Stability‐guaranteed dynamic ElGamal cryptosystem for encrypted control systems

doi: 10.1049/iet-cta.2019.0729

IET Control Theory & Applications

Research Article

IET Journals
The Institution of Engineering and Technology

Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems

ISSN 1751-8644
Received on 25th June 2019
Revised 6th November 2019
Accepted on 16th April 2020
E-First on 17th September 2020
doi: 10.1049/iet-cta.2019.0729
www.ietdl.org

Kaoru Teranishi[1] ✉, *Naoki Shimada*[2], *Kiminao Kogiso*[1]

[1]*Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan*

[2]*Department of Electronics and Information Engineering, National Institute of Technology, Ishikawa College, Kitacyujo, Tsubata, Ishikawa 929-0392, Japan*

✉ *E-mail: teranishi@uec.ac.jp*

Abstract: Despite the importance of cyber-security for networked control systems, no suitable cryptosystem exists for networked control systems that guarantees stability and has low computational complexity. This study proposes a novel dynamic ElGamal cryptosystem for encrypted control systems. The proposed cryptosystem is a multiplicative homomorphic cryptosystem, and it updates key pairs and ciphertexts by simple updating rules with modulo operations at every sampling period. Furthermore, the authors modify the proposed cryptosystem by using a dynamic encoder and decoder so that the asymptotic stability of the encrypted control systems is guaranteed. Numerical simulations demonstrate that the encrypted controller with the proposed cryptosystem achieves asymptotic stability while randomly updating key pairs and ciphertexts. The feasibility of the proposed encrypted control system is evaluated through regulation control with a positioning table testbed. The processing time of the proposed encrypted control system is on the order of milliseconds, indicating that the system achieves real-time control.

1 Introduction

The cyber-security of networked control systems is crucial, and control systems require special countermeasures considering threats at both the cyber and physical layers [1]. As cyber-attacks for networked control systems, replay attacks [2], zero-dynamics attacks [3], and denial-of-service attacks [4] have been reported. Replay attacks are performed to deceive an anomaly detector or operator of control systems. Adversaries record sensor measurements of a target system under normal conditions for a certain period; then, they alter the sensor measurements to be transmitted to a controller into recorded signals. The adversaries disturb or destroy the target system during this time. In zero-dynamics attacks, adversaries design attack signals based on plant, controller, and anomaly detector dynamics [1]. By injecting the designed signals into control inputs, the adversaries stealthily destabilise a closed-loop system by zero-dynamics. Denial-of-service attacks interfere with the operation of the target system as with the attacks on information and communication systems. The impact of such attacks on control systems is more severe because the plant becomes out of control.

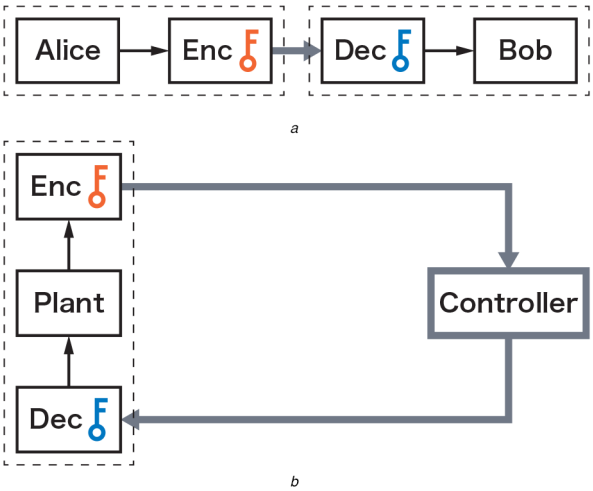

Fig. 1 *Comparison between public-key cryptography and encrypted control system*
(a) Public-key cryptography, ***(b)*** Encrypted control system

The controller encryption method is a security-enhancement method for networked control systems [5]. In this method, controller parameters and signals over communication links (i.e. sensor measurements, references, and control inputs) are encrypted with a multiplicative homomorphic cryptosystem, such as RSA [6] or ElGamal [7]. Furthermore, control inputs are calculated without decryption. As shown in Fig. 1, public-key cryptography requires Bob to share his public key with Alice in advance before sending ciphertexts of messages. In contrast, public keys and secret keys are not necessary for the controller side in encrypted control systems. The controller encryption method reduces the risk of zero-dynamics attacks due to its prevention of eavesdropping, which aims to identify the dynamics of control systems. By using the dynamic key-switching management method [8], encrypted control systems can detect controller falsification attacks and replay attacks with control input falsification. Additionally, encrypted control systems can achieve resilience against controller/signal falsification using the control-input-switching method [9].

However, the dynamic key-switching management method must prepare multiple key pairs in advance and continue managing them while encrypted control systems operate. Furthermore, encrypted control systems with the conventional ElGamal cryptosystem cannot achieve asymptotic stability because of quantisation errors caused by encoding signals into plaintexts. Stability is the most critical property for control systems, and asymptotic stability is a typical type of stability where arbitrary initial state converges to zero at some time in linear systems. The conventional ElGamal cryptosystem also has a risk to destabilise closed-loop systems in which the plant is an unstable system (e.g. airplane, quadcopter, and inverted pendulum).

The stability is not guaranteed due to the changing properties of the original closed-loop systems by encryption.

Besides, the majority of encryption security measures likely cause time delays [10]. Servo control systems for mechanical

systems, such as the positioning stage used for factory automation, typically must operate within a sampling period of a few milliseconds to hundreds of microseconds. Meanwhile, it is sufficient for information on control systems to be protected for a couple of decades because the systems are replaced. Furthermore, we do not have to protect all data of signals because adversaries are interested in eavesdropping time series data for system identification or designing attack signals. Therefore, the conventional methodology of cryptography is not suitable for encrypted control systems. The controller encryption method requires a lightweight multiplicative homomorphic cryptosystem that inherits the stability of unencrypted systems.

This study proposes a novel ElGamal-based dynamic multiplicative homomorphic cryptosystem and an encrypted control system with the proposed cryptosystem. The characteristics of the proposed encrypted control systems are as follows:

- Simple updating rules with modulo operations update key pairs and ciphertexts. Thus, adversaries cannot obtain time-series data if they do not keep cracking the code at every sampling period. Adversaries may be not able to decrypt data back towards a past time, even if they succeed in breaking a key pair at present.
- The proposed dynamic cryptosystem can be expected to achieve a security level equal to those of conventional methods with a smaller key because the hardness of cracking ciphertexts improves by the key pairs and ciphertexts updating. Smaller key length leads to low computational cost of operations in encryption and decryption (i.e. a lightweight cryptosystem).
- The encrypted control system modified to use a dynamic encoder and decoder inherits the asymptotic stability of unencrypted closed-loop systems.
- The proposed encrypted control system can detect replay attacks in the same way as that in [8, 9]. Furthermore, it is not necessary to prepare and manage multiple key pairs, unlike the method in [8, 9], because key pairs are updated at every sampling period.

Numerical simulations of encrypted state-feedback control are employed to investigate the validity of the proposed cryptosystem. Additionally, the feasibility of the proposed cryptosystem is examined through encrypted regulation control with a positioning table testbed. Control performance and processing time are evaluated.

1.1 Related works

The encrypted control method with the Paillier cryptosystem [11], additive homomorphic cryptosystem, was proposed in [12]. This method achieves *practical stability* [12] if the key length is sufficiently large. However, asymptotic stability cannot be guaranteed due to the effect of quantisation errors. Whereas, Kishida [13] considered an encrypted state-feedback controller with a dynamic quantiser proposed in [14] to achieve asymptotic stability of encrypted control systems. Encrypted control systems with an additive homomorphic cryptosystem are vulnerable against eavesdropping attacks on the controller because they cannot conceal controller parameters. Thus, encrypted control systems with a multiplicative homomorphic cryptosystem are more secure than those with an additive homomorphic cryptosystem.

Another encrypted control method with Gentry's fully homomorphic encryption [15] was proposed in [16]. Although, in this method, the controller can calculate encrypted control input by using encrypted controller parameters and encrypted sensor measurements, it requires vast computational resources compared to encrypted controllers with a partially homomorphic cryptosystem [17]. Hence, the encrypted control method with fully homomorphic encryption is not practical for real-time computation.

In the field of cryptography for information and communication, the one-time pad technique is well known. This technique has a similar methodology to the proposed method from the viewpoint that a new key is used for each communication; further, encryption schemes based on one-time pad provide perfect security as long as the schemes are correctly operated [18]. However, the conventional one-time pad schemes do not guarantee real-time computation and stability of control systems. In contrast, the proposed cryptosystem guarantees asymptotic stability of a closed-loop system with real-time updated key pairs.

The proxy re-encryption scheme [19] and bidirectional ElGamal encryption scheme [20] can translate a ciphertext for Alice into another ciphertext corresponding to Bob by using a proxy key. Although these methods are similar to the proposed method, a proxy server, which is a trustworthy third party, and proxy key are necessary. Thus, in these methods, we have to manage a proxy server and an additional key to the translation of ciphertexts throughout control system operation. Furthermore, Dodis *et al.* [21] proposed the key-insulated encryption scheme, which updates a secret key periodically; however, the updating period is more extended than in the proposed cryptosystem (one week).

1.2 Outline

The remainder of this paper is organised as follows. Section 2 introduces preliminary information of the ElGamal cryptosystem and encrypted control systems. Section 3 describes the proposed ElGamal-based dynamic multiplicative homomorphic cryptosystem. Section 4 describes an encrypted state-feedback controller with the proposed cryptosystem and a dynamic encoder and decoder. Section 5 provides numerical examples for comparison between the conventional ElGamal cryptosystem and the proposed cryptosystem. Section 6 presents several experimental results using a testbed with a regulator. Section 7 presents conclusions and discusses future works.

