [10]. The used encryption scheme, which is a DDH-based PH-PKE, is the same for the three encrypted control methods. In addition, the used control parameters are common, and the other parameters such as γ_Φ, γ_ξ, and ℓ are the same.

A. CONTROL RESULTS

We present the experimental results of position control using the proposed, conventional, and unencrypted controls with a step-like reference, which is given as follows:

$$\begin{cases} 0 & \text{if } 0 \le T_s t < 2 \text{ or } 8 \le T_s t < 10, \\ 50 & \text{if } 2 \le T_s t < 4 \text{ or } 6 \le T_s t < 8, \\ 100 & \text{if } 4 \le T_s t < 6, \end{cases} \tag{12}$$

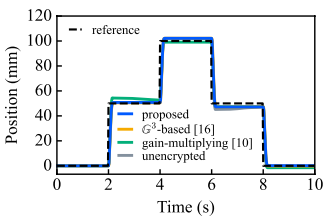
to examine the effects of the proposed secure implementation on a control system.

The control results are presented in Fig. 6. Figs. 6(a) and (b) show the time responses of the stage position and control input, respectively. In the figures, the blue, green, yellow, and gray lines represent the proposed, conventional [10], [16], and unencrypted control methods, respectively, where the broken line represents the reference. Fig. 6(c) shows three stage-position errors between each of the three encrypted controls and the unencrypted control, respectively, and Fig. 6(d) shows the three control input errors between the encrypted control and the unencrypted control. In Figs. 6(c) and (d), the blue line represents the proposed method, and green and yellow lines represent the two conventional methods. Figs. 6(e), (f), and (g) show the quantization error between the quantized and unquantized control inputs, that is, $|\check{u}(t) - u(t)|$, for the proposed method and the two conventional methods, respectively. Table 2 presents ℓ_1-norm values of the quantization-error signals for each quantizer up to 10 s. Figs. 6(h) and (i) show the time responses of the encrypted signals $\mathbf{Enc}(\Psi^1_{33}(t))$ and $\mathbf{Enc}(\xi^1_3(t))$, respectively, which correspond to parts of the output and input signals of the controller.

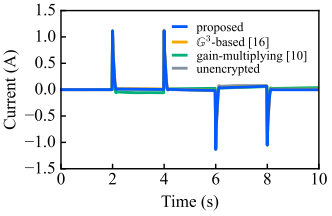
$$\mathbf{Enc}(\bar{\Phi}^1_{11}) = \begin{array}{l}\texttt{(ef99a26e99df01b7c50118dea8b8826fa169177f3c94333f6de844b7faa738a5,}\\ \texttt{f5e78a92d80b0a6ad503a8338905d373b6afae3b1615bdc6280bab18cac4571e,}\\ \texttt{da6e18939379d11f1fb6ca2a7350156adade88f55fac80ecad62b142fe34bd72,}\\ \texttt{4fe15d197c003ee86ee3a35404a8c7cde1e1c1f12a43d963c1d1e2d5f20d5a98,}\\ \texttt{b386194f8a1f016ffc6afdd8469630f7d242db11e5ff6332471048ab8ff7c7f),}\end{array} \tag{11a}$$

$$\mathbf{Enc}(\bar{\Phi}^2_{31}) = \begin{array}{l}\texttt{(c350361fb7d41633662736edb5028dba4cc7ae4d4189d75778aa73c357f2f9d0,}\\ \texttt{73bd85f730994868b02ee2512272c96452aca1575f0317c1ef32de3840c527df,}\\ \texttt{941863c7e67f6ec4f48ba7cdcb04f2da1c1871442da5daaf8e69f88987243546,}\\ \texttt{179a00c5a06fc763972cc5254bdf7beb9d8e4d3057391b679a23dc072c2e3114,}\\ \texttt{112f5a3adc5bdf4d4509195e4c97879328dd158ddee5899c978ba0defb7034b8),}\end{array} \tag{11b}$$

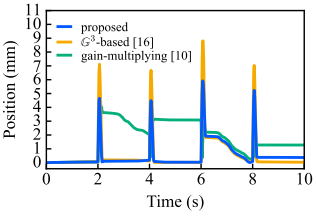
$$\mathbf{Enc}(\bar{\Phi}^2_{32}) = \begin{array}{l}\texttt{(eb6906386c2e66dbfa88403f3297ca0356c28b00e9ac6dbd1db81caffa4a7312,}\\ \texttt{ee15995c854fb987ee47338a31f4dce480635e2e75123d03dc1370b29f204abd,}\\ \texttt{e434b267068ca03fde81d39dd1644f466c8588dc91e1bae366d0591add6d5c09,}\\ \texttt{d9d89949da579ecb3b662c434575425470fffcf1e19c52f34bd9d11b36c35e65,}\\ \texttt{a4cf383732d68e30a05a96398a3dd3fdda246b08a8786c0cd4be46cfdcdcf866).}\end{array} \tag{11c}$$



