Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Event-triggered Approach to Increasing Sampling Period of Encrypted Control Systems

K. Teranishi * **J. Ueda** ** **K. Kogiso** *

* *The Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Chofu, Tokyo, Japan (e-mail: teranishi@uec.ac.jp)*
** *The George W. Woodruff School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, GA, USA*

Abstract: Controller encryption is a cryptographic approach to enhancing the security of networked control systems. The method would be effective in reducing risks of eavesdropping attacks. However, encryption may cause high communication traffic and processing delays. This study proposes a redetermination method for a sampling period of a given encrypted control system to increase the sampling period. The proposed method can reduce the bit rate of communication between a plant and controller and improving the strength of ciphertexts. The validity of the proposed method is examined through numerical simulations. The simulation results demonstrate that the sampling period-redetermined encrypted control system achieves asymptotic stability and retains control performance of the original encrypted control system.

Keywords: Secure networked control systems, Encrypted control, Homomorphic encryption, Event-triggered control, Sampling period

1. INTRODUCTION

Cybersecurity is crucial for cyber-physical systems, such as water systems, transportation, and electric power grids (Sandberg et al., 2015; Teixeira et al., 2015a,b). Attacks on control systems are more severe than ones on information systems because they may cause physical damages as well as information leakage and economic losses. Encrypted control is a cryptographic countermeasure against attacks for networked control systems (Kogiso and Fujita, 2015; Farokhi et al., 2017). This method can reduce risks of eavesdropping attacks by concealing controller parameters and signals (e.g., a reference, sensor measurement, and control input) with homomorphic encryption.

Kogiso and Fujita (2015) have proposed the controller encryption method using multiplicative homomorphic encryption such as RSA (Rivest et al., 1978) and the ElGamal encryption (Elgamal, 1985). Multiplicative encrypted control systems can encrypt both the controller parameters and signals. Additionally, the encrypted control systems lead to a detection method for controller falsification attacks and replay attacks (Kogiso, 2018; Baba et al., 2018). The feasibility of an encrypted PID controller, encrypted regulator, and encrypted observer-based servo controller has been examined (Kogiso et al., 2018; Teranishi et al., 2019a). Encrypted control systems with additive homomorphic encryption, the Paillier encryption (Paillier, 1999), can conceal either controller parameters or signals (Farokhi et al., 2017). As a variety of additive encrypted control, encrypted consensus control (Kishida, 2018), encrypted cooperative control (Darup et al., 2019), and encrypted model predictive control (Alexandru et al., 2018) were proposed.

Although encrypted control is a promising approach to enhancing the cybersecurity of networked control systems, encryption may cause high communication traffic and processing delays. Deterioration of network quality would affect the control performance and stability of networked control systems. Therefore, it is necessary to reduce the communication traffic of encrypted control systems.

Increasing the sampling period is one of the methods expected to reduce communication traffic. Sampling period selection is a traditional problem in the field of control engineering. A sampling frequency is restricted by control systems specifications, such as an actuator, sensor, sampler, and holder. Based on heuristic speculations, a sampling frequency is typically selected at least as fast as 50 times of the system bandwidth (Franklin et al., 1997). A multirate sampling technique is effective in improving the control performance of digital control systems by employing different sampling periods of the sampler and holder (Berg et al., 1988; Fujimoto et al., 2001).

Event-triggered and self-triggered control, aperiodic sampling control, are another strategy for handling communication constraints (Heemels et al., 2012). In event-triggered control systems, plant outputs are transmitted to a feedback controller when a triggering condition based on current measurements is satisfied. Thus, event-triggered control requires additional computation costs to evaluate the triggering condition. In self-triggered control systems, a feedback controller with a triggering mechanism decides a next update time by using a plant model. The triggering

condition needs to be assessed in ciphertext to implement self-triggered encrypted control. However, it may be difficult to evaluate if-then rules using ciphertext in real-time, even though homomorphic encryption is used.

This study considers the problem of increasing a sampling period of a given encrypted control system. When we reduce the communication traffic of a networked control system in operation, it is meaningful from the perspective of availability to increase the sampling period of the control system while not changing a controller. As a solution to the problem, we provide an event-triggering mechanism of an encrypted state-feedback controller and propose a lower-bound of the inter-event time of the event-triggered encrypted control system. The lower-bound is employed as a new sampling period, whose interval is longer than or equal to the original sampling period of the given encrypted control system. Computational costs of the sampling period-redetermined encrypted control system are the same as that of the original encrypted control system, unlike event-triggered encrypted control systems. Furthermore, the asymptotic stability of the encrypted control system is guaranteed. The validity of the proposed method is examined through numerical simulations.

