Malleability-Resistant Encrypted Control System with Disturbance Compensation and Real-Time Attack Detection

Naoki Aizawa, *Student Member, IEEE,* Keita Emura, and Kiminao Kogiso, *Member, IEEE*

***Abstract*—This study proposes an encrypted PID control system with a disturbance observer (DOB) using a keyed-homomorphic encryption (KHE) scheme, aiming to achieve control performance while providing resistance to malleability-based attacks. The controller integrates a DOB with a PID structure to compensate for modeling uncertainties by estimating and canceling external disturbances. To enhance security, the system is designed to output error symbols when ciphertexts are falsified during decryption or evaluation, enabling real-time detection of malleability-based signal or parameter falsification. To validate the proposed method, we conduct stage positioning control experiments and attack detection tests using an industrial linear stage. The results show that the encrypted DOB-based PID controller outperforms a conventional encrypted PID controller in terms of tracking accuracy. Furthermore, the system successfully detects two types of malleability-based attacks: one that destabilizes the control system, and another that degrades its performance. The primary contributions of this study are: (i) the implementation of a KHE-based encrypted DOB-PID controller, (ii) the improvement of control performance under uncertainties, and (iii) the experimental demonstration of attack detection capabilities in encrypted control systems.**

***Index Terms*—Cyberattack, encrypted control, keyed-homomorphic encryption.**

I. Introduction

The cybersecurity of networked control systems is critical. As these systems continue to evolve, the risk of cyberattacks targeting them has increased. For example, Stuxnet destroyed centrifuges at the Iranian nuclear facility [1], and a false data injection attack compromised sensor measurements in Ukrainian power grid [2]. Among various attacks on control systems [3]–[6], eavesdropping attacks not only steal communication signals but can also act as a precursor to more destructive intrusions [7]. Other attacks involve stealing operational information, such as controller parameters, by hacking into control devices. Therefore, enhancing the security of control systems is essential to protect them from cyber threats.

A promising approach to enhancing the security of networked control systems is encrypted control [8]–[12], which protects control system information by employing homomorphic encryption schemes. This enables the direct computation of encrypted control inputs from encrypted measurements, without requiring decryption. Encrypted control relies on various types of homomorphic encryption schemes, such as multiplicative homomorphic encryption [13], [14], additive homomorphic encryption [15], fully homomorphic encryption [16]–[18], and somewhat homomorphic encryption [19]. Furthermore, encryption schemes specifically adapted for control systems have been developed, including resilient homomorphic encryption [20], [21] and dynamic-key homomorphic encryption [22]. Although these methods can be effective for eavesdropping and mitigate several types of attack risks, they remain vulnerable to malleability, which is an inherent property of homomorphic encryption schemes [23]. Malleability is a security vulnerability that allows arithmetic operations to be performed directly on ciphertexts without knowledge of the encryption keys. In malleability-based attacks on encrypted control systems, adversaries can manipulate encrypted sensor measurements, control parameters, or control inputs without decryption, thereby destabilizing the control system [24] and compromizing the behavior of the plant [25]–[27].

The design of encrypted control systems must ensure resistance to malleability while maintaining satisfactory control performance across a range of plant dynamics. To address the vulnerability associated with malleability, keyed-homomorphic encryption (KHE) schemes have proven useful, as proposed in [28]–[32]. The concept of KHE introduces an additional private key dedicated to homomorphic operations, enabling the detection of signal or parameter falsification that exploits the malleability. To date, the only appliaction of KHE to control systems is the encrypted PID control system developed in [33]. Although this approach is effective in integrating encryption into control, it is not sufficient for ensuring satisfactory performance, particularly in systems with friction or modeling uncertainties, where PID control may fall short. To overcome the limitations of PID control in dealing with uncertainties, disturbance observers (DOBs) [34] are widely used in industrial systems. Several encrypted control systems incorporating DOBs have been proposed [35], [36]. However, all of these are based on the ElGamal encryption scheme, which is vulnerable to malleability-based attacks, thereby limiting their security guarantees. Furthermore, since numerical simulations cannot adequately account for uncertainties, it is essential to conduct experiments that not only evaluate the impact of quantization errors and determine appropriate encryption parameters, but also verify the system's ability to detect attacks in scenarios where an adversary exploits the malleability of the encryption scheme to compromise the control device and destabilize the system.

This study aims to propose an encrypted DOB-based PID

This work was supported in part by JSPS KAKENHI JP22H01509 and JP23K22779.

Naoki Aizawa is with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Chofu, Tokyo 1828585, Japan. Corresponding author(e-mail: aizawanaoki@uec.ac.jp).

Keita Emura is with Institute of Science and Engineering, Kanazawa University, Kanazawa, Ishikawa 920–1192, Japan.

Kiminao Kogiso is with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Chofu, Tokyo 1828585, Japan.

control system using a KHE scheme, in order to achieve both control performance and resistance to malleability-based attacks. To this end, a disturbance observer (DOB) is integrated with a PID controller so that the estimated disturbnace can be added to the control input, thereby compensating for modeling uncertainties. The proposed system is also designed to output error symbols when ciphertexts are falsified during decryption or evaluation, enabling the detection of malleability-based attacks. Furthermore, to validate the effectiveness of the proposed method, stage positioning control experiments and attack detection tests are conducted using an industrial linear stage. The experimental results demonstrate that the proposed encrypted DOB-based PID control system outperforms a conventional encrypted PID controller in terms of tracking performance. For attack detection, two scenarios of malleability-based control parameter falsification are evaluated: one that destabilizes the system, similar to the Stuxnet attack, and another that degrades performance. The results confirm that the system can detect and localize attacked components in real time.

The contributions of this study are threefold: i) the practical construction of an encrypted DOB-based PID controller using a KHE scheme, ii) the demonstration of improved control performance under uncertainty, and iii) the successful detection of malleability-based attacks through experimental validation. Unlike the method proposed in [33], this study integrates a disturbance observer into the control structure and addresses attack scenarios that target system destabilization. The remainder of this paper is organized as follows. Section II introduces the notations and KHE scheme as preliminaries. Section III formulates the proposed encrypted DOB-based PID controller. Section IV presents experimental results evaluating the tracking control performance. Section V demonstrates cyberattack tests to validate the feasibility of real-time detection. Finally, Section VI concludes the paper.

