ElGamal-type encryption for optimal dynamic quantizer in encrypted control systems

doi: 10.1080/18824889.2021.1906016

SICE Journal of Control, Measurement, and System Integration, Vol. 0, No. 0, pp. 001–007, xxx 2006

ElGamal-type Encryption for Optimal Dynamic Quantizer in Encrypted Control Systems

Kaoru TERANISHI * and Kiminao KOGISO *

Abstract : This study considers a quantizer design problem with controller encryption for minimizing performance degradation caused by encryption. It is difficult to design an optimal dynamic quantizer that converts real numbers to plaintexts for encrypted control systems with ElGamal encryption because the plaintext space of ElGamal encryption is intermittent and does not include zero and negative numbers. A variant of ElGamal encryption is proposed to apply a conventional optimal dynamic quantizer for encrypted control systems. The proposed multiplicative homomorphic cryptosystem, wherein the plaintext space is consecutive integers within a certain range, can handle zero and negative integers properly. Numerical simulations demonstrate that the optimal dynamic quantizer with the proposed cryptosystem improves the control performance of an encrypted regulator.

Key Words : cyber-security, encrypted control, homomorphic encryption, dynamic quantizer.

1. Introduction

Threats against control systems are essential concerns in recent years [1]–[3]. Encrypted control [4] is expected to improve the cyber-security of control systems because it reduces the risks of eavesdropping attacks, which are the main class of attacks for control systems [2]. This attack is performed for collecting information about a targeted control system to execute more severe attacks such as replay attacks [5]. In encrypted control systems, control inputs are directly determined using encrypted data without decryption, and thus, it effectively prevents eavesdropping attacks.

Encrypted control with multiplicative homomorphic encryption, such as RSA [6] and ElGamal encryption [7], was proposed in [4]. Not only signals over network links but also controller parameters are concealed by encryption. Encrypted control with additive homomorphic encryption, such as Paillier encryption [8], was studied in [9]. In this encrypted control scheme, either signals or controller gains are encrypted. Encrypted control with fully homomorphic encryption was provided in [10]. Additive and fully homomorphic encryption require higher computational costs than multiplicative homomorphic encryption; therefore, multiplicative homomorphic encryption would be most suitable for encrypting control systems. Furthermore, a detection method for falsification attacks and replay attacks based on encrypted control with multiplicative homomorphic encryption was introduced in [11], [13].

For designing encrypted control systems, controller parameters and signals should be quantized. This quantization may cause a degradation of stability and control performance [12]. Several studies were conducted to avoid destabilization by encryption. The authors of [9] introduced a binary number representation for quantization in encrypted control. This method is suitable for implementing encrypted control systems with additive homomorphic encryption on digital computers. The quantization approach of [14] was applied for an encrypted state-feedback controller with Paillier encryption to achieve asymptotic stability [16]. The quantization approach for average consensus control, event-triggered control, and control of nonlinear scalar systems were also considered [15],[16]. The authors of [17] proposed a dynamic quantizer for encrypted control systems with ElGamal encryption. The dynamic quantizer guarantees that a closed-loop system with an encrypted state-feedback controller inherits the asymptotic stability of an unencrypted closed-loop system. Furthermore, encrypted event-triggered control with the dynamic quantizer was studied [18].

Previous studies on quantization in encrypted control systems focused only on guaranteeing the stability of a control system after encryption. Despite the criticality of control performance as well as stability in control systems, the conventional quantization methods do not consider the control performance of encrypted control systems. Minimizing the degradation of control performance caused by the quantization and estimating the degree of performance degradation before control systems operation is meaningful for the efficient design of encrypted control systems and performance guarantee. Therefore, we consider the following problem.

Problem 1. Given a multiplicative homomorphic encryption scheme and a controller stabilizing a plant, assume that there exists an encrypted controller such that a closed-loop system with the plant is stable. Design a quantizer to minimize the maximum error between the output of the unencrypted control system and an encrypted control system and determine the maximum error.

Azuma and Sugie's dynamic quantizer [19] may be considered a solution to the above problem. Their dynamic quantizer is a general form of $\Delta\Sigma$ modulator consisting of a uniform mid-tread quantizer, which rounds off an argument to the nearest neighbor of a discrete output set, and a quantizer state updated based on a quantization error. The dynamic quantizer mini-

* Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Chofu, Tokyo, Japan
E-mail: teranishi@uec.ac.jp, kogiso@uec.ac.jp
(Received xxx 00, 0000)
(Revised xxx 00, 0000)

mizes the maximum quantization error within the scope of using the simple quantizer structure. Additionally, the maximum error is explicitly determined simultaneously with the quantizer design.

Despite a number of merits of the dynamic quantizer, applying it to encrypted control systems is not straightforward because, in general, a plaintext space of multiplicative homomorphic encryption does not include zero and negative numbers. Numbers not included in a plaintext space cannot be encrypted, and thus, we can handle only positive numbers as long as conventional multiplicative homomorphic encryption is used. Furthermore, using ElGamal encryption, a plaintext space is intermittent. The dynamic quantizer guarantees optimality only when the output set of the quantizer is uniform. Note that a naive variable transformation, such as adding a number to an argument to shift non-positive numbers to positive numbers, cannot be applied to convert a real number and plaintext because an identity element is not preserved before and after the transformation. Besides, in principle, zero cannot be considered in a plaintext space of conventional multiplicative homomorphic encryption no matter what a variable transformation is used since a multiplication between zero and any number is always zero.