2 Preliminaries

2.1 Notation

The sets of real numbers, rational numbers, integers, prime numbers, public keys, secret keys, plaintexts, and ciphertexts are denoted by $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{P}$, $\mathscr{K}_\mathsf{p}$, $\mathscr{K}_\mathsf{s}$, $\mathscr{M}$, and $\mathscr{C}$, respectively. The set of key pairs is denoted by $\mathscr{K} = \mathscr{K}_\mathsf{p} \times \mathscr{K}_\mathsf{s}$. We define the sets of integers $\mathbb{Z}^+ := \{z \in \mathbb{Z} \mid 0 \leq z\}$, $\mathbb{Z}_n := \{z \in \mathbb{Z} \mid 0 \leq z < n\}$, and $\mathbb{Z}_n^\times := \mathbb{Z}_n \setminus \{0\}$. The set of vectors whose sizes are n is denoted by $\mathbb{R}^n$, and the set of matrices whose sizes are $m \times n$ is denoted by $\mathbb{R}^{m\times n}$. The ith element of a vector $v = (v_i)$ is denoted by v_i, and the (i,j) entry of a matrix $M = (M_{ij})$ is denoted by M_{ij}. The ℓ_2 norm of v and the induced 2-norm of M are denoted by $\| v \|$ and $\| M \|$, respectively. The minimum eigenvalue of M is denoted by $\lambda_{\min}(M)$. The cardinality of a set A is denoted by $|A|$.

Definition 1: Let A be a finite set and X be a random variable. If

$$\Pr(X = a) = \frac{1}{|A|}, \ \forall a \in A,$$

then we say that X follows the discrete uniform distribution and is denoted as $X \sim \mathscr{U}(A)$.

2.2 ElGamal cryptosystem

Definition 2: An ElGamal cryptosystem ε [7] is a tuple

$$\varepsilon := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}),$$

where Gen is a key generation algorithm, Enc is an encryption algorithm, and Dec is a decryption algorithm

$$\mathsf{Gen} : \mathbb{P} \ni p \mapsto (\mathsf{pk}, \mathsf{sk}) = ((\mathbb{G}, q, g, h), s) \in \mathscr{K},$$
$$\mathsf{Enc} : \mathscr{M} \times \mathscr{K}_\mathsf{p} \ni (m, \mathsf{pk}) \mapsto C = (g^r \bmod p, mh^r \bmod p) \in \mathscr{C}$$
$$\mathsf{Dec} : \mathscr{C} \times \mathscr{K}_\mathsf{s} \ni (C, \mathsf{sk}) = ((c_1, c_2), \mathsf{sk}) \mapsto c_1^{-s} c_2 \bmod p \in \mathscr{M},$$

$p = 2q + 1$ is a safe prime, pk is a public key, sk is a secret key, g is a generator of a cyclic group $\mathbb{G} = \{g^i \bmod p \mid i \in \mathbb{Z}_q\} = \mathscr{M} \subset \mathbb{Z}_p^\times$

such that $g^q \bmod p = 1$, $\mathscr{C} = \mathbb{G} \times \mathbb{G}$, $r, s \sim \mathscr{U}(\mathbb{Z}_q)$, and $h = g^s \bmod p$.

Proposition 1: ε holds multiplicative homomorphism

$$\mathsf{Dec}(\mathsf{Enc}(m_1, \mathsf{pk}) * \mathsf{Enc}(m_2, \mathsf{pk}) \bmod p, \mathsf{sk}) = m_1 m_2,$$

where $*$ is the Hadamard product (i.e. element-wise multiplication).

Proposition 2: The security level of ε is indistinguishability against chosen-plaintext attacks under the decisional Diffie-Hellman assumption.

2.3 Encrypted control system

A plant P is given as follows:

$$P: \begin{cases} x(t+1) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases}$$

where $x(t) \in \mathbb{R}^n$ is a state, $u(t) \in \mathbb{R}^m$ is an input, $y(t) \in \mathbb{R}^l$ is an output, and A, B, and C are plant parameters.

A controller f is given as follows:

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

where $x_c(t) \in \mathbb{R}^{n_c}$ is a controller state, $v(t) \in \mathbb{R}^{m_c}$ is a controller input, which consists of sensor measurements and a reference, and A_c, B_c, C_c, and D_c are controller parameters. f can be rewritten as a product of a controller parameter matrix and a signal vector

$$\begin{aligned} &\psi(t) = \Phi\xi(t) =: f(\Phi, \xi(t)), \\ &\psi(t) := \begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix}, \ \Phi := \begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix}, \ \xi(t) := \begin{bmatrix} x_c(t) \\ v(t) \end{bmatrix}. \end{aligned}$$

The ElGamal cryptosystem allows multiplication to be the only calculation in the ciphertext. Thus, summation cannot be conducted in the ciphertext. f cannot be executed in ciphertext because a product of a matrix and a vector contains multiplication and summation. To avoid this problem, we divide f into $f^\times$ and f^+ as follows [5]:

$$\begin{aligned} &f = f^+ \circ f^\times, \\ &f^\times : ((\Phi_{ij}), (\xi_j)) \mapsto (\Phi_{ij}\xi_j) =: \Psi, \\ &f^+ : (\Psi_{ij}) \mapsto \left(\Sigma_j \Psi_{ij}\right) = \psi\,. \end{aligned}$$

$f^\times$ performs only element-wise multiplication of a matrix and vector, not adding up each row. Thus, we can execute $f^\times$ in the ciphertext.

Definition 3: Let C_Φ, $C_\xi(t)$, and $C_\Psi(t)$ be ciphertexts of Φ, $\xi(t)$, and $\Psi(t)$ at time $t \in \mathbb{Z}^+$, respectively. Suppose a controller f is given as $f = f^+ \circ f^\times$ [5], and ε is modified to $\varepsilon^\star = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}^+, \mathsf{Ecd}_\gamma, \mathsf{Dcd}_\gamma)$, where Ecd_γ and Dcd_γ are an encoder and decoder, respectively [22]. Then,

$$\begin{aligned} &\mathsf{Ecd}_\gamma : \mathbb{R} \ni x \mapsto \check{x} = \lceil \gamma x + \alpha(\gamma x) \rfloor \in \mathscr{M}, \\ &\alpha(\gamma x) := \begin{cases} p, & \gamma x < 0, \\ 0, & \gamma x \geq 0, \end{cases} \\ &\mathsf{Dcd}_\gamma : \mathscr{M} \ni \check{x} \mapsto \bar{x} = \frac{\check{x} - \beta(\check{x})}{\gamma} \in \mathbb{Q}, \\ &\beta(\check{x}) := \begin{cases} p, & \check{x} > q, \\ 0, & \check{x} \leq q, \end{cases} \end{aligned}$$

$\gamma \in \mathbb{R}$ is a scaling parameter, $\lceil \cdot \rfloor$ is a function, which rounds to the nearest element in $\mathscr{M}$, and $\mathsf{Dec}^+ = f^+ \circ \mathsf{Dec}$. Then, an encrypted controller $f^\times_{\varepsilon^\star}$ is defined as follows:

$$f^\times_{\varepsilon^\star} : (C_\Phi, C_\xi(t)) \mapsto C_\Psi(t) = (C_{\Phi_{ij}} * C_{\xi_j}(t) \bmod p),$$

where

$$\begin{aligned} (\mathsf{pk}, \mathsf{sk}) &= \mathsf{Gen}(p), \\ C_\Phi &= \mathsf{Enc}(\mathsf{Ecd}_{\gamma_c}(\Phi), \mathsf{pk}), \\ C_\xi(t) &= \mathsf{Enc}(\mathsf{Ecd}_{\gamma_p}(\xi(t)), \mathsf{pk}), \\ \bar{\psi}(t) &= \mathsf{Dcd}_{\gamma_c \times \gamma_p}(\mathsf{Dec}^+(C_\Psi(t), \mathsf{sk})), \end{aligned}$$

and for a vector or matrix, Enc, Dec, Ecd_γ, and Dcd_γ perform element-wise operations.

Remark 1: In encrypted control systems, the following homomorphism holds:

$$\begin{aligned} &\mathsf{Dec}(\mathsf{Enc}(\mathsf{Ecd}_{\gamma_c}(\Phi), \mathsf{pk}) * \mathsf{Enc}(\mathsf{Ecd}_{\gamma_p}(\xi(t)), \mathsf{pk}) \bmod p, \mathsf{sk}) \\ &= f^\times(\mathsf{Ecd}_{\gamma_c}(\Phi), \mathsf{Ecd}_{\gamma_p}(\xi(t)))\,. \end{aligned}$$

Remark 2: An encoder and decoder are essential for controller encryption because control systems address real numbers, while the ElGamal cryptosystem can be applied to only a subset of integers. Note that $\mathsf{Dcd}_\gamma(\mathsf{Dec}(\mathsf{Enc}(\mathsf{Ecd}_\gamma(x), \mathsf{pk}), \mathsf{sk}))$ is not equal to x, and

$$\begin{aligned} \mathsf{Dcd}_\gamma(\mathsf{Dec}(\mathsf{Enc}(\mathsf{Ecd}_\gamma(x), \mathsf{pk}), \mathsf{sk})) &= \mathsf{Dcd}_\gamma(\mathsf{Ecd}_\gamma(x)), \\ &= \frac{\lceil \gamma x + \alpha(\gamma x) \rfloor - \beta(\check{x})}{\gamma}, \\ &= \frac{\gamma x + \alpha(\gamma x) + \delta - \beta(\check{x})}{\gamma}, \\ &= x + \frac{\delta}{\gamma}, \end{aligned}$$

where δ/γ is the quantisation error. Quantisation errors are critical for control systems because these errors may destabilise control systems or degrade the control performance [14]. In this regard, the following result was revealed [23].