II. Preliminaries

This section defines the notations of variables, functions, and a quantizer, and introduces KHE for encrypting the controller and facilitating real-time attack detection.

A. Notations

The sets of real numbers, integers, plaintext spaces, and ciphertext spaces are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathcal{M}$, and $\mathcal{C}$, respectively. We define $\mathbb{R}^+ := \{x \in \mathbb{R} \mid 0 < x\}$, $\mathbb{Z}^+ := \{z \in \mathbb{Z} \mid 0 < z\}$, $\mathbb{Z}_0^+ := \{z \in \mathbb{Z} \mid 0 \leq z\}$, $\mathbb{Z}_n := \{z \in \mathbb{Z} \mid 0 \leq z < n\}$, $\mathbb{Z}_n^+ := \{z \in \mathbb{Z} \mid 0 < z < n\}$, and $\mathfrak{P}_a^b := \{a^i \bmod b \,|\, i \in \mathbb{Z}_b\}$. A multiplicative cyclic group is 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 the cyclic group $\mathbb{G}$. A set of vectors of size n is denoted by $\mathbb{R}^n$. The jth element of vector v is denoted by v_j. The set of matrices of size $m \times n$ is denoted by $\mathbb{R}^{m\times n}$. The (i, j) entry of matrix M is denoted by M_{ij}. $\mathbf{0}$ denotes a zero vector or zero matrix of an appropriate dimension. The greatest common divisor of the two positive integers $a, b \in \mathbb{Z}^+$ is denoted by $\gcd(a, b)$. The minimal residue of integer $a \in \mathbb{Z}$ modulo $m \in \mathbb{Z}^+$ is defined as $a \operatorname{Mod} m = b$ if $b < |b - m|$ holds; otherwise, $a \operatorname{Mod} m = b - m$, where $b = a \bmod m$.

Let p be an odd prime number and z be an integer satisfying $\gcd(z, p) = 1$. If there exists an integer b such that $b^2 = z \bmod p$, then integer z is a quadratic residue modulo p. If such an integer b does not exist, then z is a quadratic nonresidue modulo p. This can be expressed using the Legendre symbol $(\cdot/\cdot)_L$ as follows: $(z/p)_L = z^{\frac{p-1}{2}} \operatorname{Mod} p = 1$ if z is a quadratic residue; otherwise, -1. The rounding function $\lceil\cdot\rfloor$ of $\sigma \in \mathbb{R}^+$ to the nearest positive integer is defined as $\lceil\sigma\rfloor = \lfloor\sigma + 0.5\rfloor$ if $\sigma \geq 0.5$; otherwise, $\lceil\sigma\rfloor = 1$, where $\lfloor\cdot\rfloor$ denotes the floor function.

This study uses a quantizer that maps $x \in \mathbb{R}$ onto $\bar{x} := (\bar{x}^1, \bar{x}^2)$, proposed in [33]. An encoding map $\mathsf{Ecd}_\gamma := \mathscr{C} \circ \mathscr{A}_\gamma$ and a decoding map $\mathsf{Dcd}_\gamma := \mathscr{B}_\gamma \circ \mathscr{D}$ are described as follows:

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

where $\gamma \in \mathbb{R}^+$ is a quantization gain, $\zeta \in \{1, 2\}$ and $z := \lceil\gamma|x|\rfloor \bmod q$.

B. Keyed-Homomorphic Encryption

To construct encrypted control systems, this study uses KHE with a multiplicative homomorphism [28], which is currently the most efficient KHE scheme. The encryption scheme denoted as $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ consists of the following four algorithms.

1) Gen*:* $\kappa \mapsto (\mathsf{pk}, \mathsf{sk_d}, \mathsf{sk_h})$. The Gen algorithm takes security parameter κ and the key length ℓ regarding the ℓ-bit prime number p and outputs public, private, and homomorphic operation keys, denoted as pk, $\mathsf{sk_d}$, and $\mathsf{sk_h}$, respectively: $\mathsf{pk} = (g_0, g_1, s, \widehat{s}, \widetilde{s}_0, \widetilde{s}_1)$, $\mathsf{sk_d} = \left(k_0, k_1, \widehat{k}_0, \widehat{k}_1, \widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right)$, and $\mathsf{sk_h} = \left(\widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right)$, 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 $p = 2q + 1$.

2) Enc*:* $(\mathsf{pk}, m \in \mathcal{M}) \mapsto c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta) \in \mathcal{C}$. The Enc algorithm takes a public key 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 a target collision-resistance

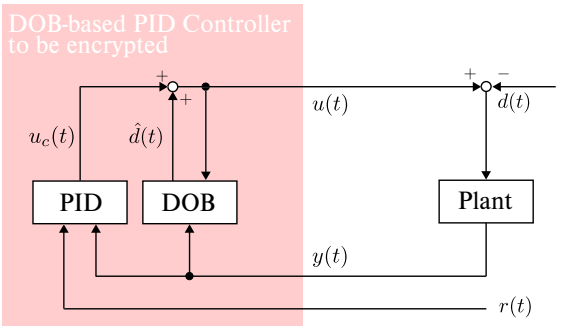


Fig. 1: Block diagram of the DOB-based PID control system

hash family and f_{hk} is a smooth function. SHA-256 is used for both Γ_{hk} and f_{hk}.

3) Dec*:* $(\mathsf{sk_d}, c \in \mathcal{C}) \mapsto m \in \mathcal{M} \cup \{\perp\}$. The Dec algorithm takes the private key $\mathsf{sk_d}$ and a ciphertext $c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta)$ and outputs a plaintext m or an error symbol $\perp$. First, compute: $\widehat{\pi}' := x_0^{\widetilde{k}_0} x_1^{\widetilde{k}_1} \bmod p$, $\delta := \Gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$, 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. 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 $\pi := x_0^{k_0} x_1^{k_1} \bmod p$.