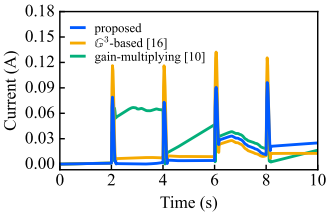
(a) Controlled output: $y(t)$.



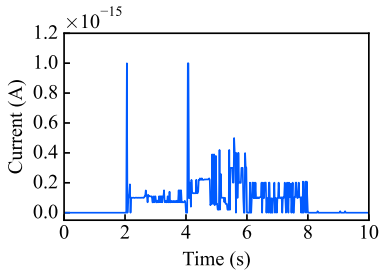
(b) Control input: $u(t)$.



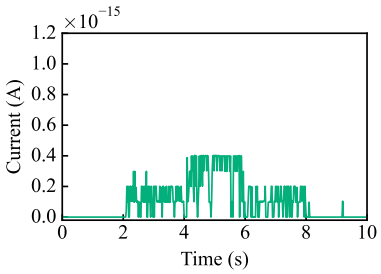
(c) Deviation from the output of the unencrypted control system.



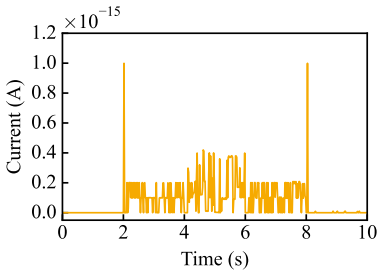
(d) Deviation from the control input of the unencrypted control system.



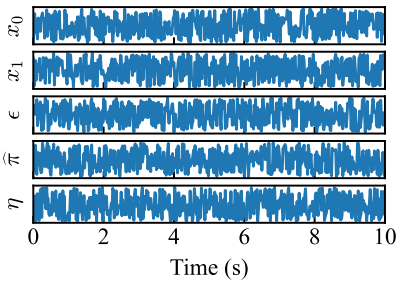
(e) Quantization error in u of the proposed $\mathbb{G}^2$-based quantizer.



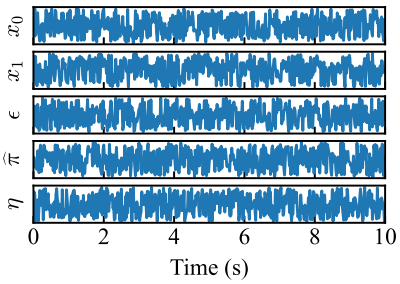
(f) Quantization error in u of the conventional gain-multiplying quantizer.



(g) Quantization error in u of the conventional $\mathbb{G}^3$-based quantizer.



(h) $\mathbf{Enc}(\Psi_{33}^1(t))$.



(i) $\mathbf{Enc}(\xi_3^1(t))$.

FIGURE 6. Experimental results of the four control methods: the KH-PKE-based encrypted control systems with the proposed $\mathbb{G}^2$-based quntizer, the conventional gain-multiplying [10] and $\mathbb{G}^3$-based [16] quantizers, and the unencrypted PID control system (10). The parameters $\ell = 256$, $\gamma_\Phi = 10^{20}$, and $\gamma_\xi = 10^{53}$ are the same for the proposed and conventional encrypted controls.

Figs. 6(c) and (d) confirm that the proposed control system achieves less deviation from the conventional method using the gain-multiplying quantizer. As shown in Table 2, the ℓ_1-norm values of the quantization-error signals in Figs. 6(e), (f), and (g) are 3.880×10^{-14}, 5.074×10^{-14}, and 3.856×10^{-14}, respectively. These scores demonstrate that the modification of the plaintext space from $\mathbb{G}^3$ to $\mathbb{G}^2$ has minimal impact on the quantization error, resulting in only a 0.6 % difference in the resulting control signals. The proposed control system achieves a 30.6 % improvement compared to the gain-multiplying quantizer. Furthermore, the parameters of (11) and signals shown in Figs. 6(h) and (i) were concealed in random numbers. The norm scores imply that the proposed control system is better than conventional systems in terms of control performance degradation and that they are negligibly small from the viewpoint of using variables in the C++ language.