The remainder of this paper is organized as follows. Section 2 introduces preliminary information on the ElGamal encryption and an encoder/decoder for controller encryption. Section 3 describes the problem setting and the main result of this study. Section 4 provides some results of numerical simulations. Section 5 presents conclusions and future works.

2. PRELIMINARIES

2.1 Notation

The sets of real numbers, integers, security parameters, key pairs, public keys, secret keys, plaintexts, and ciphertexts are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathcal{S}$, $\mathcal{K}$, $\mathcal{K}_\mathsf{p}$, $\mathcal{K}_\mathsf{s}$, $\mathcal{M}$, and $\mathcal{C}$, respectively. We define the sets $\mathbb{R}^+ \coloneqq \{x \in \mathbb{R} \mid 0 \leq x\}$, $\mathbb{Z}^+ \coloneqq \{z \in \mathbb{Z} \mid 0 \leq z\}$ and $\mathbb{Z}_n \coloneqq \{z \in \mathbb{Z} \mid 0 \leq z < n\}$. 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 is denoted by $\|v\|$. The maximum and minimum eigenvalues of M are denoted by $\lambda_{\max}(M)$ and $\lambda_{\min}(M)$, respectively. The identity map on a set A is denoted by id_A. We use $\check{x}$ and $\bar{x}$ for a plaintext and quantized value of x, respectively.

2.2 ElGamal Cryptosystem

Definition 1. (Katz and Lindell, 2014; Buchmann, 2004) We call $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ a public-key encryption if it satisfies $\mathsf{Dec} \circ \mathsf{Enc} = \mathrm{id}_\mathcal{M}$, where $\mathsf{Gen} : \mathcal{S} \to \mathcal{K} = \mathcal{K}_\mathsf{p} \times \mathcal{K}_\mathsf{s}$ is a key generation algorithm, $\mathsf{Enc} : \mathcal{K}_\mathsf{p} \times \mathcal{M} \to \mathcal{C}$ is an encryption algorithm, and $\mathsf{Dec} : \mathcal{K}_\mathsf{s} \times \mathcal{C} \to \mathcal{M}$ is a decryption algorithm.

Definition 2. (Katz and Lindell, 2014; Buchmann, 2004) We call $\mathcal{E}^\circ = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \circ)$ a homomorphic encryption if it is a public-key encryption that satisfies the following conditions.

(i) $\mathcal{M}$ and $\mathcal{C}$ are group with operations $\circ$ and $\bullet$, respectively.
(ii) Assume that $c = \mathsf{Enc}(\mathsf{pk}, m)$ and $c' = \mathsf{Enc}(\mathsf{pk}, m')$, then $\mathsf{Dec}(\mathsf{sk}, c \bullet c') = m \circ m'$.

The ElGamal encryption is a multiplicative homomorphic encryption $\mathcal{E}^\times$ that consists of

$$\mathsf{Gen} : k \mapsto (\mathsf{pk}, \mathsf{sk}) = ((\mathbb{G}, q, g, h), s),$$
$$\mathsf{Enc} : (\mathsf{pk}, m) \mapsto c = (c_1, c_2) = (g^r \bmod p, mh^r \bmod p),$$
$$\mathsf{Dec} : (\mathsf{sk}, c) \mapsto m = {c_1}^{-s} c_2 \bmod p,$$

where $\mathcal{S} = \mathbb{Z}^+$, $\mathcal{M} = \mathbb{G}$, $\mathcal{C} = \mathbb{G}^2$, q is a k bit prime, $p = 2q + 1$ is a safe prime, g is a generator of a cyclic group $\mathbb{G} = \{g^i \bmod p \mid i \in \mathbb{Z}_q\}$ such that $g^q \bmod p = 1$, r and s are random numbers in $\mathbb{Z}_q$, and $h = g^s \bmod p$. The ElGamal cryptosystem satisfies the following equality with the Hadamard product $*$:

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

2.3 Encoder and Decoder

An encoder $\mathsf{Ecd} : \mathbb{R}^+ \times \mathbb{R} \to \mathcal{M}$ and decoder $\mathsf{Dcd} : \mathbb{R}^+ \times \mathcal{M} \to \mathbb{R}$ with a scaling parameter γ are given as follows:

$$\mathsf{Ecd} : (\gamma, x) \mapsto \check{x} = \underset{m\in\mathcal{M},\ m\geq\gamma x+\alpha(x)}{\arg\min} |\gamma x + \alpha(x) - m|,$$
$$\mathsf{Dcd} : (\gamma, \check{x}) \mapsto \bar{x} = \frac{\check{x} - \beta(\check{x})}{\gamma},$$

where

$$\alpha(x) \coloneqq \begin{cases} p, & x < 0, \\ 0, & x \geq 0, \end{cases} \quad \beta(\check{x}) \coloneqq \begin{cases} p, & \check{x} > q, \\ 0, & \check{x} \leq q, \end{cases}$$

and for a vector and a matrix, Ecd and Dcd perform elementwise. Note that $\mathsf{Dcd}(\gamma, \cdot) \circ \mathsf{Ecd}(\gamma, \cdot) \neq \mathrm{id}_\mathbb{R}$, i.e., Ecd and Dcd cause quantization errors (Teranishi et al., 2019b).

3. SAMPLING PERIOD REDETERMINATION

This section describes the problem of increasing a sampling period and the main result of this study. First, we introduce an event-triggering mechanism for an encrypted controller to derive a sampling period redetermination method. Then, we give the lower-bound of inter-event time of the event-triggered encrypted control system, which guarantees asymptotic stability.

3.1 Problem Setting

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 follows:

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

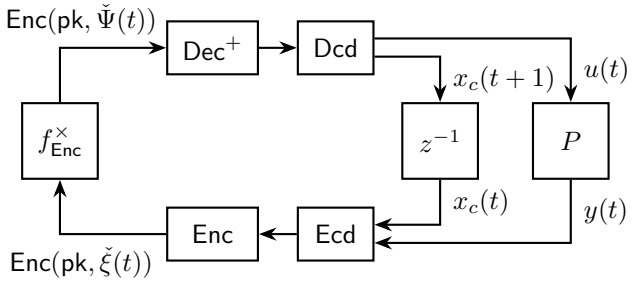


Fig. 1. Block diagram of encrypted control system.

Definition 3. Given a multiplicative homomorphic encryption $\mathcal{E}^\times$, then we call

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

an encrypted controller if it satisfies

$$\begin{aligned} &f^\times_{\mathsf{Enc}}(\mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_c, \Phi)), \mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_p, \xi))) \\ &= \mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_c\gamma_p, \Psi)), \\ &\mathsf{Dec}^+(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_c\gamma_p, \Psi))) \\ &= f^+(\mathsf{Ecd}(\gamma_c\gamma_p, \Psi)) = \check{\psi}, \end{aligned}$$

where $\mathsf{Dec}^+ \coloneqq f^+ \circ \mathsf{Dec}$, and f is divided as $f = f^+ \circ f^\times$ (Kogiso and Fujita, 2015):

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

Fig. 1 depicts a block diagram of an encrypted control system.

Definition 4. The following definition of bit rate is employed:

$$\eta \coloneqq \log_2 M \quad \text{(bits/sample)},$$

where M is a cardinality of alphabet (Nair et al., 2007). Then, the bits per second can be defined as follows:

$$\eta' \coloneqq \frac{\eta}{T_s} = \frac{\log_2 M}{T_s} \quad \text{(bits/second)},$$

where T_s is a sampling period. In encrypted control systems, M is given as follows:

$$\begin{aligned} M &= |\mathcal{C}^{n_c+l}| \times |\mathcal{C}^{(n_c+m)\times(n_c+l)}|, \\ &= 2^{2(k+1)(n_c+l)+2(k+1)(n_c+m)(n_c+l)}. \end{aligned}$$

Problem 5. Given $f^\times_{\mathsf{Enc}}$ that stabilizes P, whose sampling period is T_s. Design an increased sampling period $T_s' \geq T_s$ such that

- the bit rate decreases η' to $\eta' T_s/T_s'$.
- a closed-loop system with T_s' is asymptotically stable.
- the controller parameter matrix Φ is the same even after changing the sampling period.

This problem is critical for reducing the communication traffic of a networked control system in operation while maintaining the availability of the control system.