We propose a variant of ElGamal encryption using encoding and decoding maps, converting real numbers and plaintexts to each other to apply Azuma and Sugie's dynamic quantizer for encrypted control systems. The proposed cryptosystem can appropriately handle zero and negative numbers while preserving multiplicative homomorphism. Additionally, a plaintext space of the proposed encryption scheme can be regarded as consecutive integers through the encoding and decoding maps. Thus, the dynamic quantizer in encrypted control systems with the variant achieves optimal performance. Numerical examples confirm that the proposed scheme improves control performance compared to one in a case with the normal ElGamal cryptosystem.

The remainder of this paper is organized as follows. Section 2 summarizes the preliminaries of number theory, cryptography, and encrypted control. Section 3 describes the proposed encryption scheme with encoding and decoding maps to implement an optimal dynamic quantizer. Section 4 introduces an optimal dynamic quantizer in encrypted control systems using the proposed cryptosystem. Section 5 provides the results of numerical simulation demonstrating the validity of the proposed method. Finally, Section 6 describes the conclusions and future work.

2. Preliminaries

2.1 Notation

The sets of real numbers, integers, primes, security parameters, key pairs, public keys, secret keys, plaintexts, and ciphertexts are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{P}$, $\mathcal{S}$, $\mathcal{K}$, $\mathcal{K}_\mathsf{p}$, $\mathcal{K}_\mathsf{s}$, $\mathcal{M}$, and $\mathcal{C}$, respectively. We define sets $\mathbb{R}^+ \coloneqq \{x \in \mathbb{R} \mid 0 \leq x\}$, $\mathbb{Z}^+ \coloneqq \{z \in \mathbb{Z} \mid 0 \leq z\}$, $\mathbb{Z}_n \coloneqq \{z \in \mathbb{Z} \mid 0 \leq z < n\}$, and $\mathfrak{P}_a^b \coloneqq \{a^i \bmod b \mid i \in \mathbb{Z}_b\}$. 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}. For $a, b \in \mathbb{Z}$, we use $a \mid b$ if a divides b; otherwise, we use $a \nmid b$. The floor function is defined as $\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z} : x \mapsto \max\{z \in \mathbb{Z} \mid z \leq x\}$. The identity map on a set A is denoted by id_A.

Definition 1. The minimal residue of an integer a modulo m is defined as

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

where $b = a \bmod m$.

Definition 2. An integer a is called as a quadratic residue modulo m if there exists an integer b such that $b^2 = a \bmod m$. We use Gauss's notation, i.e., we use $a \,\mathbf{R}\, m$ if a is a quadratic residue modulo m; otherwise, we use $a \,\mathbf{N}\, m$.

Definition 3. The Legendre symbol is a map from $\mathbb{Z} \times (\mathbb{P} \setminus \{2\})$ to $\{-1, 0, 1\}$ defined as

$$\left(\frac{z}{p}\right)_L : (z, p) \mapsto z^{\frac{p-1}{2}} \operatorname{Mod} p = \begin{cases} 0, & p \mid z, \\ 1, & z \,\mathbf{R}\, p \wedge p \nmid z, \\ -1, & z \,\mathbf{N}\, p \wedge p \nmid z. \end{cases}$$

2.2 ElGamal encryption

ElGamal encryption is a tuple $\mathcal{E} \coloneqq (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, where $\mathsf{Gen} : \mathcal{S} \to \mathcal{K} = \mathcal{K}_\mathsf{p} \times \mathcal{K}_\mathsf{s} : k \mapsto (\mathsf{pk}, \mathsf{sk}) = ((p, q, g, h), s)$ is a key generation algorithm, $\mathsf{Enc} : \mathcal{K}_\mathsf{p} \times \mathcal{M} \to \mathcal{C} : (\mathsf{pk}, m) \mapsto c = (g^r \bmod p, mh^r \bmod p)$ is an encryption algorithm, $\mathsf{Dec} : \mathcal{K}_\mathsf{s} \times \mathcal{C} \to \mathcal{M} : (\mathsf{sk}, (c_1, c_2)) \mapsto {c_1}^{-s} c_2 \bmod p$ is a decryption algorithm, pk is a public key, sk is a secret key, q is a k bit prime, $p = 2q + 1$ is a safe prime, g is a generator of a cyclic group $\mathbb{G} \coloneqq \{g^i \bmod p \mid i \in \mathbb{Z}_q\} = \mathcal{M} \subset \mathbb{Z}_p \setminus \{0\}$ such that $g^q \bmod p = 1$, $h = g^s \bmod p$, $\mathcal{C} = \mathbb{G}^2$, and r and s are random numbers in $\mathbb{Z}_q$. Enc and Dec perform elementwise operations for a vector and a matrix.

Remark 1. For $m, m' \in \mathcal{M}$, ElGamal encryption satisfies the following homomorphism:

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m) * \mathsf{Enc}(\mathsf{pk}, m') \bmod p) = mm' \bmod p,$$

where $*$ is the Hadamard product.