Therefore, the control experimental results confirm that the proposed encrypted control system has a smaller impact on the control performance than the conventional encrypted control systems.

B. OVERFLOW AVOIDANCE

This section shows that **Theorem 3.3** helps us choose the appropriate values of γ_Φ and γ_ξ to avoid overflows in the control operation. Overflow avoidance is validated by showing another control result of the proposed encrypted control with inappropriate values, such as $\gamma_\Phi = 1.0 \times 10^{20}$ and $\gamma_\xi = 1.0 \times 10^{57}$, which do not satisfy the inequality in (6).

The control results for this case are shown in Fig. 7. Figs. 7(a) and (b) show the stage position and the control input, respectively, using the blue line. In this case, an overflow occurred between 2.00 s and 8.16 s, highlighted in yellow. The figures confirm that the control input was too small for the stage to follow the reference. This is because of the large γ_ξ, such that the term $\lceil \gamma |x| \rfloor$ of $\mathscr{A}_\gamma$ is greater than q in encoding, which implies an overflow. Therefore, the control result confirms that **Theorem 3.3** facilitates the desig of parameter values to avoid overflow.

Remark 5.1: If a systematic method of designing parameters is established, $||\xi(t)||_\infty$ must be estimated before starting the control operation or a dynamic quantizer related to γ_ξ using the observation of $\xi(t)$ [36], [37]. The estimation may

TABLE 2. Performance comparison of computation time and quantization error in the experimental results.

Encrypted control system with	Computation time (ms) at a 256-bit key length	Rate to the proposed quantizer (%)	Evaluation of quantization error	Rate to the proposed quantizer (%)
the proposed quantizer	9.12	100	3.880×10^{-14}	100
the $\mathbb{G}^3$-based quantizer [16]	13.43	147.3	3.856×10^{-14}	99.4
the gain-multiplying quantizer [10]	4.96	54.4	5.074×10^{-14}	130.6

be discussed using the equipment properties as stated in Section IV-B, while the dynamic quantizer design requires a different problem setting and further discussion; therefore, the systematic parameter design will be addressed in our future study.

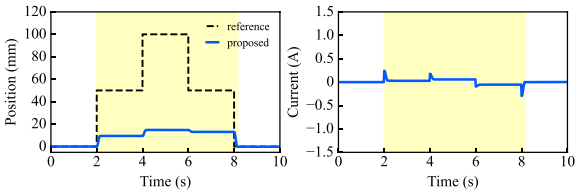
C. ATTACK DETECTION

It is demonstrated that the proposed encrypted control system enables the detection of malleability-based cyberattacks. An attacker does not know the homomorphic operation key $\mathbf{sk_h}$ for **Eval**; therefore, they tamper with the third element of the ciphertext using a constant factor. Because the homomorphic encryption scheme yields malleability, the attacker can obtain the desired decryption result by falsifying the ciphertext [25]. In KH-PKE, the last element of the **Dec** algorithm is $m = \epsilon/\pi \bmod p$, which means, if the third element e of the ciphertext is multiplied by $\lambda \in \mathbb{G}$, the decryption result is λ-fold. Therefore, even if the attackers do not know $\mathbf{sk_h}$, they can tamper with the data.

We consider two cyberattacks in this test: One falsifies an encrypted signal, double $\mathbf{Enc}(\bar{\xi}_4^2(t))$ in 4.0 s to 4.1 s, and the other falsifies two components of the control parameter triple $\mathbf{Enc}(\bar{\Phi}_{31}^2)$ and $\mathbf{Enc}(\bar{\Phi}_{32}^2)$ at 4.0 s, respectively. This means that the cyberattack doubles the signal or triples the two components of the parameter matrix.