4) Eval*:* $(\mathsf{sk_h}, c_1, c_2 \in \mathcal{C}) \mapsto c \in \mathcal{C} \cup \{\perp\}$. 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 $c_i := (x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i, \eta_i)$; $\delta := \Gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$; $\delta_i := \Gamma_{hk}(x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i)$; 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.

The KHE scheme is known to satisfy the following two conditions: i) For all $m \in \mathcal{M}$ and $c \in \mathcal{C}_{\mathsf{pk},m}$, it holds that $\mathsf{Dec}(\mathsf{sk_d}, c) = m$; ii) For all $m_1, m_2 \in \mathcal{M}$, $c_1 \in \mathcal{C}_{\mathsf{pk},m_1}$, and $c_2 \in \mathcal{C}_{\mathsf{pk},m_2}$, it holds that $\mathsf{Eval}(\mathsf{sk_h}, c_1, c_2) \in \mathcal{C}_{\mathsf{pk},m_1 \cdot m_2}$, where $\mathcal{C}_{\mathsf{pk},m}$ denotes the set of all ciphertexts of $m \in \mathcal{M}$ under the public key pk. For simplicity, the arguments pk, $\mathsf{sk_d}$, and $\mathsf{sk_h}$ will be omitted henceforth.

III. Encrypting DOB-based PID Controller

This section formulates the encrypted DOB-based PID control system.

A. DOB-based PID controller

This study considers the linear plant in the discrete-time state-space representation:

$$x_p(t+1) = A_p x_p(t) + B_p u(t) - B_p d(t), \tag{1a}$$
$$y(t) = C_p x_p(t), \tag{1b}$$

where $t \in \mathbb{Z}_0^+$ is the step, $x_p \in \mathbb{R}^2$ is the state, $u \in \mathbb{R}$ is the input, $y \in \mathbb{R}$ is the measurement (output), and $d \in \mathbb{R}$ is the exogenous disturbance, which is assumed to be unknown but constant over the steps. Moreover, the pairs (A_p, B_p) and (C_p, A_p) are controllable and observable, respectively.

This study considers the situation where for the plant (1), the following DOB-based PID controller is designed, as illustrated in Fig. 1, to achieve the tracking control for a given setpoint reference $r \in \mathbb{R}$,

$$x(t+1) = Ax(t) + Bv(t), \tag{2a}$$
$$u(t) = Cx(t) + Dv(t), \tag{2b}$$

where $x \in \mathbb{R}^5$ and $v \in \mathbb{R}^2$ are the controller's state and input, respectively. The definitions of the controller's state and coefficients are derived below.

Firstly, the PID controller from a feedback error $e := r - y \in \mathbb{R}$ to $u_c \in \mathbb{R}$:

$$u_c(t) = K_p e(t) + K_i w(t) + K_d \frac{e(t) - e(t-1)}{T_s},$$

can form into the discrete-time state-space representation:

$$x_c(t+1) = A_c x_c(t) + B_c v(t), \tag{3a}$$
$$u_c(t) = C_c x_c(t) + D_c v(t), \tag{3b}$$

where $x_c(t) := \begin{bmatrix} e(t-1) & w(t-1) \end{bmatrix}^\top \in \mathbb{R}^2$ and $v(t) := \begin{bmatrix} r(t) & y(t) \end{bmatrix}^\top \in \mathbb{R}^2$ are the PID-controller's state and input, respectively; $w \in \mathbb{R}$ is the accumulated error, i.e., $w(t) = T_s \sum_{\tau=0}^{t-1} e(\tau) = w(t-1) + T_s e(t-1)$, $\forall t \in \mathbb{Z}_0^+$, where $e(-1)$ and $w(-1)$ are set to zero; K_p, K_i, and K_d are the PID gains; $T_s > 0$ is the sampling period; The coefficients in (3) are as follows:

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

Subsequently, the DOB is given as follows:

$$x_d(t+1) = \begin{bmatrix} A_p & -B_p \\ \mathbf{0} & 1 \end{bmatrix} x_d(t) + \begin{bmatrix} B_p \\ 0 \end{bmatrix} u(t) + \begin{bmatrix} L_x \\ L_d \end{bmatrix} (y(t) - \hat{y}(t)), \tag{4a}$$
$$\begin{bmatrix} \hat{y}(t) \\ \hat{d}(t) \end{bmatrix} = \begin{bmatrix} C_p & 0 \\ \mathbf{0} & 1 \end{bmatrix} x_d(t), \tag{4b}$$

where $x_d := \begin{bmatrix} \hat{x}_p^\top & \hat{d} \end{bmatrix}^\top \in \mathbb{R}^3$ is the DOB's state consisting of the estimate $\hat{x}_p$ of the plant state x_p and the estimated disturbance $\hat{d}$; $\hat{y} \in \mathbb{R}$ is the estimated plant's output; $L_x \in \mathbb{R}^2$ and $L_d \in \mathbb{R}$ are the observer gains. Furthermore, using u_c in (3b) and $\hat{d}$ in (4b), the control input u, which is the output of the DOB-based PID controller, is given as follows:

$$u(t) = u_c(t) + \hat{d}(t),$$
$$= C_c x_c(t) + D_c v(t) + \begin{bmatrix} \mathbf{0} & 1 \end{bmatrix} x_d(t). \tag{5}$$

The state equation of the DOB-based PID controller consists of (3a) and (4a) after eliminating u and $\hat{y}$ from (4a).