2.3 Encrypted Controller

A plant P and a controller f are given as follows:

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

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

where $t \in \mathbb{Z}^+$ is a time step, $x \in \mathbb{R}^n$ is a state, $u \in \mathbb{R}^m$ is an input, $y \in \mathbb{R}^l$ is an output, A, B, and C are plant parameters, $x_c \in \mathbb{R}^{n_c}$ is a controller state, and A_c, B_c, C_c, and D_c are controller parameters. f can be rewritten as $f : \mathbb{R}^{(n_c+m)\times(n_c+l)} \times \mathbb{R}^{n_c+l} \to \mathbb{R}^{n_c+m} : (\Phi, \xi(t)) \mapsto \psi(t)$, where

$$\psi(t) \coloneqq \begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix}, \ \Phi \coloneqq \begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix}, \ \xi(t) \coloneqq \begin{bmatrix} x_c(t) \\ y(t) \end{bmatrix}.$$

Definition 4. Given a controller f and multiplicative homomorphic encryption, such as ElGamal encryption $\mathcal{E}$,

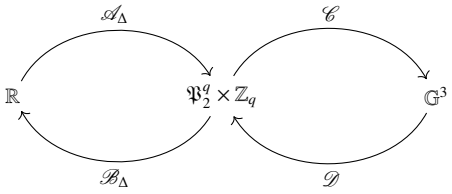


Fig. 1 Encoding and decoding maps.

$$f_{\mathsf{Enc}}^{\times} : \mathcal{C}^{(n_c+m)\times(n_c+l)} \times \mathcal{C}^{n_c+l} \to \mathcal{C}^{(n_c+m)\times(n_c+l)}$$

is called an encrypted controller [4] if it satisfies

$$\begin{aligned} f_{\mathsf{Enc}}^{\times}(\mathsf{Enc}(\check{\Phi}), \mathsf{Enc}(\check{\xi})) &= \mathsf{Enc}(\check{\Psi}), \\ \mathsf{Dec}^{+}(\mathsf{Enc}(\check{\Psi})) &= \check{\psi}, \end{aligned}$$

where f is divided as $f = f^{+} \circ f^{\times}$ [4],

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

$\mathsf{Dec}^{+} \coloneqq f^{+} \circ \mathsf{Dec}$, and $\check{\Phi}$, $\check{\xi}$, $\check{\Psi}$, and $\check{\psi}$ are plaintexts of Φ, ξ, Ψ, and ψ, respectively.

3. Variant of ElGamal Encryption

This section proposes a modified ElGamal encryption whose plaintext space has uniform width and contains zero and negative numbers. Our basic idea is based on the fact that $\mathbb{G}$ is a set of quadratic residue modulo p, and $(m/p)_L m$ can be used for encoding to $\mathbb{G}$ for all $m \in \mathbb{Z}_p \setminus \{0\}$ [20]. The proposed cryptosystem can be used to design an optimal dynamic quantizer for encrypted control systems.

Definition 5. We define encoding maps $\mathscr{A}_\Delta$ and $\mathscr{C}$, and decoding maps $\mathscr{B}_\Delta$ and $\mathscr{D}$ in Fig. 1 as

$$\begin{aligned} \mathscr{A}_\Delta &: \mathbb{R} \to \mathfrak{P}_2^q \times \mathbb{Z}_q \\ &: x \mapsto \begin{cases} (1, \lfloor |x|/\Delta + 1/2 \rfloor \bmod q), & x \geq 0, \\ (2, \lfloor |x|/\Delta + 1/2 \rfloor \bmod q), & x < 0, \end{cases} \\ \mathscr{B}_\Delta &: \mathfrak{P}_2^q \times \mathbb{Z}_q \to \mathbb{R} \\ &: (\zeta, z) \mapsto \left(\frac{\zeta}{3}\right)_L \Delta z, \\ \mathscr{C} &: \mathfrak{P}_2^q \times \mathbb{Z}_q \to \mathbb{G}^3 \\ &: (\zeta, z) \mapsto \begin{cases} \left(\left(\left(\frac{\zeta}{p}\right)_L \zeta, g, 1\right) \bmod p, & z = 0, \\ \left(\left(\left(\frac{\zeta}{p}\right)_L \zeta, 1, \left(\frac{z}{p}\right)_L z\right) \bmod p, & z \neq 0, \end{cases} \\ \mathscr{D} &: \mathbb{G}^3 \to \mathfrak{P}_2^q \times \mathbb{Z}_q \\ &: (\omega, \theta, m) \mapsto \begin{cases} (|\omega \bmod p|, |m \bmod p|), & \theta = 1, \\ (|\omega \bmod p|, 0), & \theta \neq 1, \end{cases} \end{aligned}$$

where $\Delta \in \mathbb{R}^{+} \setminus \{0\}$ is a resolution. For simplicity, we employ $\mathsf{Ecd}_\Delta \coloneqq \mathscr{C} \circ \mathscr{A}_\Delta$ and $\mathsf{Dcd}_\Delta \coloneqq \mathscr{B}_\Delta \circ \mathscr{D}$, which perform elementwise operations for a vector and a matrix.

Proposition 1. If $|x|/\Delta \in \mathbb{Z}_q$, then $\mathscr{B}_\Delta(\mathscr{A}_\Delta(x)) = x$.

Proof. Let $(\zeta, z) = \mathscr{A}_\Delta(x)$. Then, $z = |x|/\Delta$.

$$\begin{aligned} \mathscr{B}_\Delta(\mathscr{A}_\Delta(x)) &= \left(\frac{\zeta}{3}\right)_L \Delta|x|/\Delta, \\ &= \begin{cases} (1 \bmod 3) \times |x| = |x|, & x \geq 0, \\ (2 \bmod 3) \times |x| = -|x|, & x < 0, \end{cases} \\ &= x. \quad \square \end{aligned}$$

Remark 2. In practice, an error caused by $\mathscr{A}_\Delta$ and $\mathscr{B}_\Delta$ is bounded from above by $\Delta/2$, that is, $|\mathscr{B}_\Delta(\mathscr{A}_\Delta(x)) - x| \leq \Delta/2$. Therefore, the error converges to zero as Δ goes to zero.