3.2 Design of An Increased Sampling Period

In this study, we consider a networked control system with an encrypted state-feedback controller using the ElGamal encryption

$$\begin{aligned} f^\times_{\mathsf{Enc}} &: (c_F, c_x(t)) \mapsto c_u(t), \\ c_F &= \mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_c, F)), \\ c_x(t) &= \mathsf{Enc}(\mathsf{pk}, \mathsf{Ecd}(\gamma_p, x(t))), \\ c_u(t) &= c_F * c_x(t) \bmod p, \end{aligned}$$

where $\Phi = F$, $C = I_n$, $\xi(t) = y(t) = Cx(t) = x(t)$, $\psi(t) = u(t) = \bar{F}\bar{x}(t)$, F is a feedback gain, and I_n is an $n \times n$ identity matrix. Then, $M = 2^{2(k+1)(m+1)n}$ because of $n_c = 0$ and $l = n$. The closed-loop system is given as follows (Teranishi et al., 2019b):

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

This closed-loop system is not necessarily stable because of quantization errors for F and x, even if an unencrypted closed-loop system is stable. To regard this, the following result (Teranishi et al., 2019b) is used to guarantee asymptotic stability of (1).

Theorem 6. Assume that $A + BF$ is Schur. If

$$\gamma_c = \frac{d_{\max}}{\Omega(P_c, Q_c)} + \mu_c, \tag{2}$$

$$\gamma_p(t) = \frac{d_{\max}}{\|x(t)\|}(\Theta(P_p, Q_p) + \mu_p), \tag{3}$$

then $A + B\bar{F}$ is Schur and (1) becomes asymptotically stable, where $d_{\max}$ is the maximum width of $\mathcal{M}$, $\mu_c > 0$, $\mu_p > 0$,

$$\begin{aligned} \Omega(P_c, Q_c) &\coloneqq \frac{2}{\sqrt{mn}\|B^\top P_c B\|}\Bigg(-\|(A+BF)^\top P_c B\| \\ &+ \sqrt{\|(A+BF)^\top P_c B\|^2 + \lambda_{\min}(Q_c)\|B^\top P_c B\|}\Bigg), \\ \Theta(P_p, Q_p) &\coloneqq \frac{\sqrt{n}}{2\lambda_{\min}(Q_p)}\Bigg(\|(A+B\bar{F})^\top P_p B\bar{F}\| \\ &+ \sqrt{\|(A+B\bar{F})^\top P_p B\bar{F}\|^2 + \lambda_{\min}(Q_p)\|\bar{F}^\top B^\top P_p B\bar{F}\|}\Bigg), \end{aligned}$$

and Q_c, P_c, Q_p, and P_p are positive definite matrices satisfying $(A+BF)^\top P_c(A+BF) - P_c = -Q_c$ and $(A+B\bar{F})^\top P_p(A+B\bar{F}) - P_p = -Q_p$, respectively. In the following, we assume Ecd and Dcd does not cause overflow and underflow.

An event-triggered control system of (1) is given as follows:

$$\begin{aligned} x(t+1) &= Ax(t) + B\bar{F}\bar{x}(t_k), \\ &= Ax(t) + B\bar{F}(x(t) + e(t)), \\ &= (A + B\bar{F})x(t) + B\bar{F}e(t), \end{aligned} \tag{4}$$

where $e(t) \coloneqq \bar{x}(t_k) - x(t)$, $t \in [t_k, t_{k+1})$, and $\{t_k\}_{k\in\mathbb{Z}^+}$ is a time sequence of control input updates. We design a triggering condition for the time sequence by using the methodology in (Kishida, 2019).

Theorem 7. Given F such that $A + BF$ is Schur. Suppose γ_c and γ_p satisfy (2) and (3), respectively. If an event-triggered encrypted state-feedback controller is given as

$$\begin{aligned} c_u(t) &= \begin{cases} f^\times_{\mathsf{Enc}}(c_F, c_x(t)), & \|x(t)\| \leq \sigma\|e(t)\|, \\ c_u(t_k), & \text{otherwise}, \end{cases} \\ t_{k+1} &= \min\{t \geq t_k \mid \|x(t)\| \leq \sigma\|e(t)\|\}, \quad t_0 = 0, \end{aligned}$$

then (4) becomes asymptotically stable, where

$$\sigma \coloneqq \frac{1}{\lambda_{\min}(Q_e)}\Bigg(\|(A+B\bar{F})^\top P_e B\bar{F}\| + \sqrt{\|(A+B\bar{F})^\top P_e B\bar{F}\|^2 + \lambda_{\min}(Q_e)\|\bar{F}^\top B^\top P_e B\bar{F}\|}\Bigg),$$

and positive definite matrices P_e and Q_e satisfy $(A+B\bar{F})^\top P_e(A+B\bar{F}) - P_e = -Q_e$.