Consequently, defining the state in (2) as $x := \begin{bmatrix} x_c^\top & x_d^\top \end{bmatrix}^\top$, the DOB-based PID controller is described as follows:

$$x(t+1) = \begin{bmatrix} A_c & \mathbf{0} \\ B_d & A_d \end{bmatrix} x(t) + \begin{bmatrix} B_c \\ C_d \end{bmatrix} v(t), \tag{6a}$$

$$u(t) = \begin{bmatrix} C_c & \mathbf{0} & 1 \end{bmatrix} x(t) + D_c v(t), \tag{6b}$$

where $A_d \in \mathbb{R}^{3\times 3}$, $B_d \in \mathbb{R}^{3\times 2}$, and $C_d \in \mathbb{R}^{3\times 2}$ are as follows:

$$A_d = \begin{bmatrix} A_p - L_x C_p & \mathbf{0} \\ -L_d C_p & 1 \end{bmatrix}, \; B_d = \begin{bmatrix} B_p C_c \\ \mathbf{0} \end{bmatrix},$$

$$C_d = \begin{bmatrix} B_p(K_p + K_i T_s + \frac{K_d}{T_s}) & -B_p(K_p + K_i T_s + \frac{K_d}{T_s}) \\ 0 & L_d \end{bmatrix}.$$

Since (2) and (6) are identical, the coefficients (A, B, C, D) result in

$$A = \begin{bmatrix} A_c & \mathbf{0} \\ B_d & A_d \end{bmatrix}, \; B = \begin{bmatrix} B_c \\ C_d \end{bmatrix}, \; C = \begin{bmatrix} C_c & \mathbf{0} & 1 \end{bmatrix}, \; D = D_c.$$

B. Controller Encryption

The used KHE scheme is the type of multiplicatively homomorphic encryption, so the controller encryption method, proposed in [8], can be applied to secure implementation of the controller (2). It is rewritten as follows:

$$\psi(t) = \Phi\xi(t) =: f(\Phi, \xi(t)), \tag{7}$$

where $\psi \in \mathbb{R}^6$, $\Phi \in \mathbb{R}^{6\times 7}$, and $\xi \in \mathbb{R}^7$ are as follows,

$$\psi(t) := \begin{bmatrix} x(t+1) \\ u(t) \end{bmatrix} = \begin{bmatrix} e(t) \\ w(t) \\ \hat{x}_p(t+1) \\ \hat{d}(t+1) \\ u(t) \end{bmatrix}, \; \Phi := \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

$$\xi(t) := \begin{bmatrix} x(t) \\ v(t) \end{bmatrix} = \begin{bmatrix} e(t-1) \\ w(t-1) \\ \hat{x}_p(t) \\ \hat{d}(t) \\ r(t) \\ y(t) \end{bmatrix}.$$

For the DOB-based PID controller (7), since f is a composition product of multiplication $f^\times$ and addition f^+, the decryption algorithm is modified to yield $\mathsf{Dec}^+ = f^+ \circ \mathsf{Dec}$ [8]. The modified homomorphic encryption scheme $\mathcal{E}^+ = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}^+, \mathsf{Eval})$ enables to construct the encrypted controller $f^\times_{\mathcal{E}^+}$ as follows:

$$f^\times_{\mathcal{E}^+} : (\mathsf{Enc}(\bar{\Phi}), \mathsf{Enc}(\bar{\xi}(t)) \mapsto \mathsf{Enc}(\bar{\Psi}(t)), \tag{8}$$

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 $\mathsf{Enc}(\bar{\Psi}(t))$ is calculated as follows:

$$\mathsf{Enc}(\bar{\Psi}^\theta_{ij}(t)) = \mathsf{Eval}(\mathsf{Enc}(\bar{\Phi}^\theta_{ij}, \mathsf{Enc}(\bar{\xi}^\theta_j(t))), \quad \forall\theta \in \{1,2\}, \forall i \in \mathbb{Z}^+_7, \forall j \in \mathbb{Z}^+_8. \tag{9}$$

The function (8) is a ciphertext version of (7), which is realized in (9). Therefore, as shown in Fig. 2, function f running in the controller is replaced by $f^\times_{\mathcal{E}^+}$, and the controller output

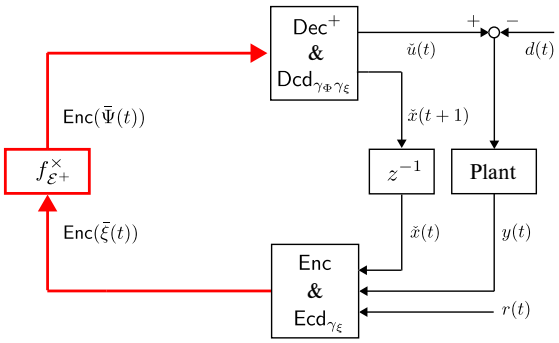


Fig. 2: Block diagram of the proposed encrypted DOB-based PID control system.

$\mathsf{Enc}(\bar{\Psi}(t))$ is decrypted and decoded at the plant side to extract control input u via a decoded (quantized) signal $\breve{\psi}$:

$$\breve{\psi} = \begin{bmatrix} \breve{x}(t+1) \\ \breve{u}(t) \end{bmatrix} := \mathsf{Dcd}_{\gamma_\Phi\gamma_\xi}(\mathsf{Dec}^+(\mathsf{Enc}(\bar{\Psi}(t)))).$$

Additionally, $u - \breve{u}$ means the quantization error in u.

The next section will discuss the effectiveness of the encrypted DOB-based PID control presented as a cybersecurity measure, using an industrial linear stage.

Remark 1: This study assumes that transmission delays between the plant and controller sides are sufficiently shorter than a sampling period to simplify the discussion. This implies that communication links can be used without their quality affecting control performance.

IV. Experimental Validation

This section validates the encrypted DOB-based PID control of an industrial linear stage, compared with the encrypted PID control addressed in [33].