Proposition 2. $\mathscr{D} \circ \mathscr{C} = \mathrm{id}_{\mathfrak{P}_2^q \times \mathbb{Z}_q}$.

Proof. Define maps $\alpha : (\mathbb{Z}_q \setminus \{0\}) \to \mathbb{G} : a \mapsto (a/p)_L a \bmod p$ and $\beta : \mathbb{G} \to (\mathbb{Z}_q \setminus \{0\}) : b \mapsto |b \bmod p|$. Let $y \in \mathbb{Z}_q$. If $(y/p)_L = 1$, then $\beta(\alpha(y)) = |y \bmod p| = |y| = y$. Similarly, if $(y/p)_L = -1$, then $\beta(\alpha(y)) = |p - y \bmod p| = |p - y - p| = y$. Thus, $\beta \circ \alpha = \mathrm{id}_{\mathbb{Z}_q \setminus \{0\}}$.

Let $(\zeta, z) \in \mathfrak{P}_2^q \times \mathbb{Z}_q$, and $(\omega, \theta, m) = \mathscr{C}(\zeta, z)$. If $z = 0$, then

$$\begin{aligned} \mathscr{D}(\mathscr{C}(\zeta, z)) &= \mathscr{D}((\zeta/p)_L \zeta \bmod p, g, 1), \\ &= \mathscr{D}(\alpha(\zeta), g, 1), \\ &= (\beta(\alpha(\zeta)), 0), \\ &= (\zeta, z). \end{aligned}$$

If $z \neq 0$, then

$$\begin{aligned} \mathscr{D}(\mathscr{C}(\zeta, z)) &= \mathscr{D}((\zeta/p)_L \zeta \bmod p, 1, (z/p)_L z \bmod p), \\ &= \mathscr{D}(\alpha(\zeta), 1, \alpha(z)), \\ &= (\beta(\alpha(\zeta)), \beta(\alpha(z))), \\ &= (\zeta, z). \quad \square \end{aligned}$$

Theorem 1. If $|x|/\Delta \in \mathbb{Z}_q$, then $\mathsf{Dcd}_\Delta(\mathsf{Ecd}_\Delta(x)) = x$.

Proof. The theorem follows from Propositions 1 and 2. $\square$

This theorem implies that the encoding and decoding maps convert an argument without loss of information when errors do not occur in $\mathscr{A}_\Delta$ and $\mathscr{B}_\Delta$.

Definition 6. We modify ElGamal encryption as $\mathcal{E}^{\dagger} \coloneqq (\mathsf{Gen}, \mathsf{Enc}^{\dagger}, \mathsf{Dec}^{\dagger})$:

$$\begin{aligned} \mathsf{Enc}^{\dagger} &: \mathcal{K}_{\mathsf{p}} \times \mathcal{M} \to \mathcal{C} \\ &: (\mathsf{pk}, (m_1, m_2, m_3)) \\ &\quad \mapsto (\mathsf{Enc}(\mathsf{pk}, m_1), \mathsf{Enc}(\mathsf{pk}, m_2), \mathsf{Enc}(\mathsf{pk}, m_3)), \\ \mathsf{Dec}^{\dagger} &: \mathcal{K}_{\mathsf{s}} \times \mathcal{C} \to \mathcal{M} \\ &: (\mathsf{sk}, (c_1, c_2, c_3)) \\ &\quad \mapsto (\mathsf{Dec}(\mathsf{sk}, c_1), \mathsf{Dec}(\mathsf{sk}, c_2), \mathsf{Dec}(\mathsf{sk}, c_3)), \end{aligned}$$

where $c_1, c_2, c_3 \in \mathbb{G}^2$, $\mathcal{M} = \mathbb{G}^3$, and $\mathcal{C} = \mathbb{G}^6$. $\mathsf{Enc}^{\dagger}$ and $\mathsf{Dec}^{\dagger}$ perform elementwise operations for a vector and a matrix. In the following, we omit pk and sk in the encryption and decryption algorithms for simplicity.

Remark 3. From Proposition 2, we can regard the plaintext space $\mathcal{M}$ as $\mathfrak{P}_2^q \times \mathbb{Z}_q$. $\mathfrak{P}_2^q$ and $\mathbb{Z}_q$ are involved with a sign and magnitude of plaintext, respectively. That is, the plaintext space can be treated as a set of consecutive integers. Although

this study considers using Azuma and Sugie's dynamic quantizer for quantization in encrypted control, the property of our proposed cryptosystem is also useful for other quantizers. For example, a logarithmic quantizer cannot be applied for quantization in encrypted control with the normal ElGamal cryptosystem because it is impossible to design a resolution to determine the quantizer's output set due to intermittence of a plaintext space of the encryption scheme. In contrast, a plaintext space of our cryptosystem is consecutive. Therefore, we can easily design a logarithmic quantizer resolution for encrypted control by using the cryptosystem.

Theorem 2. Let $|x|/\Delta, |x'|/\Delta' \in \mathbb{Z}_q$. If $|xx'|/(\Delta\Delta') \in \mathbb{Z}_q$, then $\mathcal{E}^\dagger$ satisfies the following homomorphism:

$$\begin{aligned}&\mathsf{Dcd}_{\Delta\Delta'}(\mathsf{Dec}^\dagger(\mathsf{Enc}^\dagger(\mathsf{Ecd}_\Delta(x)) * \mathsf{Enc}^\dagger(\mathsf{Ecd}_{\Delta'}(x')) \bmod p))\\ &= xx'.\end{aligned}$$

Proof. Let $(\zeta, z) = \mathscr{A}_\Delta(x)$, $(\zeta', z') = \mathscr{A}_{\Delta'}(x')$, $(\omega, \theta, m) = \mathscr{C}(\zeta, z)$, $(\omega', \theta', m') = \mathscr{C}(\zeta', z')$, $c = \mathsf{Enc}^\dagger(\omega, \theta, m)$, and $c' = \mathsf{Enc}^\dagger(\omega', \theta', m')$. Then, $z = |x|/\Delta$ and $z' = |x'|/\Delta'$.