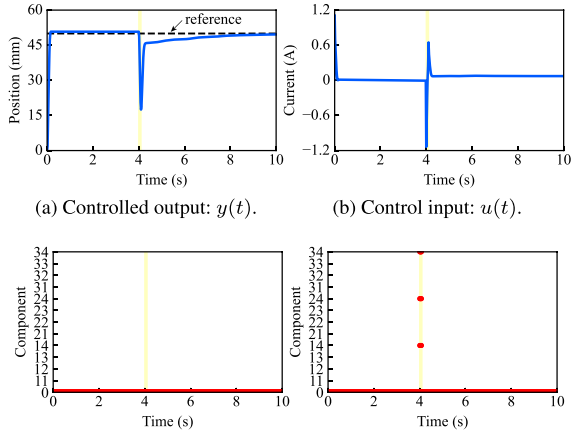
The cyberattack test results for falsifying a signal are shown in Fig. 8. Figs. 8(a) and (b) show the stage position and the control input, respectively. Figs. 8(c) and (d) show the error symbols for $\mathbf{Enc}(\bar{\Psi}^1)$ and $\mathbf{Enc}(\bar{\Psi}^2)$ in **Eval**, respectively. Fig. 8(a) shows that falsification of the sensor values caused spike-like changes in the stage position, indicating that tampering with the sensor values can destroy the control system. For such a falsification attack, the falsification time is confirmed from the error symbol, as shown in Fig. 8(c) and (d). Moreover, the indices of $\mathbf{Enc}(\bar{\Psi}_{14}^2)$, $\mathbf{Enc}(\bar{\Psi}_{24}^2)$, and $\mathbf{Enc}(\bar{\Psi}_{34}^2)$, which were calculated with the attacked signal $\mathbf{Enc}(\bar{\xi}_4^2)$ between 4.0 s and 4.1 s, can be identified.

The cyberattack test results for falsifying the two components in the control parameter are shown in Fig. 9. Figs. 9(a) and (b) show the stage positions of the stage and control input, respectively. Figs. 9(c) and (d) show the error symbols for $\mathbf{Enc}(\bar{\Psi}^1)$ and $\mathbf{Enc}(\bar{\Psi}^2)$ in **Eval**, respectively. Fig. 9(a) shows that the stage position was gradually shifted by falsifying the controller parameters. Fig. 9(b) shows that the falsification effect is not significantly reflected in the control input, which confirms that it is difficult to detect an attack using the threshold method [38]. For the falsification attack, the falsification time was confirmed using the error symbol, as shown in Figs. 9(c) and (d). The indices of the attacked signals $\mathbf{Enc}(\Phi_{31}^2)$ and $\mathbf{Enc}(\Phi_{32}^2)$ could be detected.



(a) Controlled output: $y(t)$. (b) Control input: $u(t)$.

FIGURE 7. Experimental results of the proposed encrypted PID control method. The used parameters are $\gamma_\Phi = 10^{20}$ and $\gamma_\xi = 10^{57}$, which do not satisfy the inequality condition (6).



(a) Controlled output: $y(t)$. (b) Control input: $u(t)$.

(c) Error symbol for $\mathbf{Enc}(\bar{\Psi}^1)$. (d) Error symbol for $\mathbf{Enc}(\bar{\Psi}^2)$.

FIGURE 8. Experimental result of the cyberattack performed by tampering with signals between 4.0 and 4.1 s against the proposed encrypted control system.

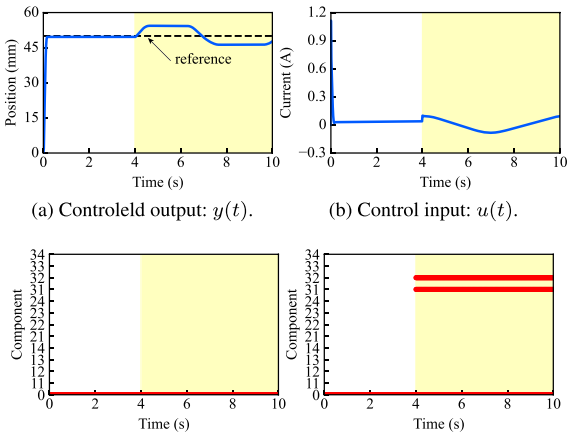
VI. DISCUSSIONS

Based on the results of this study, this section discusses two important issues for future work, to secure control systems.

A. EFFECTS OF A LEAKED HOMOMORPHIC OPERATION KEY

This study considered a situation in which the attacker never has a homomorphic operation key $\mathbf{sk_h}$ in tampering; however, it is also important to consider a situation in which a homomorphic operation key is leaked to a third party. Attackers may use a homomorphic operation to tamper with the ciphertexts in **Eval** to adjust the controlled outputs.

In this case, another detection mechanism is required because the algorithms **Eval** and **Dec** do not output error symbols for detection. One detection approach is to observe unencrypted control inputs from the perspective of a control



(a) Controleld output: $y(t)$. (b) Control input: $u(t)$.

(c) Error symbol for $\mathbf{Enc}(\bar{\Psi}^1)$. (d) Error symbol for $\mathbf{Enc}(\bar{\Psi}^2)$.