Proof. From Theorem 6, $A+B\bar{F}$ is Schur. Thus, there exist positive definite matrices P_e and Q_e such that $(A+B\bar{F})^\top P_e(A+B\bar{F}) - P_e = -Q_e$. Let $V(t) = x^\top(t)P_e x(t)$ be a Lyapunov function candidate, then

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

By using the notations $a \coloneqq -\lambda_{\min}(Q_e)$, $b \coloneqq 2\|(A+B\bar{F})^\top P_e B\bar{F}\|\|e\|$, and $c \coloneqq \|\bar{F}^\top B^\top P_e B\bar{F}\|\|e\|^2$, the solution for the quadratic equation $a\|x\|^2 + b\|x\| + c = 0$ is given as follows:

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

Therefore, $V(t+1) - V(t)$ is negative outside the ball $\{x(t) \mid \|x(t)\| \le \sigma\|e(t)\|\}$. If the control input is updated immediately when $\|x(t)\| \le \sigma\|e(t)\|$ is satisfied, then (4) achieves asymptotic stability because $V(t+1) - V(t)$ is negative for any time step t. □

Note that the event-triggered encrypted control system requires that a plant computes the triggering condition. Theorem 7 ensures the stability of the encrypted control system with aperiodic sampling. The main result of this study is given by using this result as follows:

Theorem 8. Given F such that $A+BF$ is Schur. Suppose γ_c and γ_p satisfy (2) and (3), respectively. Let $\Delta \in \mathbb{Z}^+$ be an inter-event time of the time sequence $\{t_k\}_{k\in\mathbb{Z}^+}$. If an encrypted state-feedback controller is given as

$$\begin{aligned}
c_u(t) &= f^{\times}_{\mathsf{Enc}}(c_F, c_x(t_k)),\\
t_{k+1} &= t_k + \Delta, \quad t_0 = 0,\\
\Delta &\coloneqq \max\left\{\tau \;\middle|\; \sqrt{\frac{\Gamma_X(\tau)}{\Gamma_E(\tau)}} > \sigma\right\},
\end{aligned} \tag{5}$$

then (4) becomes asymptotically stable, where

$$\begin{aligned}
\Gamma_X(\tau) &\coloneqq \lambda_{\min}(X^\top(\tau)X(\tau)) - 2\|X^\top(\tau)A^\tau\|D,\\
\Gamma_E(\tau) &\coloneqq \lambda_{\max}(E^\top(\tau)E(\tau)) + 2\|E^\top(\tau)A^\tau\|D\\
&\qquad + \lambda_{\max}((A^\tau)^\top A^\tau)D^2,\\
X(\tau) &\coloneqq A^\tau + \sum_{i=0}^{\tau-1} A^{\tau-1-i}B\bar{F},\\
E(\tau) &\coloneqq I_n - X(\tau),\\
D &\coloneqq \frac{\sqrt{n}}{\Theta(P_p, Q_p) + \mu_p}.
\end{aligned}$$

Proof. Without loss of generaliry, we set $t \in [t_k, t_{k+1})$ and $t_k = t_0 = 0$ because t_k can be regarded as an initial time after every control input update. From (4), the solution of $x(t)$ is

$$\begin{aligned}
x(t) &= A^{t-t_k}x(t_k) + \sum_{i=0}^{t-t_k-1} A^{t-t_k-1-i}B\bar{F}\bar{x}(t_k),\\
&= \left\{A^t + \sum_{i=0}^{t-1} A^{t-1-i}B\bar{F}\right\}\bar{x}(0) - A^t\delta(0),\\
&= X(t)\bar{x}_0 - A^t\delta_0,
\end{aligned}$$

where $\delta(t_k) = \bar{x}(t_k) - x(t_k)$, $\bar{x}_0 = \bar{x}(0)$, and $\delta_0 = \delta(0)$. The dynamics of $e(t)$ is given as

$$\begin{aligned}
e(t+1) &= \bar{x}(t_k) - x(t+1),\\
&= Ae(t) + (I_n - A - B\bar{F})\bar{x}(t_k).
\end{aligned}$$