(i) $z = 0 \wedge z' \neq 0 \iff x = 0 \wedge x' \neq 0$

$$\begin{aligned}&\mathsf{Dcd}_{\Delta\Delta'}(\mathsf{Dec}^\dagger(c * c' \bmod p))\\ &= \mathsf{Dcd}_{\Delta\Delta'}(\omega\omega' \bmod p, g, m'),\\ &= \mathscr{B}_{\Delta\Delta'}(1, 0),\\ &= \left(\frac{1}{3}\right)_L \Delta\Delta' \times 0,\\ &= 0.\end{aligned}$$

(ii) $(z/p)_L = 1 \wedge (z'/p)_L = 1$

$$\begin{aligned}&\mathsf{Dcd}_{\Delta\Delta'}(\mathsf{Dec}^\dagger(c * c' \bmod p))\\ &= \mathsf{Dcd}_{\Delta\Delta'}(\omega\omega' \bmod p, 1, zz' \bmod p),\\ &= \mathscr{B}_{\Delta\Delta'}(\zeta\zeta', zz'),\\ &= \left(\frac{\zeta\zeta'}{3}\right)_L \Delta\Delta'|x||x'|/(\Delta\Delta'),\\ &= \left(\frac{\zeta\zeta'}{3}\right)_L |x||x'|,\\ &= \begin{cases}(2^0 \bmod 3) \times |xx'| = |xx'|,\\ \quad \text{for } x \geq 0 \wedge x' \geq 0,\\ (2^1 \bmod 3) \times |xx'| = -|xx'|,\\ \quad \text{for } (x \geq 0 \wedge x' < 0) \vee (x < 0 \wedge x' \geq 0),\\ (2^2 \bmod 3) \times |xx'| = |xx'|,\\ \quad \text{for } x < 0 \wedge x' < 0,\end{cases}\\ &= xx'.\end{aligned}$$

(iii) $(z/p)_L = -1 \wedge (z'/p)_L = 1$

$$\begin{aligned}&\mathsf{Dcd}_{\Delta\Delta'}(\mathsf{Dec}^\dagger(c * c' \bmod p))\\ &= \mathsf{Dcd}_{\Delta\Delta'}(\omega\omega' \bmod p, 1, (p - z)z' \bmod p),\\ &= \mathscr{B}_{\Delta\Delta'}(\zeta\zeta', |p - zz' - p|),\\ &= \mathscr{B}_{\Delta\Delta'}(\zeta\zeta', zz'),\\ &= xx'.\end{aligned}$$

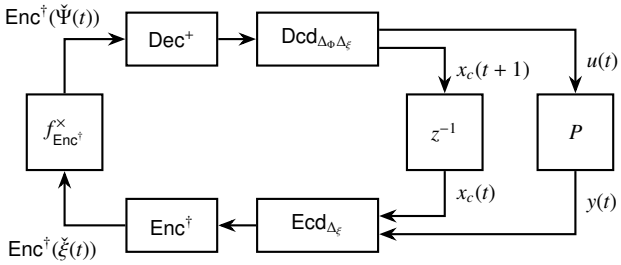


Fig. 2 Block diagram of encrypted control system.

(iv) $(z/p)_L = -1 \wedge (z'/p)_L = -1$

$$\begin{aligned}&\mathsf{Dcd}_{\Delta\Delta'}(\mathsf{Dec}^\dagger(c * c' \bmod p))\\ &= \mathsf{Dcd}_{\Delta\Delta'}(\omega\omega' \bmod p, 1, (p - z)(p - z') \bmod p),\\ &= \mathsf{Dcd}_{\Delta\Delta'}(\omega\omega' \bmod p, 1, zz' \bmod p),\\ &= xx'.\end{aligned}$$

Because of the symmetry of x and x', the proofs for the cases of $z \neq 0 \wedge z' = 0$ and $(z/p)_L = 1 \wedge (z'/p)_L = -1$ are the same as (i) and (iii), respectively. □

Remark 4. In the modified ElGamal encryption scheme, multiplication between ciphertexts is allowed up to $\lfloor \log_2 q \rfloor$ times.

Fig. 2 depicts a block diagram of an encrypted control system with the modified ElGamal cryptosystem. In this case, the plaintexts are denoted as $\breve{\Phi} = \mathsf{Ecd}_{\Delta_\Phi}(\Phi)$, $\breve{\xi} = \mathsf{Ecd}_{\Delta_\xi}(\xi)$, $\breve{\Psi} = \mathsf{Ecd}_{\Delta_\Phi\Delta_\xi}(\Psi) = f^\times(\breve{\Phi}, \breve{\xi})$, and $\breve{\psi} = \mathsf{Ecd}_{\Delta_\Phi\Delta_\xi}(\psi) = f(\breve{\Phi}, \breve{\xi})$.

4. Optimal Dynamic Quantizer

To implement encrypted controllers, controller parameters and signals should be converted into the plaintext space. This process can be regarded as the quantization of controller parameters and signals in a closed-loop system [17].