FIGURE 9. Experimental results of the cyberattack performed by tampering with control parameters within 4 s against the proposed encrypted control system.

theory, such as threshold-based detection methods [38], [39]. The other is to update the encryption keys in time from the perspective of cryptography, such as storing and replacing the keys periodically [40] and employing an updatable public-key ElGamal encryption scheme [36], [41]. The switching and updatable encryption schemes make it easy to detect falsification and replay attacks, which are difficult to detect in [4]. In this sense, an updatable KH-PKE scheme is expected to enhance the ability to detect cyberattacks on the control systems.

In addition, even if the homomorphic operation key is leaked, the proposed encrypted control system is more secure than an ElGamal-based encryption control system [10]. This is because the KH-PKE scheme retains stronger security than indistinguishability under chosen-ciphertext (IND-CCA1) security even when a key is leaked [14], where IND-CCA1 is the security that homomorphic encryption schemes can achieve [42]. Furthermore, because the controller parameters and signals remain encrypted, the control system is resistant to cyberattacks that require a model of the control system [6], [43].

B. APPROPRIATE SECURITY FOR CONTROL SYSTEMS

Implementing a key of several thousand bits in an encrypted control system with a real-time constraint is challenging, implying the control processes must be completed within a sampling period. The KH-PKE scheme is based on the DDH assumption, and from the viewpoint of cryptology, a key length that can assume the DDH-hardness is needed. Specifically, the NIST document [44] states that a key length of at least 2048 bits is desirable. However, the key length set used in this study was 256 bits to fulfill the real-time constraint under a sampling period of 20 ms, as shown in Fig. 5.

Currently, it is difficult to conclude whether the key length is satisfactory because the answer depends on the security concept we consider. An appropriate security concept exists for control systems, such as indistinguishability against parameter estimation attack (IND-PEA), proposed in [45], which is in provable security and revealed that IND-PEA is equal to indistinguishability under the chosen plaintext attack (IND-CPA). The updatable ElGamal-based encrypted control system [41], [46], which covers computational security, protects the controller parameters from being identified by attackers, even though the key length is shorter than that required by NIST. Furthermore, key updating ideas help solve real-time constraint issues. Such a security concept that is appropriate for control systems has recently been studied; therefore, appropriate security may exist for the 256-bits KH-PKE scheme. Exploring the appropriate security concept is significant for developing the control theory and cryptography fields, which will be explored in our future study. Additionally, in the sense of achieving IND-CCA1/2, the key length is insufficient because it is less than 2048 bits.

VII. CONCLUSION

This study proposed a cyberattack-detectable encrypted control system and validated its effectiveness using an industrial motor PID position-control system. The KH-PKE scheme was employed in the proposed control system for real-time cyberattack detection, and our novel quantizer was used to reduce computation time, as demonstrated by experiments that showed a 47.3 % reduction in computation time while maintaining similar quantization-error impact (with only a 0.6 % difference) compared to our previous quantizer. Furthermore, this study analyzed the conditions for overflow, which are summarized in **Theorem 3.3**. Experimental validations confirmed that the proposed control system concealed the control operation, and the results also confirmed that the theorem helps design quantization gains to avoid overflows. Importantly, this study demonstrated the results of falsification attack tests using homomorphism and confirmed that the proposed control system enables real-time detection of attacked components within signals and control parameters, which is a significant advantage.

Future studies will focus on the following areas. Firstly, the development of countermeasures against leaked homomorphic operation keys to potential attackers, as mentioned in Section VI. The homomorphic operation key is placed in the controller, which poses a risk of leakage to attackers who are interested in breaking into and compromising the control system. Secondly, ensuring the stability of the proposed encrypted control system. The stability of control systems is crucial for safe operation, but the proposed system requires a quantizer, which may destabilize the control system if not stabilized in advance. Finally, exploring security concepts appropriate for control systems and evaluating the security of the encrypted control system developed in this study.

APPENDIX A ALGORITHMS OF DDH-BASED KH-PKE SCHEME

This study uses KH-PKE with multiplicative homomorphism [14] to construct encrypted control systems. The KH-PKE scheme, denoted as $\mathcal{E} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}, \mathbf{Eval})$, consists of the following four algorithms.