A. Positioning Control System for Linear Stage

This study considers the DOB-based positioning control system for the linear stage, as shown in Fig. 3. The stage and the computer setup are the same as those used in [33], with their specifications summarized in TABLE I. The input to the stage is current (A), and its output is position measured by a linear encoder. The stage model is expressed as $P(s) = s^{-1}\tilde{P}(s)$, where $\tilde{P}(s)$ captures the dynamics from the current input to velocity. Based on a step-response experiment, the dynamics were identified as:

$$\tilde{P}(s) = \frac{28.288}{s + 34},$$

where the step input was $u(t) = 0.7$. The results of the model identification are shown in Fig. 4. Figs. 4(a) and (b) illustrate the time responses of the stage velocity and control input, respectively. In these figures, black dots represent the measured velocity, and the red line corresponds to the output of $\tilde{P}(s)$. Defining the plant state as $x_p \in \mathrm{Re}^2$ and discretizing the dynamics using a zero-order hold with a sampling period

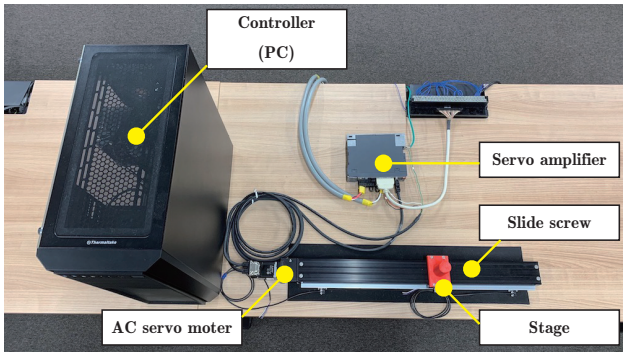
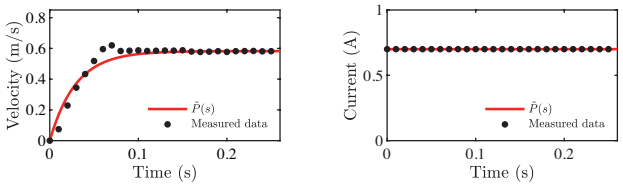


Fig. 3: Whole view of positioning control system for industrial linear stage [33].



(a) Velocity output $v(t)$ (b) Input current $u(t)$

Fig. 4: Model identification by step-response experiment.

$T_s = 10$ ms, the discrete-time state-space representation of $P(s)$ is realized with the following system matrices:

$$A = \begin{bmatrix} 1 & 0.0085 \\ 0 & 0.7118 \end{bmatrix}, \; B = \begin{bmatrix} 0.0013 \\ 0.2398 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

where the state is defined as $x_p := \begin{bmatrix} x_{p,1} \, x_{p,2} \end{bmatrix}^\top$, with $x_{p,1}$ and $x_{p,2}$ representing the stage position (m) and velocity (m/s), repsectivey.

The observer gains were designed as follows:

$$L_x = \begin{bmatrix} 2.7118 & 199.2800 \end{bmatrix}^\top, \quad L_d = -380.4456,$$

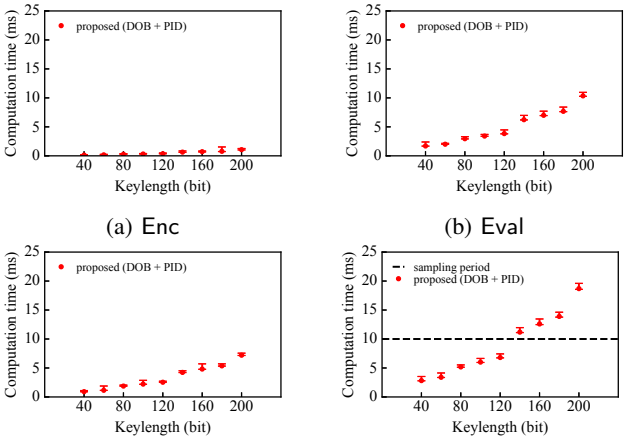
ensuring that the eigenvalues of the DOB are smaller than those of the plant. The position reference was given as:

$$r(t) = \begin{cases} 0 & \text{if } \; 0 \le T_s t < 2.0, \\ 0.05 & \text{if } \; 2.0 \le T_s t < 4.0, \\ 0.10 & \text{if } \; 4.0 \le T_s t < 6.0, \\ 0.05 & \text{if } \; 6.0 \le T_s t < 8.0, \\ 0 & \text{if } \; 8.0 \le T_s t. \end{cases} \tag{10}$$

Based on the control objective of tracking the reference, the PID controller parameters were tuned through trial and error and set as follows: $K_p = 12$, $K_i = 0.25$, and $K_d = 0.030$. In this case, Φ is given as follows:

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0.01 & -0.01 \\ -0.0039 & 0.0003 & -1.7118 & 0.0085 & 0 & 0.0195 & 2.6923 \\ -0.7194 & 0.0600 & -199.2800 & 0.7118 & 0 & 3.5976 & 195.6824 \\ 0 & 0 & 380.4456 & 0 & 1 & 0 & -380.4456 \\ -3 & 0.25 & 0 & 0 & 1 & 15.0025 & -15.0025 \end{bmatrix}$$

The key length was set to 120 bits for encrypting the controller. This value was determined by evaluating the computation time of the encrypted control processes, including



(a) Enc (b) Eval

(c) Dec$^+$ (d) Total time

Fig. 5: Computation time of each process over the key length.

Enc, Eval, Dec$^+$ across different key lengths. The average computation times, measured over 1,000 trials for key lengths ranging from 40 to 200 bits in increments of 20 bits, are presented in Fig. 5. Figs. 5(a), (b), and (c) show the computation times for Enc, Eval, and Dec$^+$, respectively, and Fig. 5(d) shows the total computation time. The red dots represent the proposed control systems. The key length was set to 120 bits based on the observation that the average computation time at this length is 6.806 ms, with a variation of 0.685 ms between the maximum and minimum values, which is less than T_s. This configuration ensures real-time performance. Furthermore, for preventing overflow, quantization gains were set to $\gamma_\Phi = 10^{15}$ and $\gamma_\xi = 10^{16}$, determined through trial and error based on Theorem 3.3 in [33].

Remark 2: To ensure the security of the KHE scheme used in this study, the key length needs to be 2048 bits, as recommended by the NIST document [37]. However, such a long key can impact the efficiency of the control system, making alternative approaches, such as key updates, a potential solution. Additionally, the current static key setting allows replay attacks despite the detection mechanism. Enhancing security without compromising efficiency, for instance, through key updates, remains an important direction for future work.