Proposition 3: Let e and k be quantisation errors caused by encryption and key length, respectively. Then, $e \to 0$ as $k \to \infty$.

This proposition claims that quantisation errors can be ignored when the key length is sufficiently large, while the conventional encrypted control systems cannot achieve asymptotic stability as long as the key length is finite. After this, we denote quantisation error of x as $\tilde{x} = \mathsf{Dcd}_\gamma(\mathsf{Ecd}_\gamma(x)) - x$ for convenience.

3 Dynamic ElGamal cryptosystem

Definition 4: Dynamic ElGamal cryptosystem $\varepsilon_{\mathrm{dyn}}(t)$ at time t is a tuple

$$\varepsilon_{\mathrm{dyn}}(t) := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, T_{\mathscr{K}}, T_{\mathscr{C}}),$$

where $T_{\mathscr{K}}$ and $T_{\mathscr{C}}$ are transition maps

$$\begin{aligned} &T_{\mathscr{K}} : ((\mathbb{G}, q, g, h), s) \mapsto ((\mathbb{G}, q, g, hg^{w(t)} \bmod p), s + w(t) \bmod q), \\ &T_{\mathscr{C}} : (c_1, c_2) \mapsto (c_1, c_1^{w(t)} c_2 \bmod p), \end{aligned}$$

and $w(t) \sim \mathscr{U}(\mathbb{Z}_q)$.

Corollary 1: The codomains of $T_{\mathscr{K}}$ and $T_{\mathscr{C}}$ are $\mathscr{K}$ and $\mathscr{C}$, respectively.

Proof: From the definition, $h, c_2, g^{w(t)} \bmod p, c_1^{w(t)} \bmod p \in \mathbb{G}$. Therefore, $hg^{w(t)} \bmod p \in \mathbb{G}$ and $c_1^{w(t)}c_2 \bmod p \in \mathbb{G}$. Additionally, $s + w(t) \bmod q \in \mathbb{Z}_q$ because $\mathbb{Z}_q$ is a group with respect to addition modulo q. □

Theorem 1: Let $\mathsf{pk}(t)$ and $\mathsf{sk}(t)$ be a public key and secret key at time t, respectively. If $(\mathsf{pk}(0), \mathsf{sk}(0)) = \mathsf{Gen}(p)$ with a safe prime p and $(\mathsf{pk}(t+1), \mathsf{sk}(t+1)) = T_{\mathscr{K}}(\mathsf{pk}(t), \mathsf{sk}(t))$, then

$$\begin{aligned}&\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(t)), \mathsf{sk}(t))\\ &= \mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(t+1)), \mathsf{sk}(t+1)),\ \forall t \in \mathbb{Z}^+.\end{aligned} \tag{1}$$

Proof: We prove the proposition through mathematical induction. When $t = 0$

$$\begin{aligned}\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(0)), \mathsf{sk}(0)) &= c_1^{-s(0)}c_2 \bmod p,\\ &= g^{-rs(0)}m(h(0))^r \bmod p,\\ &= g^{-rs(0)}mg^{rs(0)} \bmod p,\\ &= m.\end{aligned}$$

Assume that $\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(t)), \mathsf{sk}(t)) = m$. Then

$$\begin{aligned}&\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(t+1)), \mathsf{sk}(t+1))\\ &= c_1^{-s(t+1)}c_2 \bmod p,\\ &= g^{-rs(t+1)}m(h(t+1))^r \bmod p,\\ &= g^{-r(s(t)+w(t))}m(h(t)g^{w(t)})^r \bmod p,\\ &= g^{-rs(t)}g^{-rw(t)}mg^{rs(t)}g^{rw(t)} \bmod p,\\ &= m.\end{aligned}$$

Therefore, (1) holds for all $t \in \mathbb{Z}^+$. □

Corollary 2: If $(\mathsf{pk}(t+1), \mathsf{sk}(t+1)) = T_{\mathscr{K}}(\mathsf{pk}(t), \mathsf{sk}(t))$ for all $t \in \mathbb{Z}^+$, then $\mathsf{sk}(t)$ follows a discrete uniform distribution

$$\mathsf{sk}(t) \sim \mathscr{U}(\mathbb{Z}_q). \tag{2}$$

Proof: $\mathbb{Z}_q$ is a group with respect to addition modulo q. Define $T_s: w(t) \mapsto s(t) + w(t) \bmod q$. For $s(t), s'(t), w(t) \in \mathbb{Z}_q$, if $s(t) + w(t) = s'(t) + w(t) \bmod q$, then

$$\begin{aligned}s(t) + w(t) + (q - w(t)) &= s'(t) + w(t) + (q - w(t)) \bmod q,\\ s(t) + q &= s'(t) + q \bmod q,\\ s(t) &= s'(t) \bmod q.\end{aligned}$$

Thus, T_s is bijective. Therefore, if $w(t) \sim \mathscr{U}(\mathbb{Z}_q)$, then $s(t) + w(t) \bmod q \sim \mathscr{U}(\mathbb{Z}_q)$. □

Theorem 2: Let $C(t)$ be a ciphertext at time t. Suppose $C(0) = \mathsf{Enc}(m, \mathsf{pk}(0))$, $C(t+1) = T_{\mathscr{C}}(C(t))$, $(\mathsf{pk}(0), \mathsf{sk}(0)) = \mathsf{Gen}(p)$, and $(\mathsf{pk}(t+1), \mathsf{sk}(t+1)) = T_{\mathscr{K}}(\mathsf{pk}(t), \mathsf{sk}(t))$. Then

$$\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}(t)), \mathsf{sk}(t)) = \mathsf{Dec}(C(t), \mathsf{sk}(t)),\ \forall t \in \mathbb{Z}^+. \tag{3}$$

Proof: From Theorem 1, if $\mathsf{Dec}(C(t), \mathsf{sk}(t)) = m$ for all $t \in \mathbb{Z}^+$, then the proposition is true

$$\begin{aligned}&\mathsf{Dec}(C(t), \mathsf{sk}(t))\\ &= c_1^{-s(t)}c_2(t) \bmod p,\\ &= c_1^{-s(t)}c_1^{w(t-1)}c_2(t-1) \bmod p,\\ &= g^{-rs(t)}g^{rw(t-1)}m(h(t-1))^r \bmod p,\\ &= g^{-r(s(t-1)+w(t-1))}g^{rw(t-1)}mg^{rs(t-1)} \bmod p,\\ &= m.\end{aligned}$$

□

Lemma 1: $\mathbb{G}$ is isomorphic to $\mathbb{Z}_q$.

Proof: We prove that there exists an isomorphism from $\mathbb{Z}_q$ to $\mathbb{G}$. From Lagrange's theorem, $|\mathbb{G}| = q$. Define the map $\phi: \mathbb{Z}_q \ni x \mapsto g^x \bmod p \in \mathbb{G}$. Then, ϕ is bijective. Additionally, for $a, b \in \mathbb{Z}_q$,

$$\phi(a+b) = g^{a+b} \bmod p = g^a g^b \bmod p = \phi(a)\phi(b).$$

Therefore, ϕ is an isomorphism. □

Corollary 3: If $C(t+1) = T_{\mathscr{C}}(C(t))$ for all $t \in \mathbb{Z}^+$, then $c_2(t)$ follows a discrete uniform distribution

$$c_2(t) \sim \mathscr{U}(\mathbb{G}). \tag{4}$$

Proof: From Lemma 1, $T_{\mathscr{C}}$ can be a bijection from $w(t)$ to $c_1^{w(t)}c_2 \bmod p$. Therefore, if $w(t) \sim \mathscr{U}(\mathbb{Z}_q)$, then $c_2(t) \sim \mathscr{U}(\mathbb{G})$. □

Corollary 4: $\varepsilon_{\mathrm{dyn}}(t)$ holds multiplicative homomorphism

$$\begin{aligned}&\mathsf{Dec}(\mathsf{Enc}(m_1, \mathsf{pk}(t)) * \mathsf{Enc}(m_2, \mathsf{pk}(t)) \bmod p, \mathsf{sk}(t))\\ &= m_1 m_2,\ \forall t \in \mathbb{Z}^+.\end{aligned}$$

Proof: From Theorem 1, Proposition 1 holds for all $t \in \mathbb{Z}^+$. □

Remark 3: We use the same random number $w(t)$ to update key pairs and ciphertexts of controller parameters. Thus, in practice, we have to share $w(t)$ securely or use an identical random number generator with the same seed. In this paper, we focus on the proposed cryptosystem's properties from the control-theoretic viewpoint under the assumption that $w(t)$ is appropriately shared.

4 Encrypted control system with dynamic ElGamal cryptosystem

This section describes the main result of this study. The proposed encrypted controller with the dynamic ElGamal cryptosystem achieves asymptotic stability. Furthermore, key pairs and ciphertexts of controller parameters are updated at every sampling period. Thus, the security level of the proposed encrypted control system may be higher than that of the conventional one.

A state-feedback controller is one of the basic controllers and determines control inputs as $u(t) = Fx(t)$. In this case, we can interpret that $\Phi = F$, $\xi(t) = x(t)$, and $\psi(t) = u(t)$. Two lemmas on a quantised state-feedback controller, which were discussed in our previous conference paper [22], should be introduced before we present the main result. The lemmas give the method of choosing a scaling parameter for the encoder/decoder to achieve asymptotic stability.