Then, the solution of $e(t)$ is

$$\begin{aligned}
e(t) &= A^{t-t_k}e(t_k) + \sum_{i=0}^{t-t_k-1} A^{t-t_k-1-i}(I_n - A - B\bar{F})\bar{x}(t_k),\\
&= \left\{I_n - A^t - \sum_{i=0}^{t-1} A^{t-1-i}B\bar{F}\right\}\bar{x}(0) + A^t\delta(0),\\
&= E(t)\bar{x}_0 + A^t\delta_0,
\end{aligned}$$

where $e(t_k) = \bar{x}(t_k) - x(t_k) = \delta(t_k)$. Thus,

$$\begin{aligned}
&\|x(t)\| > \sigma\|e(t)\|\\
\iff &\|X(t)\bar{x}_0 - A^t\delta_0\| > \sigma\|E(t)\bar{x}_0 + A^t\delta_0\|,\\
\iff &\sqrt{\bar{x}_0^\top X^\top X\bar{x}_0 - 2\bar{x}_0^\top X^\top A^t\delta_0 + \delta_0^\top(A^t)^\top A^t\delta_0}\\
&\quad > \sigma\sqrt{\bar{x}_0^\top E^\top E\bar{x}_0 + 2\bar{x}_0^\top E^\top A^t\delta_0 + \delta_0^\top(A^t)^\top A^t\delta_0},\\
\impliedby &\sqrt{\lambda_{\min}(X^\top X) - 2\|X^\top A^t\|\kappa}\\
&\quad > \sigma\sqrt{\lambda_{\max}(E^\top E) + 2\|E^\top A^t\|\kappa + \lambda_{\max}((A^t)^\top A^t)\kappa^2}.
\end{aligned}$$

where $\kappa = \|\delta_0\|/\|\bar{x}_0\|$. Because $\|\delta(t_k)\|$ is bounded from above by $\sqrt{n}d_{\max}/\gamma_p(t_k)$ (Teranishi et al., 2019b),

$$\kappa = \frac{\|\delta_0\|}{\|x_0 + \delta_0\|} \le \frac{\|\delta_0\|}{\|x_0\|} \le \frac{\sqrt{n}}{\Theta(P_p, Q_p) + \mu_p} = D,$$

where $x_0 = x(0)$. Note that elements of $\delta(t_k)$ are non-negative due to the definition of Ecd. Then, we obtain

$$\begin{aligned}
&\|x(t)\| > \sigma\|e(t)\|\\
\impliedby &\sqrt{\lambda_{\min}(X^\top X) - 2\|X^\top A^t\|D}\\
&\quad > \sigma\sqrt{\lambda_{\max}(E^\top E) + 2\|E^\top A^t\|D + \lambda_{\max}((A^t)^\top A^t)D^2},\\
\iff &\sqrt{\frac{\Gamma_X(t)}{\Gamma_E(t)}} > \sigma.
\end{aligned}$$

Therefore, if the time sequence $\{t_k\}_{k\in\mathbb{Z}^+}$ is decided by $t_{k+1} = t_k + \Delta$, then $\|x(t)\| > \sigma\|e(t)\|$ is satisfied for any time step t. □

Remark 9. Δ can be calculated offline because (5) does not depend on the initial condition. Thus, the time sequence $\{t_k\}_{k\in\mathbb{Z}^+}$ is determined in advance of control systems operation, that is, the sampling period is redetermined as $T_s' = \Delta T_s$.

Remark 10. Sampling period-redetermined control systems may become weaker against plant parameter variations and noises. In future work, we will extend Theorem 8 so as to consider their effects.

Theorem 8 allows us to redetermine the sampling period of control systems while retaining the stability of an original encrypted state-feedback control system. By increasing the sampling period T_s to ΔT_s, the bit rate decreases η' to η'/Δ. It is also possible to increase the key length instead of decreasing the bit rate because the processing time for encryption and decryption can be increased.

4. NUMERICAL EXAMPLE

Consider the following continuous-time plant:

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

This plant is discretized with $T_s = 1$ ms as follows:

$$A = \begin{bmatrix} 0.999 & 0 \\ 0.001 & 1.001 \end{bmatrix}, B = \begin{bmatrix} 9.995 \times 10^{-4} \\ 5.000 \times 10^{-7} \end{bmatrix}.$$