Gen: $\kappa \mapsto (\mathbf{pk}, \mathbf{sk_d}, \mathbf{sk_h})$. The **Gen** algorithm takes security parameter κ and key length ℓ regarding ℓ-bit prime number p and outputs public, private, and homomorphic operation keys, denoted as $\mathbf{pk}$, $\mathbf{sk_d}$, and $\mathbf{sk_h}$, respectively:

$$\begin{aligned}\mathbf{pk} &= (g_0, g_1, s, \widehat{s}, \widetilde{s}_0, \widetilde{s}_1)\,,\\ \mathbf{sk_d} &= \left(k_0, k_1, \widehat{k}_0, \widehat{k}_1, \widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right),\\ \mathbf{sk_h} &= \left(\widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right),\end{aligned}$$

where g_0 and g_1 are randomly chosen from $\mathbb{G}$; $s := g_0^{k_0} g_1^{k_1} \bmod p$; $\widehat{s} := g_0^{\widehat{k}_0} g_1^{\widehat{k}_1} \bmod p$; $\widetilde{s}_0 := g_0^{\widetilde{k}_{0,0}} g_1^{\widetilde{k}_{0,1}} \bmod p$; $\widetilde{s}_1 := g_0^{\widetilde{k}_{1,0}} g_1^{\widetilde{k}_{1,1}} \bmod p$; k_0, k_1, $\widehat{k}_0$, $\widehat{k}_1$, $\widetilde{k}_{0,0}$, $\widetilde{k}_{0,1}$, $\widetilde{k}_{1,0}$, and $\widetilde{k}_{1,1}$ are randomly chosen from $\mathbb{Z}_q$, where $p = 2q + 1$.

Enc: $(\mathbf{pk}, m \in \mathcal{M}) \mapsto c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta) \in \mathcal{C}$. The **Enc** algorithm takes a public key $\mathbf{pk}$ and a plaintext m and outputs a ciphertext c. The components of c are as follows: $x_0 := g_0^{\omega} \bmod p$; $x_1 := g_1^{\omega} \bmod p$; $\epsilon := m\pi \bmod p$; $\widehat{\pi} := \widehat{s}^{\omega} \bmod p$, where $\pi := s^{\omega} \bmod p$ and ω is chosen randomly from $\mathbb{Z}_q$; $\eta := f_{hk}\left(\left(\widetilde{s}_0 \cdot \widetilde{s}_1^{\delta}\right)^{\omega} \bmod p\right)$ with $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$, where γ_{hk} is target collision resistance hash family and f_{hk} is a smooth function [14]. We use SHA-256 to both γ_{hk} and f_{hk}.

Dec: $(\mathbf{sk_d}, c \in \mathcal{C}) \mapsto m \in \mathcal{M} \cup \{\perp\}$. The **Dec** algorithm takes a private key and a ciphertext $c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta)$ and outputs a plaintext m or an error symbol $\perp$. Compute $\widehat{\pi}' := x_0^{\widehat{k}_0} x_1^{\widehat{k}_1} \bmod p$, $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$, and $\eta' := f_{hk}\left(x_0^{\widetilde{k}_{0,0}+\delta\widetilde{k}_{1,0}} x_1^{\widetilde{k}_{0,1}+\delta\widetilde{k}_{1,1}} \bmod p\right)$, where f_{hk} is a smooth function [14]. If either $\widehat{\pi} \neq \widehat{\pi}'$ or $\eta \neq \eta'$, then return an error symbol $\perp$; Otherwise, return $m = \epsilon/\pi \bmod p$, where $\pi := x_0^{k_0} x_1^{k_1} \bmod p$.

Eval: $(\mathbf{sk_h}, c_1, c_2 \in \mathcal{C}) \mapsto c \in \mathcal{C} \cup \{\perp\}$. The **Eval** algorithm takes a homomorphic operation key and two ciphertexts c_i $\forall i \in \{1, 2\}$ and outputs a ciphertext $(x_0, x_1, \epsilon, \widehat{\pi}, \eta)$ or an error symbol $\perp$. The components of the output c are computed as follows: $x_0 := x_{1,0} x_{2,0} g_0^{\omega} \bmod p$, $x_1 := x_{1,1} x_{2,1} g_1^{\omega} \bmod p$, $\epsilon := \epsilon_1 \epsilon_2 s^{\omega} \bmod p$, $\widehat{\pi} := \widehat{\pi}_1 \widehat{\pi}_2 \widehat{s}^{\omega} \bmod p$, and $\eta = f_{hk}\left(x_0^{\widetilde{k}_{0,0}+\delta\widetilde{k}_{1,0}} x_1^{\widetilde{k}_{0,1}+\delta\widetilde{k}_{1,1}} \bmod p\right)$, where $c_i := (x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i, \eta_i)$; $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$; $\delta_i := \gamma_{hk}\left(x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i\right)$; ω is randomly chosen from $\mathbb{Z}_q$; $\eta_i' := f_{hk}\left(x_{i,0}^{\widetilde{k}_{0,0}+\delta_i\widetilde{k}_{1,0}} x_{i,1}^{\widetilde{k}_{0,1}+\delta_i\widetilde{k}_{1,1}} \bmod p\right)$. If either $\eta_1 \neq \eta_1'$ or $\eta_2 \neq \eta_2'$, then return $\perp$; Otherwise, return c.