$\tilde{P}$ and $\bar{f}$ in Fig. 3, which is a quantized control system equivalent to Fig. 2, are given as follows:

$$\begin{aligned}\tilde{P}&: \begin{cases}\begin{bmatrix}x_c(t+1)\\ x(t+1)\end{bmatrix} = \begin{bmatrix}O & O\\ O & A\end{bmatrix}\begin{bmatrix}x_c(t)\\ x(t)\end{bmatrix} + \begin{bmatrix}I & O\\ O & B\end{bmatrix}\psi(t),\\ \qquad \xi(t) = \begin{bmatrix}I & O\\ O & C\end{bmatrix}\begin{bmatrix}x_c(t)\\ x(t)\end{bmatrix},\end{cases}\\ \bar{f}&: \psi(t) = \bar{\Phi}\bar{\xi}(t) = \begin{bmatrix}\bar{A}_c & \bar{B}_c\\ \bar{C}_c & \bar{D}_c\end{bmatrix}\bar{\xi}(t),\end{aligned}$$

where $\mathcal{Q} : \xi \mapsto \bar{\xi}$ is a quantizer, I and O are, respectively, an identity matrix and a zero matrix of an appropriate size, and $\bar{\Phi} = \mathsf{Dcd}_{\Delta_\Phi}(\mathsf{Ecd}_{\Delta_\Phi}(\Phi))$. The closed-loop system can be written as

$$\Sigma : \begin{cases}x_\Sigma(t+1) = A_\Sigma x_\Sigma(t) + B_\Sigma\bar{\xi}(t),\\ \qquad \xi(t) = C_\Sigma x_\Sigma(t),\end{cases}$$

where

$$x_\Sigma(t) = \begin{bmatrix}x_c(t)\\ x(t)\end{bmatrix}, \qquad A_\Sigma = \begin{bmatrix}O & O\\ O & A\end{bmatrix},$$
$$B_\Sigma = \begin{bmatrix}\bar{A}_c & \bar{B}_c\\ B\bar{C}_c & B\bar{D}_c\end{bmatrix}, \quad C_\Sigma = \begin{bmatrix}I & O\\ O & C\end{bmatrix}.$$

Theorem 3. Suppose A is Schur, and $C_\Sigma B_\Sigma$ is a non-singular matrix. An optimal dynamic quantizer in Fig. 4,

$$\mathcal{Q}^\star : \begin{cases} x_q(t+1) = A_q x_q(t) + B_q(\bar{\xi}(t) - \xi(t)), \\ \bar{\xi}(t) = \mathsf{Dcd}_{\Delta_\xi}(\mathsf{Ecd}_{\Delta_\xi}(C_q x_q(t) + \xi(t))), \end{cases}$$

minimizing

$$E(\mathcal{Q}) \coloneqq \sup_{x_\Sigma(0)\in\mathbb{R}^{n_c+n}} \sup_{t\in\mathbb{Z}^+} \|\bar{\xi}(t) - \xi_I(t)\|_\infty$$

can be designed as

$$A_q = A_\Sigma,\ B_q = B_\Sigma, \text{ and } C_q = -(C_\Sigma B_\Sigma)^{-1} C_\Sigma A_\Sigma,$$

where x_q is a quantizer state, $x_q(0) = 0$, A_q, B_q, and C_q are quantizer parameters, and ξ_I is an output of $\tilde{P}$ in Fig. 3 when the quantizer $\mathcal{Q}$ is not involved. Furthermore, the maximum difference between $\bar{\xi}(t)$ and $\xi_I(t)$ is given as

$$E(\mathcal{Q}^\star) = \|C_\Sigma B_\Sigma\|_\infty \frac{\Delta_\xi}{2}.$$

The proof is omitted due to space constraints. The complete proof of an optimal dynamic quantizer is shown in [19].

Remark 5. $\mathcal{Q}^\star$ is stable if and only if the following system is stable [19]:

$$\begin{aligned} x_q(t+1) &= (A_\Sigma - B_\Sigma(C_\Sigma B_\Sigma)^{-1} C_\Sigma A_\Sigma) x_q(t) + B_\Sigma w(t), \\ \bar{\xi}(t) &= -(C_\Sigma B_\Sigma)^{-1} C_\Sigma A_\Sigma x_q(t) + \xi(t) + w(t), \end{aligned}$$

where $w(t) = \mathsf{Dcd}_{\Delta_\xi}(\mathsf{Ecd}_{\Delta_\xi}(C_q x_q(t) + \xi(t))) - (C_q x_q(t) + \xi(t))$.

Remark 6. The dynamic quantizer may be applied for encrypted control systems even though the normal ElGamal cryptosystem is employed by using the conventional encoding and decoding maps [4], [17]. However, the quantization results are not optimal [19] because the intermittence of a plaintext space is not solved, and the maps cannot consider zero. In these cases, $E(\mathcal{Q}^\star)$ is upper-bounded as

$$E(\mathcal{Q}^\star) \le \|C_\Sigma B'_\Sigma\|_\infty \frac{\Delta_\xi d_{\max}}{2}, \quad B'_\Sigma = \begin{bmatrix} \bar{A}'_c & \bar{B}'_c \\ B\bar{C}'_c & B\bar{D}'_c \end{bmatrix},$$

where $d_{\max}$ is the maximum width of $\mathcal{M}$, and $\bar{A}'_c$, $\bar{B}'_c$, $\bar{C}'_c$, and $\bar{D}'_c$ are given by the encoding and decoding maps. Unfortunately, there is no efficient method to search $d_{\max}$ of a given cryptosystem in our best knowledge. The computation time of the linear search for finding $d_{\max}$ is $O(2^k)$. Thus, using the previous encoding and decoding maps and the calculation of the upper-bound are not practical if the key length is large.