Note that in encrypted control systems, a state-feedback gain is quantised as well as a plant state because the cryptosystem can handle only an element of $\mathbb{G}$. A closed-loop system with a quantised state-feedback gain is not necessarily stable even if an original state-feedback gain stabilises a plant. Therefore, we must choose proper encoder/decoder scaling parameters for the state-feedback gain and state, respectively.

Lemma 2: Let $d_{\max}$ be the maximum width of $\mathscr{M}$. Let $\bar{F} = \mathsf{Dcd}_{\gamma_c}(\mathsf{Ecd}_{\gamma_c}(F))$ be a quantised state-feedback gain. Assume that $A + BF$ is a Schur matrix [22], and $u(t) = \bar{F}x(t)$. If γ_c satisfies

$$\begin{aligned}&\left|\gamma_c\right| > \frac{1}{\Omega(P,Q)}d_{\max},\\ &\Omega(P,Q) := \frac{2}{\sqrt{mn}\parallel B^{\top}PB \parallel}\Big(-\parallel (A+BF)^{\top}PB \parallel\\ &\quad + \sqrt{\parallel (A+BF)^{\top}PB \parallel^2 + \lambda_{\min}(Q)\parallel B^{\top}PB \parallel}\Big),\end{aligned}$$

for a given matrix $Q = Q^\top > 0$ and the corresponding matrix $P = P^\top > 0$ satisfying $(A+BF)^\top P(A+BF) - P = -Q$, then $A + B\tilde{F}$ is a Schur matrix.

Proof: From the assumption, the closed-loop system with the quantised state-feedback gain is given as follows:

$$x(t+1) = Ax(t) + B\bar{F}x(t) = (A+BF)x(t) + B\tilde{F}x(t),$$

and there exists $P = P^\top > 0$ for any $Q = Q^\top > 0$ such that

$$(A+BF)^\top P(A+BF) - P = -Q.$$

Let $V(x,t) = x^\top(t)Px(t)$ be a Lyapunov function candidate. Then

$$\begin{aligned}
&V(x,t+1) - V(x,t)\\
&= ((A+BF)x + B\tilde{F}x)^\top P((A+BF)x + B\tilde{F}x) - x^\top Px,\\
&= ((A+BF)x + B\tilde{F}x)^\top P((A+BF)x + B\tilde{F}x)\\
&\quad -x^\top((A+BF)^\top P(A+BF) + Q)x,\\
&= x^\top(A+BF)^\top PB\tilde{F}x + x^\top\tilde{F}^\top B^\top P(A+BF)x\\
&\quad +x^\top\tilde{F}^\top B^\top PB\tilde{F}x - x^\top Qx,\\
&\le \| B^\top PB \| \, \| x \|^2 \, \| \tilde{F} \|^2 + 2 \| (A+BF)^\top PB \| \, \| x \|^2 \, \| \tilde{F} \|\\
&\quad -\lambda_{\min}(Q) \| x \|^2 .
\end{aligned}$$

By using the notations

$$\begin{aligned}
a &:= \| B^\top PB \| \, \| x \|^2,\\
b &:= 2 \| (A+BF)^\top PB \| \, \| x \|^2,\\
c &:= -\lambda_{\min}(Q) \| x \|^2,
\end{aligned}$$

the solution for the quadratic equation $a \| \tilde{F} \|^2 + b \| \tilde{F} \| + c = 0$ is given as follows:

$$\begin{aligned}
\| \tilde{F} \| &= \frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right),\\
&= \frac{1}{\| B^\top PB \|}\Big(- \| (A+BF)^\top PB \|\\
&\quad +\sqrt{\| (A+BF)^\top PB \|^2 + \lambda_{\min}(Q) \| B^\top PB \|}\Big).
\end{aligned}$$

Therefore, $V(x,t+1) - V(x,t)$ is negative when γ_c satisfies the abovementioned condition because $\tilde{F}$ is bounded from above as follows [22]:

$$\| \tilde{F} \| \le \frac{\sqrt{mn}}{2} \frac{d_{\max}}{|\gamma_c|}.$$

A system matrix is a Schur matrix if the difference value of a Lyapunov function is negative for all $t \in \mathbb{Z}^+$. □

Lemma 3: Let $d_{\max}$ be the maximum width of $\mathscr{M}$. Let $\bar{F} = \mathsf{Dcd}_{\gamma_c}(\mathsf{Ecd}_{\gamma_c}(F))$ and $\bar{x}(t) = \mathsf{Dcd}_{\gamma_p(t)}(\mathsf{Ecd}_{\gamma_p(t)}(x(t)))$ be a quantised state-feedback gain and quantised state, respectively. Assume that $A + BF$ is a Schur matrix, and $u(t) = \bar{F}\bar{x}(t)$. If γ_c satisfies Lemma 2 and $\gamma_p(t)$ satisfies

$$\begin{aligned}
&\left|\gamma_p(t)\right| > \frac{\Theta(\bar{P},\bar{Q})}{\| x(t) \|} d_{\max},\\
&\Theta(\bar{P},\bar{Q}) := \frac{\sqrt{n}}{2\lambda_{\min}(\bar{Q})}\Big(\| (A+B\bar{F})^\top \bar{P}B\bar{F} \|\\
&\quad +\sqrt{\| (A+B\bar{F})^\top \bar{P}B\bar{F} \|^2 + \lambda_{\min}(\bar{Q}) \| \bar{F}^\top B^\top \bar{P}B\bar{F} \|}\Big),
\end{aligned}$$

for a given matrix $\bar{Q} = \bar{Q}^\top > 0$ and the corresponding matrix $\bar{P} = \bar{P}^\top > 0$ satisfying $(A+B\bar{F})^\top \bar{P}(A+B\bar{F}) - \bar{P} = -\bar{Q}$, then the closed-loop system achieves asymptotic stability [22].

Proof: From Lemma 2, we can choose γ_c such that $A + B\bar{F}$ becomes a Schur matrix. Then, the closed-loop system with the quantised state-feedback gain and quantised state is given as follows:

$$x(t+1) = Ax(t) + B\bar{F}\tilde{x}(t) = (A+B\bar{F})x(t) + B\bar{F}\tilde{x}(t),$$

and there exists $\bar{P} = \bar{P}^\top > 0$ for any $\bar{Q} = \bar{Q}^\top > 0$ such that

$$(A+B\bar{F})^\top \bar{P}(A+B\bar{F}) - \bar{P} = -\bar{Q}.$$

Let $V(x,t) = x^\top(t)\bar{P}x(t)$ be a Lyapunov function candidate. Then

$$\begin{aligned}
&V(x,t+1) - V(x,t)\\
&= ((A+B\bar{F})x + B\bar{F}\tilde{x})^\top \bar{P}((A+B\bar{F})x + B\bar{F}\tilde{x}) - x^\top \bar{P}x,\\
&= ((A+B\bar{F})x + B\bar{F}\tilde{x})^\top \bar{P}((A+B\bar{F})x + B\bar{F}\tilde{x})\\
&\quad -x^\top((A+B\bar{F})^\top \bar{P}(A+B\bar{F}) + \bar{Q})x,\\
&= x^\top(A+B\bar{F})^\top \bar{P}B\bar{F}\tilde{x} + \tilde{x}^\top\bar{F}^\top B^\top \bar{P}(A+B\bar{F})x\\
&\quad +\tilde{x}^\top\bar{F}^\top B^\top \bar{P}B\bar{F}\tilde{x} - x^\top\bar{Q}x,\\
&\le -\lambda_{\min}(\bar{Q}) \| x \|^2 + \| (A+B\bar{F})^\top \bar{P}B\bar{F} \| \, \| \tilde{x} \| \, \| x \|\\
&\quad + \| \bar{F}^\top B^\top \bar{P}B\bar{F} \| \, \| \tilde{x} \|^2 .
\end{aligned}$$

By using the notations

$$\begin{aligned}
a &:= -\lambda_{\min}(\bar{Q}),\\
b &:= \| (A+B\bar{F})^\top \bar{P}B\bar{F} \| \, \| \tilde{x} \|,\\
c &:= \| \bar{F}^\top B^\top \bar{P}B\bar{F} \| \, \| \tilde{x} \|^2,
\end{aligned}$$

the solution for the quadratic equation $a \| x \|^2 + b \| x \| + c = 0$ is given as follows:

$$\begin{aligned}
\| x \| &= \frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right),\\
&= \frac{\| \tilde{x} \|}{\lambda_{\min}(Q)}\Big(\| (A+B\bar{F})^\top \bar{P}B\bar{F} \|\\
&\quad +\sqrt{\| (A+B\bar{F})^\top \bar{P}B\bar{F} \|^2 + \lambda_{\min}(\bar{Q}) \| \bar{F}^\top B^\top \bar{P}B\bar{F} \|}\Big).
\end{aligned}$$

Therefore, $V(x,t+1) - V(x,t)$ is negative outside the ball

$$\left\{ x \,\middle|\, \| x \| \le \frac{\Theta(\bar{P},\bar{Q})}{\left|\gamma_p(t)\right|} d_{\max} \right\}.$$

Furthermore, the closed-loop system is Lyapunov stable when $\gamma_p(t)$ satisfies the abovementioned condition. Define $\Delta(t+1) := \left|\gamma_p(t+1)\right|^{-1} - \left|\gamma_p(t)\right|^{-1}$. Then, $\Delta(t) < 0$ because the closed-loop system is Lyapunov stable. Therefore, $\left|\gamma_p(t)\right|^{-1} \to 0$ and $\| x(t) \| \to 0$ as $t \to \infty$. □