A state feedback controller is designed by using the discrete-time linear quadratic regulator problem as follows:

$$F = [-2.541 \ \ -5.270],$$

where the cost function is

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

state and input weights are respectively set to $Q = \epsilon I_2$ and $R = 1 - \epsilon$, and the design parameter $\epsilon = 0.5$. ElGamal encryption parameters and design parameters are shown in Tables 1 and 2. With these parameters, we obtain $\gamma_c = 1049.233$, $\gamma_p(0) = 22831.334$, $\sigma = 12.745$ and $\Delta = 11$ (i.e., $T_s' = 11$ ms), where

$$P_c = \begin{bmatrix} 424.244 & 1001.095 \\ 1001.095 & 4780.781 \end{bmatrix},$$

$$P_p = P_e = \begin{bmatrix} 424.884 & 1003.089 \\ 1003.089 & 4786.590 \end{bmatrix},$$

$$\bar{F} = [-2.540 - 5.266],$$

and $x(0) = [1 \ \ 1]^\top$. Thus, the bit rate η' decreases 264000 bit/s to 24000 bit/s.

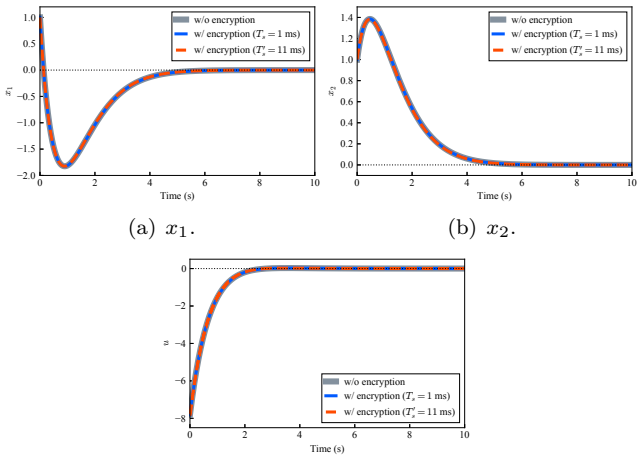
Fig. 2 shows a comparison of the control performance between the original encrypted control system with the sampling period $T_s = 1$ ms and the proposed encrypted control system with the redetermined sampling period $T_s' = 11$ ms. Fig. 3 depicts absolute errors between the control input/state of the original encrypted control system and those of the proposed encrypted control system. These results confirm that stability and control performance of the encrypted control system are retained even after the sampling period is modified T_s to T_s'.

Table 1. ElGamal encryption parameters.

Parameter	Value	Parameter	Value
k	32	h	5527055734
p	6848919887	s	1076876626
q	3424459943	$d_{\max}$	32
g	2		

Table 2. Design parameters.

Parameter	Value	Parameter	Value
ϵ	0.5	Q_c	I_2
μ_c	10^3	Q_p	I_2
μ_p	10^3	Q_e	I_2



(a) x_1. (b) x_2.

(c) u.

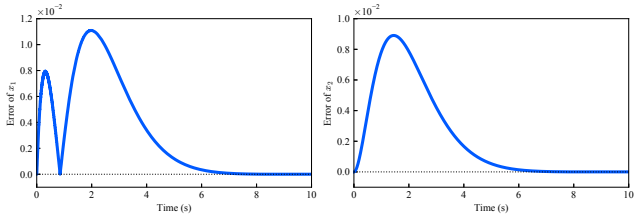
Fig. 2. Comparison of the control performance between the original encrypted control system ($T_s = 1$ ms) and the proposed encrypted control system, whose sampling period is redetermined ($T_s' = 11$ ms).

Fig. 4 illustrates the relationship between the fixed inter-event time Δ and the controller design parameter ϵ. A total of 99 different values for ϵ varying from 0.01 to 0.99 were used. The result shows that Δ tends to decrease as ϵ increases. This implies that faster dynamics may require more frequent updates of the control input than the one with slow dynamics. We also can balance a trade-off between a sampling period and control performance by tuning ϵ.

5. CONCLUSION

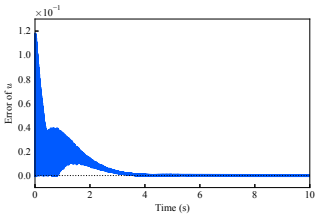
This study proposed the redetermination method of a sampling period for encrypted control systems while guaranteeing asymptotic stability. By increasing the sampling period, it would be possible either to reduce the bit rate for communication between a plant and controller or to increase the key length of encryption. A lower bit rate may lead to improving network quality, addressing such as latencies and packet dropouts. A longer key length results in making ciphertexts stronger.

The validity of the proposed method was investigated through numerical simulations of an encrypted state-feedback control system. Furthermore, the relationship between an inter-event time and a controller design parameter was examined. A trade-off between the sampling period and control performance can be considered by tuning the design parameter based on the relationship.