REFERENCES

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, p. 210, Feb. 2019.

[4] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[5] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[8] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 968–978.

[9] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surveys*, vol. 51, no. 4, pp. 1–35, Jul. 2019.

[10] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Proc. 54th IEEE Conf. Decis. Control (CDC)*, Dec. 2015, pp. 6836–6843.

[11] 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.

[12] 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.

[13] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Syst.*, vol. 41, no. 3, pp. 58–78, Jun. 2021.

[14] K. Emura, G. Hanaoka, K. Nuida, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen ciphertext secure keyed-homomorphic public-key cryptosystems," *Designs, Codes Cryptogr.*, vol. 86, no. 8, pp. 1623–1683, Aug. 2018.

[15] K. Teranishi, N. Shimada, and K. Kogiso, "Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems," *IET Control Theory Appl.*, vol. 14, no. 16, pp. 2242–2252, Nov. 2020.

[16] K. Teranishi and K. Kogiso, "ElGamal-type encryption for optimal dynamic quantizer in encrypted control systems," *SICE J. Control, Meas., Syst. Integr.*, vol. 14, no. 1, pp. 59–66, Jan. 2021.

[17] A. B. Alexandru, M. S. Darup, and G. J. Pappas, "Encrypted cooperative control revisited," in *Proc. IEEE Conf. Decis. Control*, Mar. 2019, pp. 7196–7202.

[18] N. Schluter and M. S. Darup, "Encrypted explicit MPC based on two-party computation and convex controller decomposition," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 5469–5476.

[19] M. Kishida, "Encrypted control system with quantizer," *IET Control Theory Appl.*, vol. 13, no. 1, pp. 146–151, 2019.

[20] R. Alisic, J. Kim, and H. Sandberg, "Model-free undetectable attacks on linear systems using LWE-based encryption," *IEEE Control Syst. Lett.*, vol. 7, pp. 1249–1254, 2023.

[21] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Trans. Autom. Control*, vol. 68, no. 2, pp. 660–672, Feb. 2023.

[22] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, vol. 5, 1999, pp. 223–238.

[23] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[24] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[25] K. Teranishi and K. Kogiso, "Control-theoretic approach to malleability cancellation by attacked signal normalization," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 297–302, 2019.

[26] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, "Need for controllers having integer coefficients in homomorphically encrypted dynamic system," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5020–5025.

[27] M. Fauser and P. Zhang, "Resilient homomorphic encryption scheme for cyber-physical systems," in *Proc. 60th IEEE Conf. Decis. Control (CDC)*, Dec. 2021, pp. 5634–5639.

[28] M. Fauser and P. Zhang, "Detection of cyber attacks in encrypted control systems," *IEEE Control Syst. Lett.*, vol. 6, pp. 2365–2370, 2022.

[29] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen ciphertext secure keyed-homomorphic public-key encryption," in *Proc. Int. Workshop Public Key Cryptography*. Cham, Switzerland: Springer, 2013, pp. 32–50.