Theorem 3: Let $C_F(t)$, $C_x(t)$, and $C_\Psi(t)$ be ciphertexts of F, $x(t)$, and $\Psi(t)$ at time $t \in \mathbb{Z}^+$, respectively. Suppose a state-feedback controller f is given as $f = f^+ \circ f^\times$ such that a closed-loop system is asymptotically stable, and $\varepsilon_{\mathrm{dyn}}(t)$ is modified to $\varepsilon^\star_{\mathrm{dyn}}(t) := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}^+, T_{\mathscr{K}}, T_{\mathscr{C}}, \mathsf{Ecd}_{\gamma(t)}, \mathsf{Dcd}_{\gamma(t)})$. Then, there exists the following encrypted state-feedback controller that achieves asymptotic stability while concealing a state-feedback gain F, plant state $x(t)$, and control input $u(t)$ with dynamic key pairs $(\mathsf{pk}(t), \mathsf{sk}(t))$:

$$f^{\times}_{\varepsilon^{\star}_{\mathrm{dyn}}(t)}\colon (C_F(t), C_x(t)) \mapsto C_\Psi(t) = (C_{F_{ij}}(t) * C_{x_j}(t) \bmod p),$$

where

$$\begin{aligned}
(\mathsf{pk}(0), \mathsf{sk}(0)) &= \mathsf{Gen}(p),\\
C_F(0) &= \mathsf{Enc}(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{pk}(0)),\\
(\mathsf{pk}(t+1), \mathsf{sk}(t+1)) &= T_{\mathscr{K}}(\mathsf{pk}(t), \mathsf{sk}(t)),\\
C_F(t+1) &= T_{\mathscr{E}}(C_F(t)),\\
C_x(t) &= \mathsf{Enc}(\mathsf{Ecd}_{\gamma_p(t)}(x(t)), \mathsf{pk}(t)),\\
u(t) &= \mathsf{Dcd}_{\gamma_c\times\gamma_p(t)}(\mathsf{Dec}^{+}(C_\Psi(t), \mathsf{sk}(t))),\\
\gamma_c &= \frac{1}{\Omega(P,Q)}\, d_{\max} + \mu_c,\\
\gamma_p(t) &= \frac{\Theta(\bar{P},\bar{Q})}{\parallel x(t) \parallel}\, d_{\max} + \mu_p,
\end{aligned}$$

$d_{\max}$ is the maximum width of $\mathscr{M}$, Q, and $\bar{Q}$ are any positive definite matrices, P and $\bar{P}$ are the corresponding matrices for Q and $\bar{Q}$, respectively, and $\mu_c > 0$ and $\mu_p > 0$ are design parameters.

Proof: An encrypted state-feedback controller with $\varepsilon^{\star}_{\mathrm{dyn}}(t)$ can be transformed as follows:

$$\begin{aligned}
&\mathsf{Dcd}_{\gamma_c\times\gamma_p(t)}(\mathsf{Dec}^{+}(\mathsf{Enc}(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{pk}(t))\\
&\quad * \mathsf{Enc}(\mathsf{Ecd}_{\gamma_p(t)}(x(t)), \mathsf{pk}(t)) \bmod p, \mathsf{sk}(t)))\\
&= \mathsf{Dcd}_{\gamma_c\times\gamma_p(t)}(f^{+}(f^{\times}(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{Ecd}_{\gamma_p(t)}(x(t))))),\\
&= \mathsf{Dcd}_{\gamma_c\times\gamma_p(t)}(f(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{Ecd}_{\gamma_p(t)}(x(t)))),\\
&= f(\bar{F}, \bar{x}(t)),\\
&= \bar{F}\bar{x}(t)\,.
\end{aligned}$$

Then, the closed-loop system with the encrypted state-feedback controller is given as follows:

$$x(t+1) = Ax(t) + B\bar{F}\bar{x}(t)\,.$$

This closed-loop system is the same as the system discussed in Lemma 3. Therefore, the closed-loop system with the encrypted state-feedback controller achieves asymptotic stability when γ_c and $\gamma_p(t)$ satisfy Lemmas 2 and 3, respectively. □

Remark 4: In encrypted state-feedback control systems, the following homomorphism holds:

$$\begin{aligned}
&\mathsf{Dec}(\mathsf{Enc}(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{pk}(t)) * \mathsf{Enc}(\mathsf{Ecd}_{\gamma_p(t)}(x(t)), \mathsf{pk}(t)) \bmod p, \mathsf{sk}(t))\\
&= f^{\times}(\mathsf{Ecd}_{\gamma_c}(F), \mathsf{Ecd}_{\gamma_p(t)}(x(t)))\,.
\end{aligned}$$

Remark 5: $\mathscr{M}$ is a finite set. Therefore, μ_c and μ_p should be chosen such that encoded values do not overflow or underflow [22].

Remark 6: In general, not all elements of $x(t)$ are directly observable. Thus, we should use an observer [24]. Theorem 3 should be extended to consider an observer state when we use an observer unless a plant state can be approximated sufficiently to the observer state.

Fig. 2 shows a flow of the proposed encrypted state-feedback control system with $\varepsilon^{\star}_{\mathrm{dyn}}(t)$.

5 Numerical simulation

Consider the following continuous-time plant:

$$\begin{aligned}
\dot{x}(\tau) &= \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} x(\tau) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(\tau),\\
y(\tau) &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x(\tau),
\end{aligned}$$

where τ is continuous time. This plant is discretised as follows:

$$\begin{aligned}
x(t+1) &= \begin{bmatrix} 1.01005 & -0.01015 \\ 0 & 1.02020 \end{bmatrix} x(t) + \begin{bmatrix} -5.05029\times10^{-5} \\ 1.01007\times10^{-2} \end{bmatrix} u(t),\\
y(t) &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x(t),
\end{aligned}$$

where the sampling period is set to be 10 ms. The following state-feedback gain is employed:

$$F = \begin{bmatrix} 6.57458 & -6.20107 \end{bmatrix}.$$

We select $p = 1,128,503$, and then the key pair at initial time $t = 0$ is given as follows:

$$\begin{aligned}
&\mathsf{pk}(0) = (\{1, \ldots, 1,128,498\}, 564,251,\ 2,\ 1,004,992),\\
&\mathsf{sk}(0) = 97,859.
\end{aligned}$$

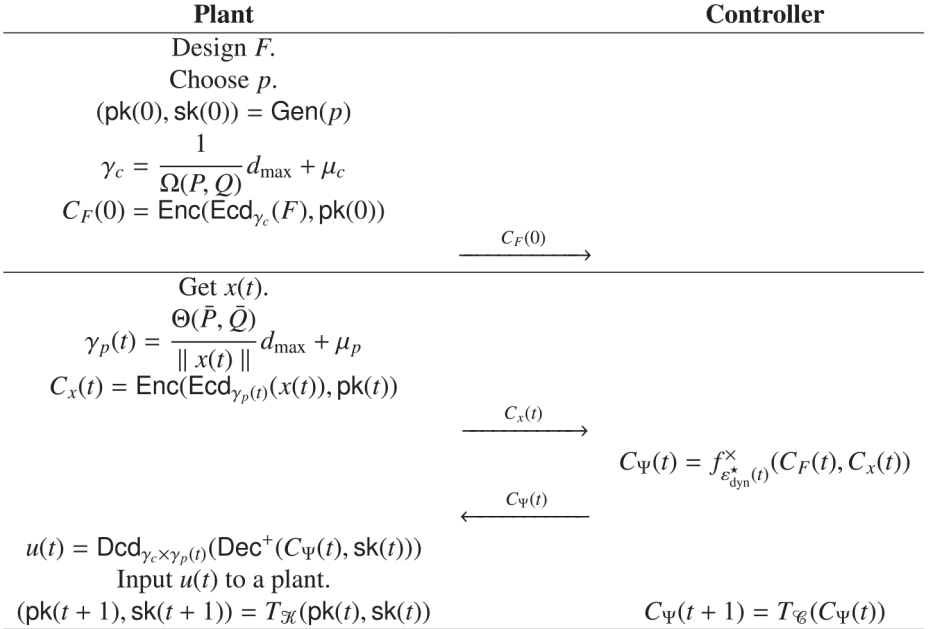

Fig. 2 *Flow of encrypted state-feedback control with dynamic ElGamal cryptosystem*

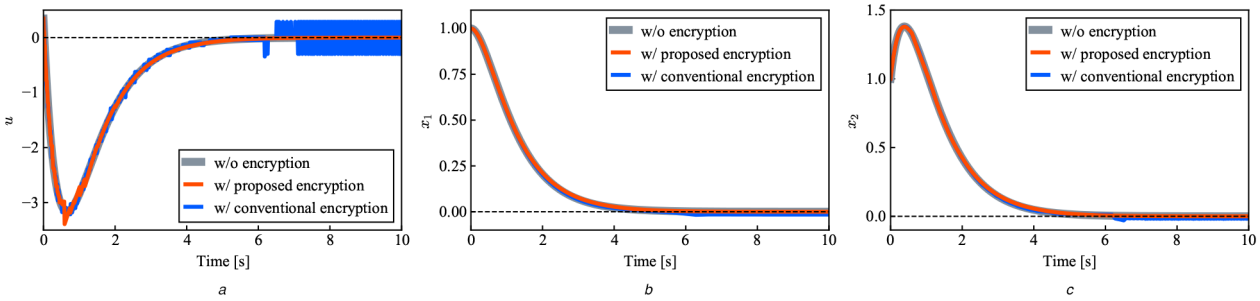

Fig. 3 *Comparison of signals between an encrypted control system with the conventional cryptosystem and that with the proposed one*
(a) Control input, ***(b)*** First element of state, ***(c)*** Second element of state