B. Experimental Control Results and Evaluations

This section addresses two methods: One is the proposed encrypted DOB-based PID control method, and the other is the conventional encrypted PID control method [33]. The following time-averaged ℓ_1-norm index is introduced to measure the tracking performance between 2 s and 10 s:

$$\rho(e) := \frac{1}{10^3 - 200} \sum_{t=200}^{10^3-1} |r(t) - y(t)|,$$

where $e := r - y$ is the feedback (tracking) error, and $|\cdot|$ denotes the absolute value operator.

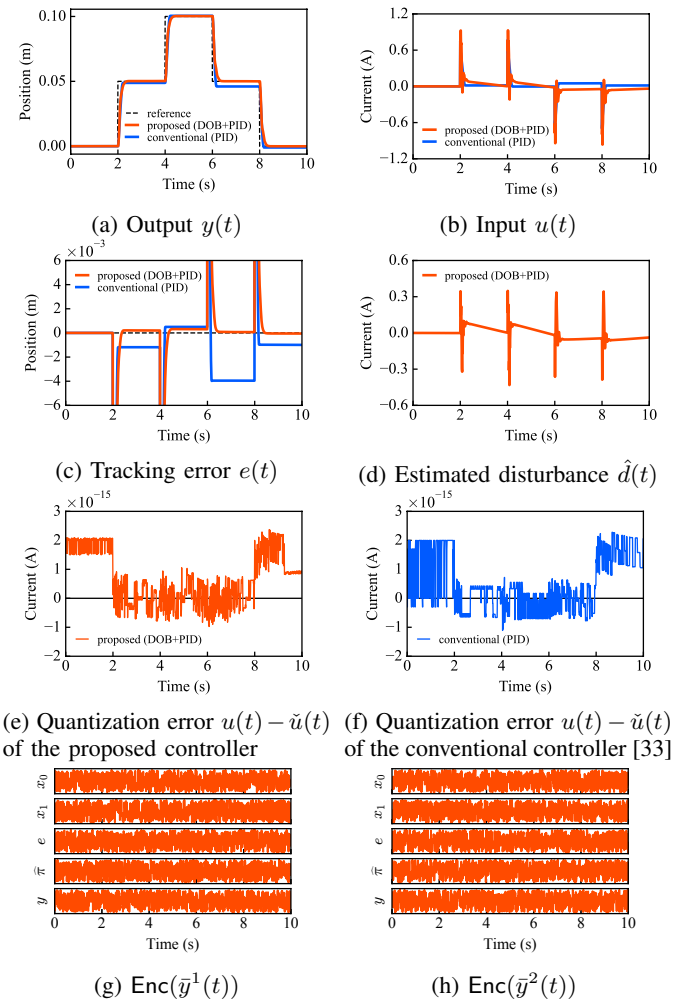
The positioning control results of the proposed control system and the conventional control system are shown in Fig. 6. Figs. 6(a) and (b) show the time responses of the

TABLE I: Experimental apparatus [33]

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
Lead	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)

measured stage position and the control input, respectively, and Fig. 6(c) shows the tracking error. In these figures, the red and blue lines represent the proposed control system and the conventional control system, respectively, and the black broken line represents the reference (10). Fig. 6(d) shows the time response of the disturbance estimated by the DOB. Figs. 6(e) and (f) show the time responses of the quantization error $u(t)-\breve{u}(t)$ of the proposed control system and the conventional control system, respectively. Figs. 6(g) and (h) show the time responses of the encrypted output $\mathsf{Enc}(\bar{\xi}_7^1(t))$ and $\mathsf{Enc}(\bar{\xi}_7^2(t))$, respectively, where ξ_7 is corresponding to the stage position y in the proposed control system.

In Fig. 6(c), The tracking performance index scores $\rho(e)$ for the proposed and the conventional control system are 2.669×10^{-3} and 3.737×10^{-3}, respectively. The results demonstrate that the proposed control system improves tracking performance by compensating for the disturbance through DOB. Figs. 6(e) and (f) confirm that the quantization errors induced in both the proposed and the conventional control systems are negligible because it is in the 10^{-15} ampere range and too small to affect the stage. Furthermore, Figs. 6(g) and (h) validate that the stage position y is effectively concealed by random numbers. Therefore, these experimental control results confirm that the proposed control system achieves better tracking performance than the conventional control system.



(a) Output $y(t)$ (b) Input $u(t)$

(c) Tracking error $e(t)$ (d) Estimated disturbance $\hat{d}(t)$

(e) Quantization error $u(t)-\breve{u}(t)$ of the proposed controller

(f) Quantization error $u(t)-\breve{u}(t)$ of the conventional controller [33]

(g) $\mathsf{Enc}(\bar{y}^1(t))$ (h) $\mathsf{Enc}(\bar{y}^2(t))$

Fig. 6: Experimental results of the proposed and conventional encrypted controls.

V. Demonstration Of Attack Detection

This section demonstrates the effectiveness of malleability-based falsification attack detection through experimental attack tests.

A. Attack Models

In this study, we assume that the attackers have internal access to the controller and understand the structure of the ciphertext c, as well as the method to compute the plaintext m from c, i.e., $m = \epsilon(\pi)^{-1} \bmod p$. However, attackers do not possess the private or homomorphic operation keys, $\mathsf{sk_d}$ and $\mathsf{sk_h}$. During a falsification attack, attackers overwrite the third component of the encrypted data c by multiplying it with $\lambda \in \mathbb{G}$, as follows:

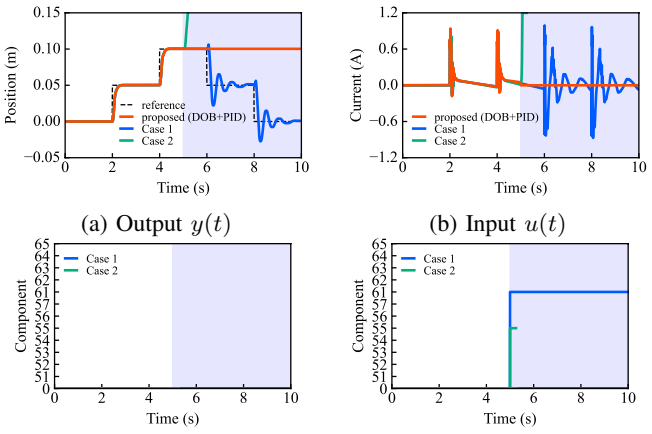
$$c^a = (x_0, x_1, \lambda\epsilon, \widehat{\pi}, \eta) \in \mathcal{C}.$$

As a result, the falsified ciphertext c^a leads to $\lambda\epsilon(\pi)^{-1} \bmod p = \lambda m$. Even without knowledge of the private key, attackers can manipulate the third component of the ciphertext to scale the control parameter by an integer factor of λ. However, if the Eval and Dec algorithms are correctly implemented, such manipulation will result in the output of an error symbol.