(a) Error of x_1.

(b) Error of x_2.



(c) Error of u.

Fig. 3. Error of the signals between the original encrypted control system and the proposed encrypted control system.

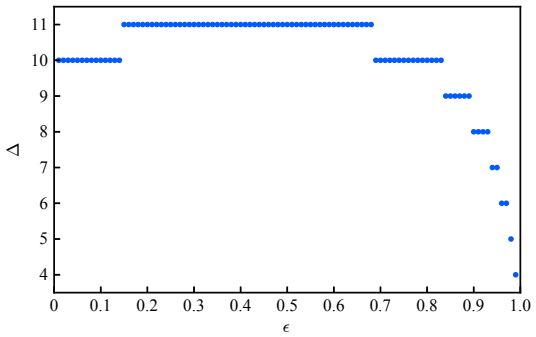


Fig. 4. Relationship between the fixed inter-event time Δ and the controller design parameter ϵ.

Future work includes robustness analysis for sampling period-redetermined encrypted control systems. We will also extend the proposed method so as to consider disturbances and delayed control inputs.

REFERENCES

Alexandru, A.B., Morari, M., and Pappas, G.J. (2018). Cloud-based MPC with encrypted data. In *IEEE Conference on Decision and Control*, 5014–5019.

Baba, R., Kogiso, K., and Kishida, M. (2018). Detection method of controller falsification attacks against encrypted control system. In *SICE Annual Conference*, 244–248.

Berg, M.C., Amit, N., and Powell, J.D. (1988). Multirate digital control system design. *IEEE Transactions on Automatic Control*, 33(12), 1139–1150.

Buchmann, J. (2004). *Introduction to Cryptography*. Springer-Verlag New York, 2nd edition.

Darup, M.S., Redder, A., and Quevedo, D.E. (2019). Encrypted cooperative control based on structured feedback. *IEEE Control Systems Letters*, 3(1), 37–42.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), 469–472.

Farokhi, F., Shames, I., and Batterham, N. (2017). Secure and private control using semi-homomorphic encryption. *Control Engineering Practice*, 67, 13–20.

Franklin, G.F., Workman, M.L., and Powell, D. (1997). *Digital control of dynamic systems*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition.

Fujimoto, H., Hori, Y., and Kawamura, A. (2001). Perfect tracking control based on multirate feedforward control with generalized sampling periods. *IEEE Transactions on Industrial Electronics*, 48(3), 636–644.

Heemels, W.P.M.H., Johansson, K.H., and Tabuada, P. (2012). An introduction to event-triggered and self-triggered control. In *IEEE Conference on Decision and Control*, 3270–3285.

Katz, J. and Lindell, Y. (2014). *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2nd edition.

Kishida, M. (2018). Encrypted average consensus with quantized control law. In *IEEE Conference on Decision and Control*, 5850–5856.

Kishida, M. (2019). Encrypted control system with quantizer. *IET Control Theory & Applications*, 13(1), 146–151.

Kogiso, K. (2018). Attack detection and prevention for encrypted control systems by application of switching-key management. In *IEEE Conference on Decision and Control*, 5032–5037.

Kogiso, K., Baba, R., and Kusaka, M. (2018). Development and examination of encrypted control systems. In *IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, 1338–1343.

Kogiso, K. and Fujita, T. (2015). Cyber-security enhancement of networked control systems using homomorphic encryption. In *IEEE Conference on Decision and Control*, 6836–6843.

Nair, G.N., Fagnani, F., Zampieri, S., and Evans, R.J. (2007). Feedback control under data rate constraints: An overview. *Proceedings of the IEEE*, 95(1), 108–137.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques*, 223–238.

Rivest, R.L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

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

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2015a). A secure control framework for resource-limited adversaries. *Automatica*, 51, 135–148.

Teixeira, A., Sou, K.C., Sandberg, H., and Johansson, K.H. (2015b). Secure control systems: A quantitative risk management approach. *IEEE Control Systems Magazine*, 35(1), 24–45.

Teranishi, K., Kusaka, M., Shimada, N., Ueda, J., and Kogiso, K. (2019a). Secure observer-based motion control based on controller encryption. In *American Control Conference*, 2978–2983.

Teranishi, K., Shimada, N., and Kogiso, K. (2019b). Stability analysis and dynamic quantizer for controller encryption. In *IEEE Conference on Decision and Control*, 7184–7189.