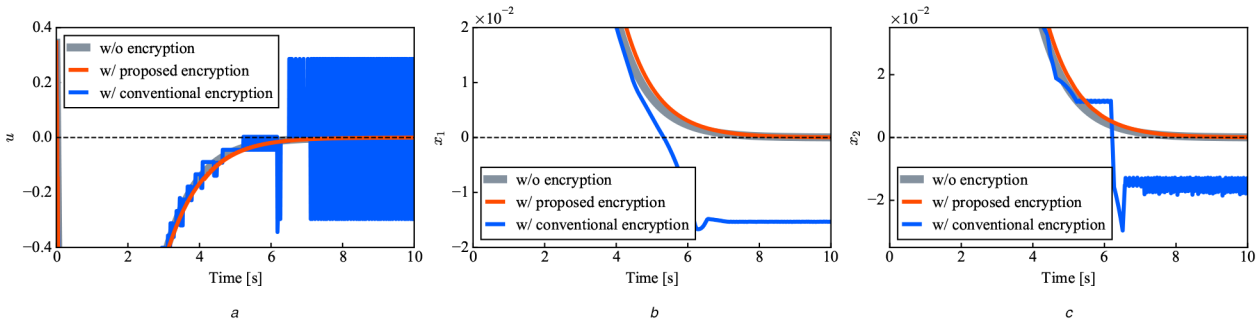

Fig. 4 *Enlarged graphs of Fig. 3*
(a) Control input, ***(b)*** First element of state, ***(c)*** Second element of state

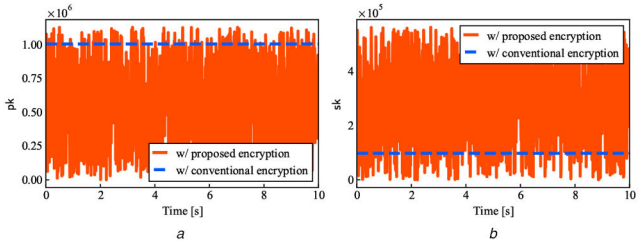

Fig. 5 *Comparison of key pairs between an encrypted control system with the conventional cryptosystem and that with the proposed one*
(a) Public key, ***(b)*** Secret key

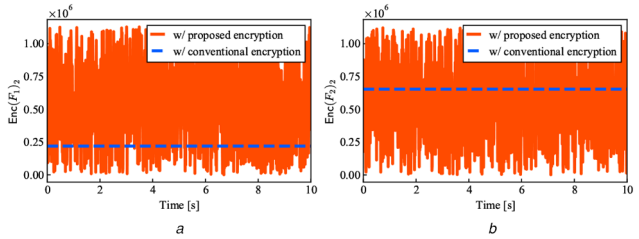

Fig. 6 *Comparison of ciphertexts of the state-feedback gain between an encrypted control system with the conventional cryptosystem and that with the proposed one*
(a) First element of controller gain in ciphertext, ***(b)*** Second element of controller gain in ciphertext

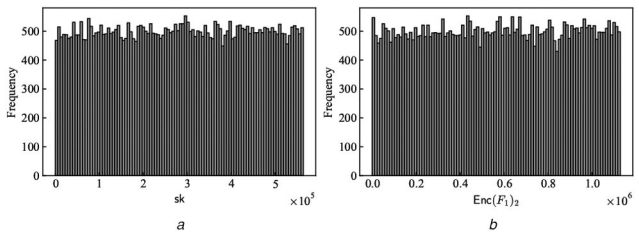

Fig. 7 *Histograms of secret key and ciphertext in the proposed cryptosystem within 0 to 500 s (*number of bins = 100*)*
(a) Histogram of secret key, ***(b)*** Histogram of first element of controller gain in ciphertext

Furthermore, the scaling parameters are given as follows:

$$\gamma_c = 20.28758, \quad \gamma_p(0) = 130.44016,$$

where $Q = \bar{Q} = \mathrm{diag}(1, 1)$, $\mu_c = \mu_p = 0.01$, and $d_{\max} = 19$.

Fig. 3 shows the results of encrypted state-feedback control with the conventional ElGamal cryptosystem ε and the proposed dynamic ElGamal cryptosystem $\varepsilon^{\star}_{\mathrm{dyn}}(t)$. Fig. 4 is the enlarged graph of Fig. 3. Figs. 5 and 6 show sequences of keypair and ciphertext of controller gain.

Figs. 4*b* and *c* demonstrate the encrypted controller with the dynamic encoder and decoder achieves asymptotic stability. Figs. 5 and 6 demonstrate that the key pair and ciphertext of controller gain in the conventional ElGamal cryptosystem each keep their initial values. In contrast, those in the proposed dynamic ElGamal cryptosystem are randomly updated at every time step. Furthermore, Fig. 7 shows histograms of the secret key and ciphertext in the proposed encrypted control system for 500 s. It can be said that the secret key and ciphertext in the proposed cryptosystem follow a discrete uniform distribution because the distributions of the histograms are almost flat.

6 Experimental verification

6.1 Experimental testbed

The testbed shown in Fig. 8 consists of a DC motor, a table operated by the DC motor through a belt with a pulley, a rotary encoder to measure the position of the table, and two Raspberry Pi3s that are connected via an ethernet cable. The DC motor is driven by a motor driver with its input and output as voltages. The operating system of the Raspberry Pi3s is Raspbian with Xenomai. One of the Raspberry Pi3s is for processing on the encrypted controller, and the other is for encrypting, decrypting, reading sensors, and inputting control commands to the DC motor. The Raspberry Pi3s communicate with TCP/IP. See [25] for specifications of the testbed.

A model of the testbed is obtained by system identification as follows:

$$A = \begin{bmatrix} 0.99984 & -0.00089 \\ 0 & 0.39985 \end{bmatrix}, \; B = \begin{bmatrix} 0.03624 \\ 4.42333 \end{bmatrix}, \; C = [0.17778 \quad 0],$$

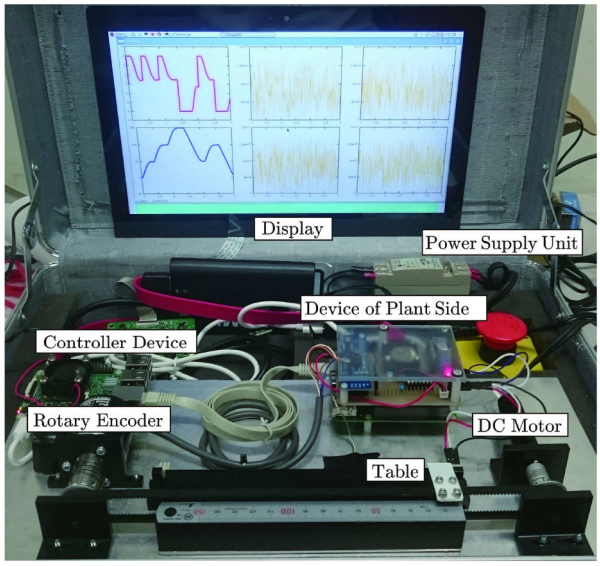

Fig. 8 *Experimental testbed [25]*

where the input is a voltage to the motor driver, the output is a position of the table, and the sampling period is set to be 10 ms.

6.2 Controller design

In this study, we use a regulator that is a basic controller in the field of control engineering. An observer for P is given as follows:

$$\hat{x}(t+1) = A\hat{x}(t) + Bu(t) + L(y(t) - \hat{y}(t)),$$

where $\hat{x}(t) \in \mathbb{R}^n$ is an estimated state, $\hat{y}(t) = C\hat{x}(t) \in \mathbb{R}^l$ is an estimated output, and $L \in \mathbb{R}^{n\times l}$ is an observer gain.

Then, a regulator is given as follows:

$$\begin{cases} \hat{x}(t+1) = (A + BF - LC)\hat{x}(t) + Ly(t), \\ u(t) = F\hat{x}(t), \end{cases}$$

where F is state-feedback gain. In this case, the elements of Φ and $\xi(t)$ are given as follows:

$$A_c = A + BF - LC, \quad B_c = L, \quad C_c = F, \quad D_c = O,$$
$$x_c(t) = \hat{x}(t), \quad v(t) = y(t).$$

For simplicity of regulator design, we use the discrete-time linear quadratic regulator problem [26] with the cost function

$$J = \sum_{t=0}^{\infty} (x(t)^\top Q x(t) + u(t)^\top R u(t)),$$

where Q is a state weight, and R is an input weight. The state weights for the observer and controller are, respectively, set to be

$$Q_o = \mathrm{diag}(1,1), \quad Q_c = \mathrm{diag}(1,1),$$

and the input weights are set to be

$$R_o = 1, \quad R_c = 1.$$

Then, L and F are designed as follows:

$$L = \begin{bmatrix} 0.91423 \\ -0.00004 \end{bmatrix}, \quad F = \begin{bmatrix} -0.21067 & -0.08517 \end{bmatrix}.$$

The controller parameter Φ of the regulator is given as follows:

$$\Phi = \begin{bmatrix} A + BF - LC & L \\ F & O \end{bmatrix} = \begin{bmatrix} 0.82969 & -0.00398 & 0.91423 \\ -0.93186 & 0.02311 & -0.00004 \\ -0.21067 & -0.08517 & 0 \end{bmatrix}.$$

Then, an encrypted parameter with a 33-bit key at initial time $t = 0$ is given as follows:

$$C_\Phi(0) = \left(\begin{bmatrix} \texttt{158D57DA2} & \texttt{9A053022} & \texttt{6E9FF885} \\ \texttt{100071917} & \texttt{1EDF60174} & \texttt{69DC9B2F} \\ \texttt{1C564BB44} & \texttt{10EC81D5C} & \texttt{6017DDE2} \end{bmatrix}, \begin{bmatrix} \texttt{173E5ECBF} & \texttt{109542ED3} & \texttt{141B148E6} \\ \texttt{2061B8FB} & \texttt{F28330DB} & \texttt{12CF7EDDC} \\ \texttt{1558F4EAE} & \texttt{1C5568353} & \texttt{F48DF955} \end{bmatrix} \right),$$

where the elements of $C_\Phi(0)$ are displayed as hexadecimal numbers.