This study examines two falsification attack scenarios targeting control parameters: i) Case 1: The 61th component of the encrypted system matrix Φ corresponding to the control parameters, denoted as Φ_{61}, is multiplied by $\lambda = 12$:

$$c_{\bar{\Phi}_{61}^2}(t) = \begin{cases} c^a_{\bar{\Phi}_{61}^2}(t), & \text{if } \ T_s t \in [5, 10), \\ c_{\bar{\Phi}_{61}^2}(t), & \text{otherwise.} \end{cases}$$

Because $\Phi_{61}^2 = C_{11}$, multiplying Φ_{61}^2 by 12 inceases u, leading to degraded control performance. Additionally, because attackers can regulate u using λ, the attack is difficult to detect using threshold-based detection methods, such as the one presented in [38], and ii) Case 2: This scenario considers an



(a) Output $y(t)$ (b) Input $u(t)$

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

Fig. 7: Results of falsification attack against the proposed encrypted control system

attack that destabilizes the control system by modifying Φ_{55}. Specifically, Φ_{55} is multiplied by $\lambda = 2$:

$$c_{\bar{\Phi}^2_{55}}(t) = \begin{cases} c^a_{\bar{\Phi}^2_{55}}(t), & \text{if } \ T_s t \in [5, 10), \\ c_{\bar{\Phi}^2_{55}}(t), & \text{otherwise.} \end{cases}$$

As a result, the absolute values of the control system's eigenvalues change from $\{0.3571, 0.3571, 0.0083, 0.1768, 0.9618, 0.9618, 0.9998\}$ to $\{0.5476, 0.5476, 1.7145, 0.0051, 0.5570, 1.2074, 1.0001\}$, which indicates that the attack destabilizes the system.

B. Detection Results

In the experiment, the control input is set to zero whenever an error symbol is detected in the components of $C_{\bar{\Psi}}$ because the stage can accelerate rapidly and potentially damage the experimental setup. The control system and objectives remain identical to those in Section IV.

The detection results of the proposed encrypted control system under falsification attacks are shown in Fig. 7. Figs. 7(a) and (b) show the time responses of the measured stage position and the control input, respectively. Figs. 7(c) and (d) show the error symbols for 51th to 65th components of $C_{\bar{\Psi}^1}$ and $C_{\bar{\Psi}^2}$ in Eval, respectively. In these figures, the red, blue, and green lines correspond to: i) The proposed control system against the attack in both Case 1 and Case 2 (results are identical for both cases), ii) The response when the proposed control system ignores the detection in Case 1, and iii) The response when the proposed control system ignores the detection in Case 2, respectively. The blue-shaded area indicates the duration of the falsification attack. In Case 2, the stage was stopped at 5.32 s by activating the emergency stop button due to its rapid acceleration.

Figs. 7(d) confirms that the indices of the attacked components, $C_{\bar{\Psi}^2_{61}}$ and $C_{\bar{\Psi}^2_{55}}$, are successfully detected by the proposed control system. Consequently, the control input u was set to zero during the attack period, maintaining the stage position, as shown by the red line of Fig. 7(a). These results demonstrate that the proposed encrypted control system can detect falsification attacks in real time and accurately identify the affected components.

VI. Conclusion

This study proposed an encrypted DOB-based PID control system using a KHE scheme, aiming to achieve control performance and resistance to malleability-based attacks. The system was experimentally validated on an industrial linear stage through both tracking control tests and attack detection experiments. The results demonstrated that the proposed controller outperformed a conventional encrypted PID controller in terms of tracking accuracy while maintaining the confidentiality of communication signals and control parameters. Furthermore, the attack detection experiments confirmed that the system could successfully identify malleability-based falsifications and localize the compromised components in real time.

For future work, we plan to explore the integration of updatable KHE to further enhance both the security and computational efficiency of encrypted control systems. This extension would enable the detection of replay attacks and support longer key lengths while maintaining real-time feasibility. We also intend to investigate countermeasures against the leakage of homomorphic operation keys to ensure security even under partial exposure of cryptographic information. In addition, developing methods to estimate or detect the manipulation factor λ would enhance system resilience by enabling real-time identification of unauthorized modifications. Finally, exploring (attribute-based) keyed fully homomorphic encryption schemes [39], [40] represents a promising direction for advancing the design and capabilities of encrypted control systems.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE security & privacy*, vol. 9, no. 3, pp. 49–51, 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 Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[3] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th annual Allerton conference on communication, control, and computing (Allerton)*, pp. 911–918, 2009.

[4] ——, "False data injection attacks in control systems," in *Preprints of the 1st workshop on Secure Control Systems*, vol. 1, 2010.

[5] 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, 2019.

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

[7] M. S. Chong, H. Sandberg, and A. M. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," *18th European Control Conference (ECC)*, pp. 968–978, 2019.

[8] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *IEEE Conference on Decision and Control*, pp. 6836–6843, 2015.

[9] J. Kim, D. Kim, Y. Song, H. Shim, H. Sandberg, and K. H. Johansson, "Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption," *Annual Reviews in Control*, vol. 54, pp. 200–218, 2022.

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

[11] N. Schlüter, P. Binfet, and M. Schulze Darup, "A brief survey on encrypted control: From the first to the second generation and beyond," *Annual Reviews in Control*, vol. 56, p. 100913, 2023.