[30] B. Libert, T. Peters, M. Joye, and M. Yung, "Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures," in *Proc. Adv. Cryptol. EUROCRYPT*, 2014, pp. 514–532.
[31] C. Jutla and A. Roy, "Dual-system simulation-soundness with applications to UC-PAKE and more," in *Proc. Adv. Cryptol. ASIACRYPT*, 2015, pp. 630–655.
[32] Y. Maeda and K. Nuida, "Chosen ciphertext secure keyed two-level homomorphic encryption," in *Proc. Inf. Secur. Privacy*, 2022, pp. 209–228.
[33] J. Lai, R. H. Deng, C. Ma, K. Sakurai, and J. Weng, "CCA-secure keyed-fully homomorphic encryption," in *Proc. Public-Key Cryptography (PKC)*, 2016, pp. 70–98.
[34] S. Sato, K. Emura, and A. Takayasu, "Keyed-fully homomorphic encryption without indistinguishability obfuscation," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 13269, G. Ateniese and D. Venturi, Eds. Cham, Switzerland: Springer, 2022, pp. 3–23.
[35] Y. Yokokura. *Side Warehouse of Laboratory*. Accessed: Apr. 19, 2023. [Online]. Available: https://www.sidewarehouse.net/arcs6/index.html
[36] K. Teranishi and K. Kogiso, "Dynamic quantizer for encrypted observer-based control," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 5477–5482.
[37] H. Kawase, K. Teranishi, and K. Kogiso, "Dynamic quantizer synthesis for encrypted state-feedback control systems with partially homomorphic encryption," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2022, pp. 75–81.
[38] B. Rikuna, K. Kogiso, and M. Kishida, "Detection method of controller falsification attacks against encrypted control system," in *Proc. SICE Annu. Conf.*, 2018, pp. 5032–5037.
[39] D. Martynova and P. Zhang, "An approach to encrypted fault detection of cyber-physical systems," in *Proc. Asian Control Conf.*, 2019, pp. 1501–1506.
[40] K. Kogiso, "Attack detection and prevention for encrypted control systems by application of switching-key management," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5032–5037.
[41] K. Teranishi, T. Sadamoto, A. Chakrabortty, and K. Kogiso, "Designing optimal key lengths and control laws for encrypted control systems based on sample identifying complexity and deciphering time," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2183–2198, Apr. 2023.
[42] R. Canetti, S. Raghuraman, S. Richelson, and V. Vaikuntanathan, "Chosen-ciphertext secure fully homomorphic encryption," in *Proc. Public Key Cryptography*. Cham, Switzerland: Springer, 2017, pp. 213–240.
[43] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 90–95, Jan. 2011.
[44] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 5)," Special Publication, NIST, Gaithersburg, MD, USA, Tech. Rep. 800–57, 2020.
[45] K. Teranishi and K. Kogiso, "Towards provably secure encrypted control using homomorphic encryption," in *Proc. IEEE 61st Conf. Decis. Control (CDC)*, Dec. 2022, pp. 7740–7745.
[46] K. Teranishi and K. Kogiso, "Optimal controller and security parameter for encrypted control systems under least squares identification," 2023, *arXiv:2302.12154*.

MASAKI MIYAMOTO (Graduate Student Member, IEEE) received the B.E. and M.E. degrees from The University of Electro Communications, Tokyo, Japan, in 2021 and 2023, respectively. His research interest includes encrypted controls.

KAORU TERANISHI (Graduate Student Member, IEEE) received the B.E. degree in electromechanical engineering from the National Institute of Technology, Ishikawa College, Ishikawa, Japan, in 2019, and the M.E. degree in mechanical and intelligent systems engineering from The University of Electro-Communications, Tokyo, Japan, in 2021, where he is currently pursuing the Ph.D. degree. From October 2019 to September 2020, he was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA. Since April 2021, he has been a Research Fellow with the Japan Society for the Promotion of Science. His research interests include control theory and cryptography for the cybersecurity of control systems.

KEITA EMURA received the M.E. degree from Kanazawa University, in 2004, and the Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST), in 2010. He was with Fujitsu Hokuriku Systems Ltd., from 2004 to 2006. He was a Postdoctoral Researcher with the Center for Highly Dependable Embedded Systems Technology, JAIST, from 2010 to 2012. He has been a Researcher with the National Institute of Information and Communications Technology (NICT), since 2012. Since 2014, he has been a Senior Researcher with NICT, where he has been a Research Manager, since 2021. His research interests include public-key cryptography and information security. He is a member of IEICE, IPSJ, and IACR. He was a recipient of the SCIS Innovation Paper Award from IEICE, in 2012, the CSS Best Paper Award from IPSJ, in 2016, the IPSJ Yamashita SIG Research Award, in 2017, and the Best Paper Award from ProvSec 2022.

KIMINAO KOGISO (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in mechanical engineering from Osaka University, Japan, in 1999, 2001, and 2004, respectively. He was appointed as a Postdoctoral Fellow with the 21st Century COE Program and as an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan, in April 2004 and July 2005, respectively. From November 2010 to December 2011, he was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA. In March 2014, he was promoted to the position of Associate Professor with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan, where he has been a Full Professor, since April 2023. His research interests include cybersecurity of control systems, constrained control, control of decision-makers, and their applications.