6.3 Signals, controller parameters, and key pairs

Figs. 9*a* and *b* demonstrate the results of regulation control, and Figs. 10*a* and *b* are the second element of ciphertexts of control input and output, respectively. Fig. 9*c* shows the transition of $\gamma_p(t)$ at this time. These results confirm that the encrypted controller conceals the signals over network links, and the scaling parameter is tuned with the signals. Fig. 10*c* demonstrates the transition of a second element of the $(2,2)$ entry of controller parameter in the ciphertext. Figs. 11*a* and *b* show the transitions of the public key and secret key, respectively. These results confirm that key pairs and ciphertexts are updated randomly. From the above, adversaries cannot obtain a time series of input/output data and controller parameters if they do not solve a discrete logarithm problem at every sampling period.

6.4 Static and dynamic encoder/decoder

An encrypted controller with a static encoder and decoder cannot achieve asymptotic stability, while that with a dynamic one can achieve asymptotic stability. In this subsection, the effect of dynamic encoder and decoder is examined.

Figs. 12*a* and *b* show the control input and output of encrypted control systems with a static or dynamic encoder/decoder in the same control of Section 6.3, respectively. Figs. 12*c* and *d* are enlarged graphs of Figs. 12*a* and *b*, respectively. These results show that a steady-state error of an encrypted control system with a dynamic encoder/decoder is small in comparison with that of static

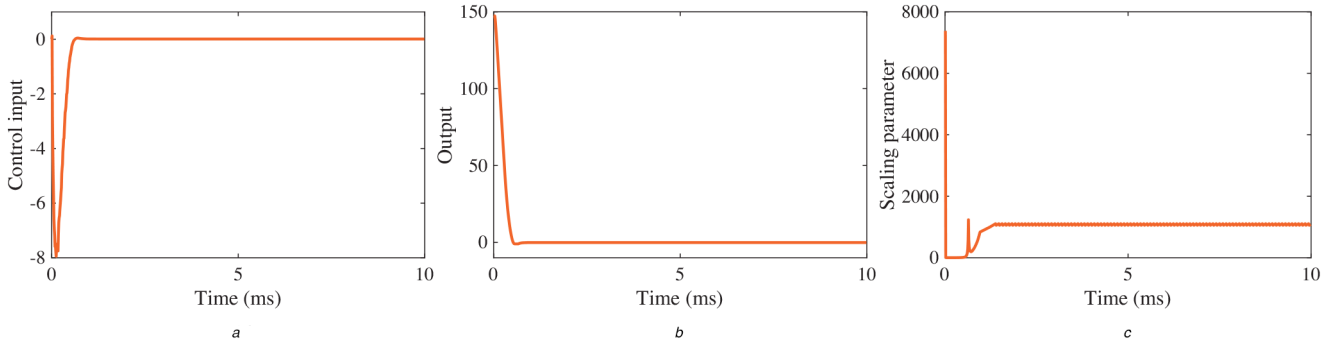

Fig. 9 *Signals and scaling parameter*
(a) Control input, ***(b)*** Output, ***(c)*** Scaling parameter for signals

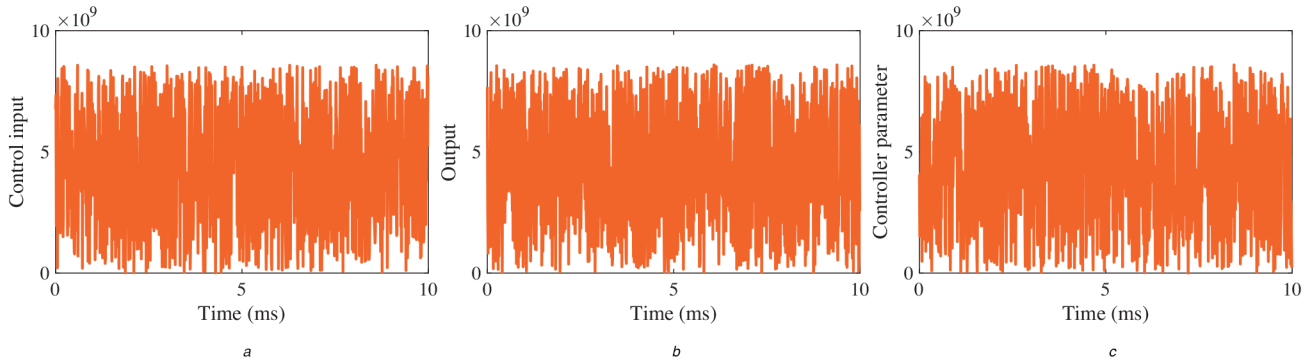

Fig. 10 *Signals and controller parameter in ciphertext*
(a) Control input in ciphertext, ***(b)*** Output in ciphertext, ***(c)*** Controller parameter in ciphertext

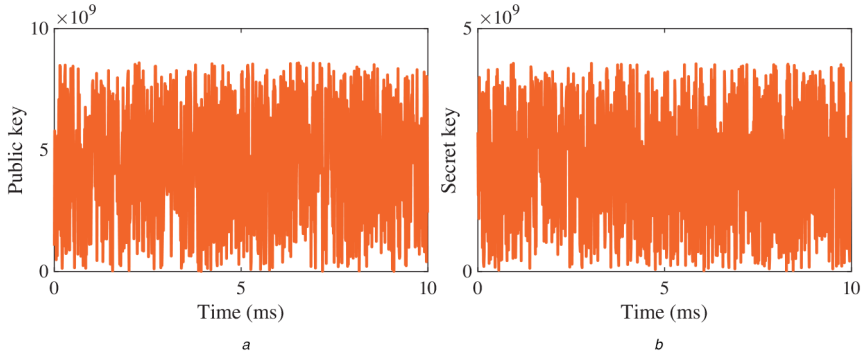

Fig. 11 *Key pairs*
(a) Public key, ***(b)*** Secret key

ones. Thus, it is confirmed that a dynamic encoder/decoder improves the control performance of encrypted control systems, while the output of the encrypted control system with a dynamic encoder/decoder does not perfectly converge to zero. This result may be caused by a non-linearity such as friction.

6.5 Processing time

Control operation must be completed within a sampling period because behaviour and stability are not guaranteed if processing time is more than the sampling period. In this subsection, the processing time of the proposed encrypted control system is investigated.

Table 1 shows the maximum, mean, and minimum processing times of the proposed encrypted control system in the experiment of Section 6.3. The results confirm that the processes of the proposed encrypted control system finished within the sampling period, and the system operates in real-time. However, the processing time of the encrypted control system is exponentially increased with key length [27]. Therefore, we conjecture that the selection of key length is a critical issue for the proposed cryptosystem as well as for conventional ones.

7 Conclusion

This study proposed a novel ElGamal-based dynamic multiplicative homomorphic cryptosystem with a dynamic encoder and decoder for encrypted control systems. Key pairs and ciphertexts are updated randomly at every sampling period, and an encrypted state-feedback controller with the proposed cryptosystem achieves asymptotic stability. The feasibility of the proposed encrypted control system was examined through several experiments with the positioning table testbed. The experimental results confirmed that key pairs, controller parameters, and signals are concealed against adversaries. Furthermore, it was shown to improve the control performance of encrypted control systems by using a dynamic encoder and decoder.

In this paper, we did not discuss the decision problem of proper or optimal key length. The key length should be chosen by considering the trade-off between security level and computational latency; however, the security index of encrypted control systems has not yet been established. We considered the dynamic cryptosystem methodology and its properties from the control-theoretic perspective rather than information security, and thus, the proposed cryptosystem requires security proof so that the security level of it is evaluated quantitatively. Moreover, the proposed method may be secure for information leakage, such as leakage of