[12] S. Bian, Y. Fu, D. Zhao, H. Pan, Y. Jin, J. Sun, H. Qiao, and Z. Guan, "FHECAP: An Encrypted Control System with Piecewise Continuous Actuation," *IEEE Transactions on Information Forensics and Security*, pp. 4551–4566, 2025.
[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[15] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*, pp. 223–238, 1999.
[16] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, pp. 1–36, 2014.
[17] C. Gentry, "A fully homomorphic encryption scheme," Ph. D. dissertation, Stanford, CA, USA, 2009.
[18] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Advances in cryptology–ASIACRYPT 2017: 23rd international conference on the theory and applications of cryptology and information security*, pp. 409–437, 2017.
[19] J. Dyer, M. Dyer, and J. Xu, "Practical homomorphic encryption over the integers for secure computation in the cloud," *International Journal of Information Security*, vol. 18, pp. 549–579, 2019.
[20] M. Fauser and P. Zhang, "Resilient homomorphic encryption scheme for cyber-physical systems," in *60th IEEE Conference on Decision and Control (CDC)*, pp. 5634–5639, 2021.
[21] ——, "A secure resilient homomorphic encryption scheme for control systems," *IEEE Transactions on Automatic Control*, pp. 3711–3726, 2024.
[22] 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 Transactions on Automatic Control*, vol. 68, no. 4, pp. 2183–2198, 2022.
[23] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," *Taylor and Francis Group, LLC*, 2015.
[24] 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.
[25] H. Kwon, H. Kawase, H. A. Nieves-Vazquez, K. Kogiso, and J. Ueda, "Perfectly Undetectable False Data Injection Attacks on Encrypted Bilateral Teleoperation System based on Dynamic Symmetry and Malleability," in *IEEE International Conference on Robotics and Automation (ICRA)*, 2025.
[26] H. Kwon, J. Blevins, and J. Ueda, "Defense Mechanisms Against Undetectable Cyberattacks on Encrypted TeleroboticControl Systems," in *IEEE/ASME Transactions on Mechatronics*, 2025.
[27] J. Blevins and J. Ueda, "Encrypted Model Reference Adaptive Control with False Data Injection Attack Resilience via Somewhat Homomorphic Encryption-Based Overflow Trap," *IEEE Transactions on Industrial Cyber-Physical Systems*, 2025.
[28] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption," in *Public-Key Cryptography*, pp. 32–50, 2013.
[29] 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 *Advances in Cryptology – EUROCRYPT 2014*, pp. 514–532, 2014.
[30] C. S. Jutla and A. Roy, "Dual-System Simulation-Soundness with Applications to UC-PAKE and More," in *Advances in Cryptology – ASIACRYPT 2015*, pp. 630–655, 2015.
[31] Y. Maeda and K. Nuida, "Chosen Ciphertext Secure Keyed Two-Level Homomorphic Encryption," in *Information Security and Privacy*, pp. 209–228, 2022.
[32] H. Shinoki and K. Nuida, "On Extension of Evaluation Algorithms in Keyed-Homomorphic Encryption," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E107.A, no. 3, pp. 218–233, 2024.
[33] M. Miyamoto, K. Teranishi, K. Emura, and K. Kogiso, "Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption," *IEEE Access*, vol. 11, pp. 45749–45760, 2023.
[34] W. Chen, J. Yang, L. Guo, and S. Li, "Disturbance-observer-based control and related methods—An overview," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 2, pp. 1083–1095, 2015.
[35] K. Teranishi, M. Kusaka, N. Shimada, J. Ueda, and K. Kogiso, "Secure observer-based motion control based on controller encryption," in *American Control Conference (ACC)*, pp. 2978–2983, 2019.
[36] H. Takanashi, A. Kosugi, K. Teranishi, T. Mizuya, K. Abe, and K. Kogiso, "Cyber-Secure Teleoperation With Encrypted Four-Channel Bilateral Control," *IEEE Transactions on Control Systems Technology*, pp. 1–15, 2025.
[37] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 5)," *NIST special publication*, pp. 800–857, 2020.
[38] R. Baba, K. Kogiso, and M. Kishida, "Detection method of controller falsification attacks against encrypted control system," in *SICE Annual Conference*, pp. 244–248, 2018.
[39] S. Sato, K. Emura, and A. Takayasu, "Keyed-Fully Homomorphic Encryption without Indistinguishability Obfuscation," in *20th International Conference on Applied Cryptography and Network Security, LNCS*, vol. 13269, pp. 3–23, 2022.
[40] K. Emura, S. Sato, and A. Takayasu, "Attribute-Based Keyed Fully Homomorphic Encryption," in *14th International Conference on Security and Cryptography for Networks, LNCS*, vol. 14974, pp. 47–67, 2024.

Naoki Aizawa received the B. E. degree from The University of Electro-Communications, Tokyo, Japan, in 2024, and he is currently an M. E. student at The University of Electro-Communications, Tokyo, Japan. His research interest includes encrypted controls.

Keita Emura received his M.E. degree from Kanazawa University in 2004. He was with Fujitsu Hokuriku Systems Ltd., from 2004 to 2006. He received his Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST) in 2010, where he was with the Center for Highly Dependable Embedded Systems Technology as a post-doctoral researcher in 2010-2012.

He has been a researcher with the National Institute of Information and Communications Technology (NICT) since 2012, has been a senior researcher at NICT since 2014, and has been a research manager at NICT since 2021. His research interests include public-key cryptography and information security. 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. He is a member of IEICE, IPSJ, and IACR.

Kiminao Kogiso received his 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 in the 21st Century COE Program and as an Assistant Professor in 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 at the Georgia Institute of Technology, Atlanta, GA, USA. In March 2014, he was promoted to the position of Associate Professor in the Department of Mechanical and Intelligent Systems Engineering at The University of Electro-Communications, Tokyo, Japan. Since April 2023, he has been serving as a full Professor in the same department. His research interests include cybersecurity of control systems, constrained control, control of decision-makers, and their applications.