Remark 7. Although the dynamic quantizer does not necessarily guarantee the stability of a closed-loop system, it is possible to achieve asymptotic stability by changing the resolution Δ_ξ according to plant behavior [17].

5. Numerical Example

Consider the following continuous-time plant:

$$A = \begin{bmatrix} -0.1 & 0.1 \\ 0 & -0.3 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 \end{bmatrix}.$$

This plant is discretized as

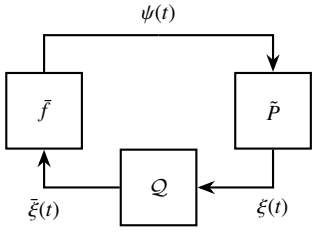


Fig. 3 Equivalent block diagram of encrypted control system.

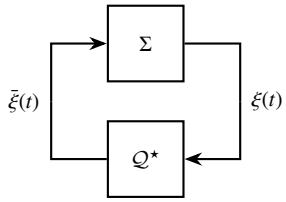


Fig. 4 Optimal dynamic quantizer.

$$A = \begin{bmatrix} 0.990 & 0.010 \\ 0 & 0.970 \end{bmatrix}, \ B = \begin{bmatrix} 4.934 \times 10^{-4} \\ 0.099 \end{bmatrix}, \ C = \begin{bmatrix} 1 & 1 \end{bmatrix},$$

where a sampling period is set to 0.1 s.

A regulator for the plant is given as

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

where $\hat{x} \in \mathbb{R}^n$ is an estimated state, $L \in \mathbb{R}^{n\times l}$ is an observer gain, and $F \in \mathbb{R}^{m\times n}$ is a state-feedback gain. In this case, controller parameters are $A_c = A + BF + LC$, $B_c = -L$, $C_c = F$, and $D_c = O$. The observer gain and the state-feedback gain are designed by using the discrete-time linear quadratic regulator problem as

$$F = \begin{bmatrix} -0.351 & -0.739 \end{bmatrix}, \quad L = \begin{bmatrix} -0.402 \\ -0.318 \end{bmatrix},$$

where state weights and input weights are set to I and 1, respectively.

The parameters of $\mathcal{E}^\dagger$ are $k = 32$, $p = 6848919887$, $q = 3424459943$, $g = 2$, $h = 5527055734$, $s = 1076876626$, and $d_{\max} = 32$. We select $\Delta_\Phi = 1 \times 10^{-2}$ and $\Delta_\xi = 5 \times 10^{-2}$, and then, $\mathcal{Q}^\star$ is designed as

$$A_q = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.990 & 0.010 \\ 0 & 0 & 0 & 0.970 \end{bmatrix},$$

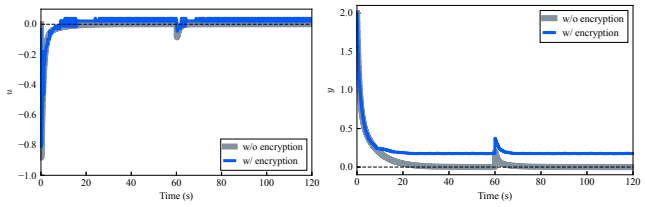
$$B_q = \begin{bmatrix} 0.590 & -0.390 & 0.400 \\ -0.350 & 0.580 & 0.320 \\ -1.727 \times 10^{-4} & -3.651 \times 10^{-4} & 0 \\ -0.034 & -0.073 & 0 \end{bmatrix},$$

$$C_q = \begin{bmatrix} 0 & 0 & 9.690 & 9.594 \\ 0 & 0 & 8.930 & 8.841 \\ 0 & 0 & -5.587 & -5.531 \end{bmatrix},$$

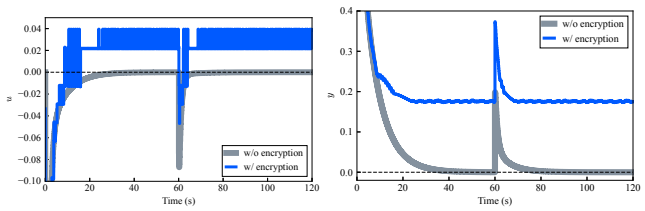
and

$$E(\mathcal{Q}^\star) = 0.034, \quad \|C_\Sigma B'_\Sigma\|_\infty \frac{\Delta_\xi d_{\max}}{2} = 1.120.$$

Fig. 5(a) and (b) show the input and output of the encrypted control system using the dynamic quantizer with the normal

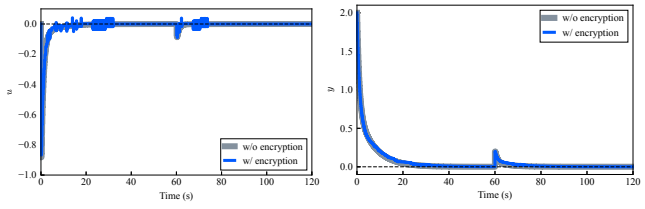


(a) u. (b) y.

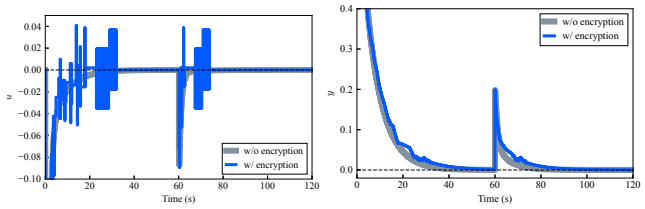


(c) Enlarged graph of u. (d) Enlarged graph of y.