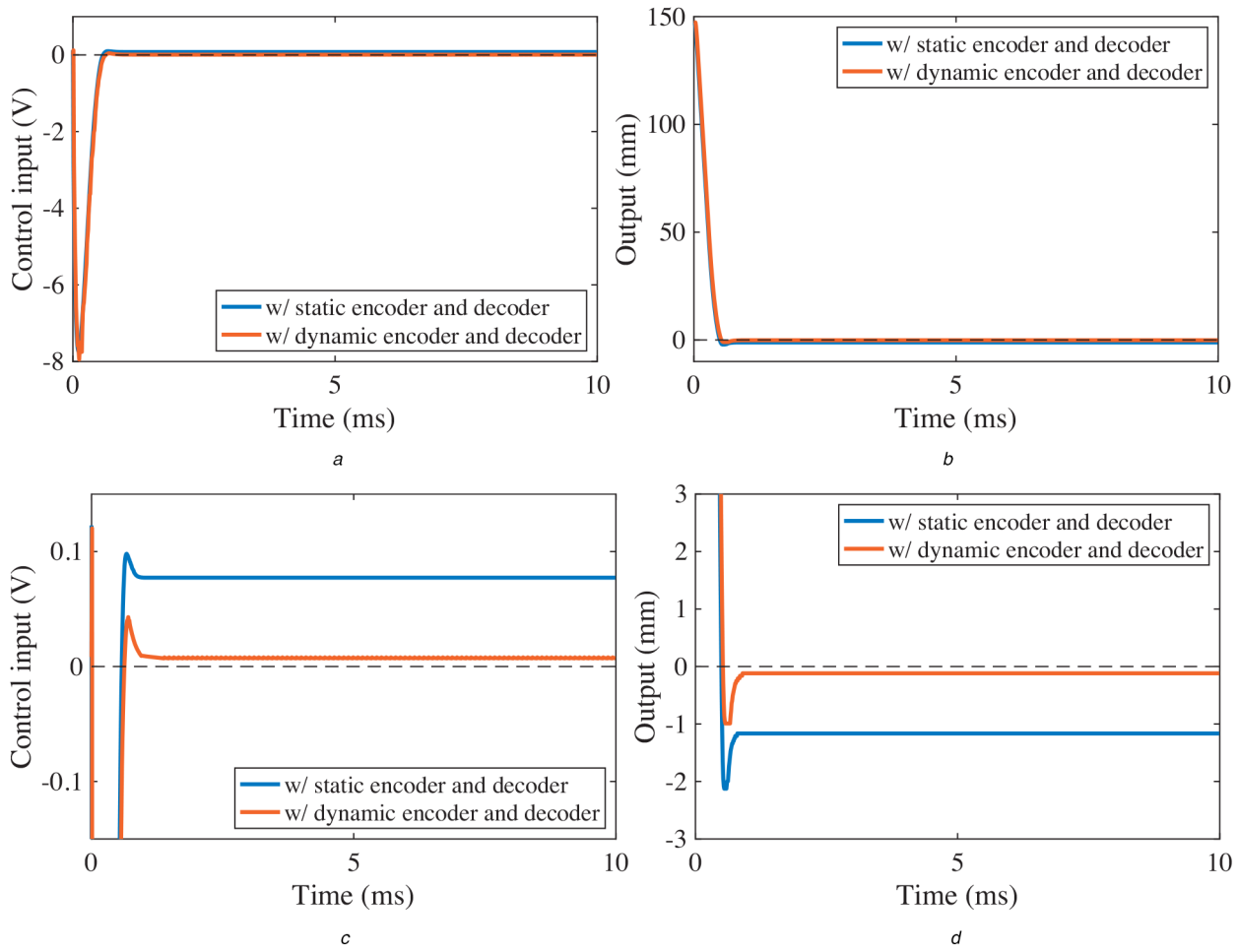

Fig. 12 *Comparison between an encrypted control system with a static encoder/decoder and that with a dynamic one*
(a) Control input, ***(b)*** Output, ***(c)*** Enlarged graph of (a), ***(d)*** Enlarged graph of (b)

Table 1 Processing time

Max	Mean	Min
4.4931 ms	3.9674 ms	3.3684 ms

a secret key at a certain time, and adversaries may not be able to estimate a secret key from the previous/following one. We plan to address these issues in future work.

Encrypted control under network constraints, such as transmission channel noises [28, 29] and packet dropouts [30], is also an open issue. We must give a theoretical foundation for implementing encrypted control systems using actual networks. The network constraints in encrypted control systems may be addressed as with those in unencrypted control systems because a closed-loop system with an encrypted controller is the same as an unencrypted closed-loop system. Encrypted model predictive control is one of the schemes expected to be effective for encrypted control under constraints [31, 32].

Additionally, we will modify the proposed cryptosystem not to use the same random number for updating key pairs and ciphertexts of controller parameters. We will also analyse the resilience of the proposed cryptosystem against major cyber-attacks and consider the proposed cryptosystem in terms of information security.

8 Acknowledgments

The authors express their gratitude to Mr. Masahiro Kusaka, a PhD student at the University of Electro-Communications, who conducted practical verification of the proposed method.

9 References

[1] Teixeira, A., Shames, I., Sandberg, H., *et al.*: 'A secure control framework for resource-limited adversaries', *Automatica*, 2015, **51**, pp. 135–148
[2] Mo, Y., Sinopoli, B.: 'Secure control against replay attacks'. Annual Allerton Conf. on Communication, Control, and Computing, Monticello, IL, 2009, pp. 911–918
[3] Pasqualetti, F., Dörfler, F., Bullo, F.: 'Attack detection and identification in cyber-physical systems', *IEEE Trans. Autom. Control*, 2013, **58**, (11), pp. 2715–2729
[4] Yuan, Y., Yuan, H., Guo, L., *et al.*: 'Resilient control of networked control system under DoS attacks: a unified game approach', *IEEE Trans. Ind. Inf.*, 2016, **12**, (5), pp. 1786–1794
[5] Kogiso, K., Fujita, T.: 'Cyber-security enhancement of networked control systems using homomorphic encryption'. IEEE Conf. on Decision and Control, Osaka, 2015, pp. 6836–6843
[6] Rivest, R.L., Shamir, A., Adleman, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, (2), pp. 120–126
[7] Elgamal, T.: 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Inf. Theory*, 1985, **31**, (4), pp. 469–472
[8] Kogiso, K.: 'Attack detection and prevention for encrypted control systems by application of switching-key management'. IEEE Conf. on Decision and Control, Miami Beach, FL, 2018, pp. 5032–5037
[9] Baba, R., Kogiso, K., Kishida, M.: 'Detection method of controller falsification attacks against encrypted control system'. SICE Annual Conf., Nara, 2018, pp. 244–248
[10] Sandberg, H., Amin, S., Johansson, K.H.: 'Cyberphysical security in networked control systems: an introduction to the issue', *IEEE Control Syst. Mag.*, 2015, **35**, (1), pp. 20–23
[11] Paillier, P.: 'Public-key cryptosystems based on composite degree residuosity classes'. Advances in Cryptology (EUROCRYPT' 99), Berlin, Heidelberg, 1999, pp. 223–238
[12] Farokhi, F., Shames, I., Batterham, N.: 'Secure and private control using semi-homomorphic encryption', *Control Eng. Pract.*, 2017, **67**, pp. 13–20
[13] Kishida, M.: 'Encrypted control system with quantiser', *IET Control Theory Applic.*, 2019, **13**, (1), pp. 146–151
[14] Brockett, R.W., Liberzon, D.: 'Quantized feedback stabilization of linear systems', *IEEE Trans. Autom. Control*, 2000, **45**, (7), pp. 1279–1289
[15] Gentry, C. (2009). 'A fully homomorphic encryption scheme'. PhD thesis, Stanford University. Stanford, CA, USA

[16] Kim, J., Lee, C., Shim, H., *et al.*: 'Encrypting controller using fully homomorphic encryption for security of cyber-physical systems', *IFAC-PapersOnLine*, 2016, **49**, (22), pp. 175–180
[17] Cheon, J.H., Han, K., Kim, H., *et al.*: 'Need for controllers having integer coefficients in homomorphically encrypted dynamic system'. IEEE Conf. on Decision and Control, Miami Beach, FL, 2018, pp. 5020–5025
[18] Shannon, C.E.: 'Communication theory of secrecy systems', *Bell Syst. Techn. J.*, 1949, **28**, (4), pp. 656–715
[19] Blaze, M., Bleumer, G., Strauss, M.: 'Divertible protocols and atomic proxy cryptography'. Advances in Cryptology (EUROCRYPT '98), Berlin, Heidelberg, 1998, pp. 127–144
[20] Ivan, A., Dodis, Y.: 'Proxy cryptography revisited'. Network and Distributed System Security Symp., San Diego, CA, 2003
[21] Dodis, Y., Katz, J., Xu, S., *et al.*: 'Key-insulated public key cryptosystems'. Advances in Cryptology (EUROCRYPT 2002), Berlin, Heidelberg, 2002, pp. 65–82
[22] Teranishi, K., Shimada, N., Kogiso, K.: 'Stability analysis and dynamic quantizer for controller encryption'. IEEE Conf. on Decision and Control, Nice, 2019, pp. 7184–7189
[23] Kogiso, K.: 'Upper-bound analysis of performance degradation in encrypted control system'. Annual American Control Conf., Milwaukee, WI, 2018, pp. 1250–1255
[24] Luenberger, D.: 'An introduction to observers', *IEEE Trans. Autom. Control*, 1971, **16**, (6), pp. 596–602
[25] Kogiso, K., Baba, R., Kusaka, M.: 'Development and examination of encrypted control systems'. IEEE/ASME Int. Conf. on Advanced Intelligent Mechatronics, Auckland, 2018, pp. 1338–1343
[26] Dorato, P., Levis, A.: 'Optimal linear regulators: the discrete-time case', *IEEE Trans. Autom. Control*, 1971, **16**, (6), pp. 613–620
[27] Teranishi, K., Kusaka, M., Shimada, N., *et al.*: 'Secure observer-based motion control based on controller encryption'. Annual American Control Conf., Philadelphia, PA, 2019, pp. 2978–2983
[28] Zhu, Y., Zheng, W.X., Zhou, D.: 'Quasi-synchronization of discrete-time Lur'e-type switched systems with parameter mismatches and relaxed PDT constraints', *IEEE Trans. Cybern.*, 2020, **50**, (5), pp. 2026–2037
[29] Zhang, L., Zhuang, S., Shi, P., *et al.*: 'Uniform tube based stabilization of switched linear systems with mode-dependent persistent dwell-time', *IEEE Trans. Autom. Control*, 2015, **60**, (11), pp. 2994–2999
[30] Zhu, Y., Zhong, Z., Zheng, W.X., *et al.*: 'HMM-based $\mathscr{H}_\infty$ filtering for discrete-time markov jump LPV systems over unreliable communication channels', *IEEE Trans. Syst.*, 2018, **48**, (12), pp. 2035–2046
[31] Darup, M.S., Redder, A., Quevedo, D.E.: 'Encrypted cloud-based MPC for linear systems with input constraints', *IFAC-PapersOnLine*, 2018, **51**, (20), pp. 535–542
[32] Darup, M.S., Redder, A., Shames, I., *et al.*: 'Towards encrypted MPC for linear constrained systems', *IEEE Control Syst. Lett.*, 2018, **2**, (2), pp. 195–200