Fig. 5 Control performance of the encrypted control system using dynamic quantizer with ElGamal encryption.



(a) u. (b) y.



(c) Enlarged graph of u. (d) Enlarged graph of y.

Fig. 6 Control performance of the encrypted control system using optimal dynamic quantizer with the proposed cryptosystem.

ElGamal cryptosystem. Similarly, Fig. 6(a) and (b) depict the signals with the optimal dynamic quantizer based on the proposed ElGamal-type encryption scheme. In both the simulation results, an impulse disturbance is added to the control input at 60 s to evaluate whether the encrypted control system is stable under the disturbance even after quantization and encryption. Figs. 5(c)(d) and Figs. 6(c)(d) are enlarged graphs of Figs. 5(a)(b) and Figs. 6(a)(b), respectively. These results confirm that the optimal dynamic quantizer with the proposed cryptosystem improves the control performance of the encrypted control system, and the encrypted control system inherits the stability of the original control system.

6. Conclusions

This study proposed a variant of ElGamal encryption, in which the width of the plaintext space is uniform and it can properly handle zero to implement an optimal dynamic quantizer in encrypted control systems. The proposed cryptosystem employs encoding and decoding maps, which convert between integers and quadratic residues without loss of information. The optimal dynamic quantizer minimizes the maximum difference between outputs of an extended plant in an encrypted control system with the proposed encryption scheme and that in unencrypted control system. The numerical simulations demonstrated that the proposed cryptosystem allowed the implementation of the optimal dynamic quantizer, and the quantizer improved the control performance of an encrypted control system.

In future work, we will consider implementing an encrypted optimal dynamic quantizer whose processes are addressed in ciphertext space.

References

[1] H. Sandberg, S. Amin, and K. H. Johansson: Cyberphysical security in networked control systems: An introduction to the issue, *IEEE Control Systems Magazine,* Vol. 35, pp. 20–23, 2015.

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

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

[4] 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.

[5] Y. Mo and B. Sinopoli: Secure control against replay attacks, *in Annual Allerton Conference on Communication, Control, and Computing,* pp. 911–918, 2009.

[6] 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.

[7] 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.

[8] P. Paillier: Public-key cryptosystems based on composite degree residuosity classes, *in Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques,* pp. 223–238, 1999.

[9] F. Farokhi, I. Shames, and N. Batterham: Secure and private control using semi-homomorphic encryption, *Control Engineering Practice,* Vol. 67, pp. 13–20, 2017.

[10] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, M. Kim, and Y. Song: Encrypting controller using fully homomorphic encryption for security of cyber-physical systems, *IFAC-PapersOnLine,* Vol. 49, No. 22, pp. 175–180, 2016.

[11] 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.

[12] K. Kogiso: Attack detection and prevention for encrypted control systems by application of switching-key management, *in IEEE Conference on Decision and Control,* pp. 5032–5037, 2018.

[13] K. Kogiso: Upper-bound analysis of performance degradation in encrypted control system, *in American Control Conference,* pp. 1250–1255, 2018.

[14] R. W. Brockett and D. Liberzon: Quantized feedback stabilization of linear systems, *IEEE Transactions on Automatic Control,* Vol. 45, No. 7, pp. 1279–1289, 2000.

[15] M. Kishida: Encrypted control system with quantiser, *IET Control Theory & Applications,* Vol. 13, No. 1, pp. 146–151, 2019.

[16] M. Kishida: Encrypted average consensus with quantized control law, *in IEEE Conference on Decision and Control,* pp. 5850–5856, 2018.

[17] K. Teranishi, N. Shimada, and K. Kogiso: Stability analysis and dynamic quantizer for controller encryption, *in IEEE Con-*

ference on Decision and Control, pp. 7184–7189, 2019.
[18] K. Teranishi and K. Kogiso: Dynamic quantizer for encrypted observer-based control, *in IEEE Conference on Decision and Control,* pp. 5477–5482, 2020.
[19] S. Azuma and T. Sugie: Optimal dynamic quantizers for discrete-valued input control, *Automatica,* Vol. 44, No. 2, pp. 396–406, 2008.
[20] G. Castagnos, L. Imbert, and F. Laguillaumie: Encryption switching protocols revisited: Switching modulo *p*, *in Advances in Cryptology – CRYPTO 2017,* pp. 255–287, 2017.

Kaoru TERANISHI (Student Member)

He received his B.S. degree from National Institute of Technology, Ishikawa College, Ishikawa, Japan, in 2019. He is currently an M.S. student at The University of Electro-Communications, Tokyo, Japan. From October 2019 to September 2020, he was a visiting scholar of the Georgia Institute of Technology, GA, USA. His research interests include control theory and cryptography for cyber-security of control systems. He is a student member of IEEE.

Kiminao KOGISO (Member)

He received the B.S., M.S., and Ph.D. degrees in Mechanical Engineering from Osaka University, Japan, in 1999, 2001, and 2004, respectively. He was a postdoctoral researcher in the 21st Century COE Program in 2004 and became an Assistant Professor in the Department of Information Systems, Nara Institute of Science and Technology, Nara, Japan, in 2005. Since March 2014, he has been an Associate Professor in the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan. From November 2010 to December 2011, he was a visiting scholar of the Georgia Institute of Technology, GA, USA. His research interests include constrained control, control of decision makers, cyber-security of control systems, and their applications. He is a member of IEEE.