Designing Optimal Key Lengths and Control Laws for Encrypted Control Systems Based on Sample Identifying Complexity and Deciphering Time

Kaoru Teranishi, Student Member, IEEE, Tomonori Sadamoto, Member, IEEE, Aranya Chakrabortty, Senior Member, IEEE, and Kiminao Kogiso, Member, IEEE

Abstract—In the state-of-the-art literature on cryptography and control theory, there has been no systematic methodology of constructing cyber–physical systems that can achieve the desired control performance while being protected against eavesdropping attacks. In this article, we tackle this challenging problem. We first propose two novel notions referred to as sample identifying complexity and sample deciphering time in an encrypted control framework. The former explicitly captures the relation between the dynamical characteristics of control systems and the level of identifiability of the systems while the latter shows the relation between the computation time for the identification and the key length of a cryptosystem. Based on these two tractable new notions, we propose a systematic method for designing both of an optimal key length to prevent system identification with a given precision within a given life span of systems and of an optimal controller to maximize both of the control performance and the difficulty of the identification. The efficiency of the proposed method in terms of security level and realtime-ness is investigated through numerical simulations. To the best of our knowledge, this article first connects the relationship between the security of cryptography and dynamical systems from a control-theoretic perspective.

Index Terms—Cyber–physical system, cyber-security, eavesdropping attack, encrypted control, homomorphic encryption, system identification.

I. INTRODUCTION

Cyber–Physical systems have attracted the attention in numerous areas, such as power grids, transportation, manufacturing, and healthcare [1]–[3]. Integrating communication and computation layers with a physical layer, cyber–physical systems are expected to overwhelm the traditional systems with respect to efficiency, reliability, and sustainability [1], [4]. Meanwhile, cyber–physical systems often face security threats in exchange for the advantages because, in general, they communicate with a public and untrustworthy computer, e.g., cloud, over insecure channels for decision making.

One of major security threats is the eavesdropping attack that tries to disclose confidential information of cyber–physical systems [5]. Once an adversary completes the attacks, more destructive and undetectable attacks can be designed based on a target system model learned by the disclosed information [6]. Therefore, it is crucial for realizing secure cyber–physical systems to prevent eavesdropping attacks.

To fulfill this objective, we definitely need a measure for quantifying the security level against the attacks. Some studies have employed information-theoretic measures, such as mutual information and directed information, for designing estimators and controllers with information leakage constraints under the presence of eavesdroppers [7]. Additionally, differential privacy [8], another well-known measure used in information community, has been adopted for private filtering and controls of dynamical systems [9], [10]. However, these existing measures are not suitable for dynamical systems because it is not clear that the systems should satisfy how the level of security. Furthermore, a controller design method based on the measures has an intrinsic tradeoff between the security and quality of controls due to noise injection [7], [9]. It should be noted here that some recent papers have proposed control-theoretic security quantities [3], [11].

Manuscript received 15 February 2022; accepted 1 May 2022. Date of publication 12 May 2022; date of current version 29 March 2023. This work was supported in part by JSPS Grant-in-Aid for JSPS Fellows under Grant JP21J22442 and in part by JSPS KAKENHI under Grant JP22H01509. Recommended by Associate Editor G. Gu. (Corresponding author: Kaoru Teranishi.)

Kaoru Teranishi is with the Department of Mechanical and Intelligent Systems Engineering, University of Electro-Communications, Tokyo 182-8585, Japan, and also with Japan Society for the Promotion of Science, Tokyo 102-0083, Japan (e-mail: teranishi@uec.ac.jp).
Tomonori Sadamoto and Kiminao Kogiso are with the Department of Mechanical and Intelligent Systems Engineering, University of Electro-Communications, Tokyo 182-8585, Japan (e-mail: sadamoto@uec.ac.jp; kogiso@uec.ac.jp).
Aranya Chakrabortty is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695 USA (e-mail: achakra2@ncsu.edu).
Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2022.3174691.
Digital Object Identifier 10.1109/TAC.2022.3174691
However, the quantities cannot measure the security level against eavesdropping attacks because they focus on other attacks.

Encrypted control [16] is the state-of-the-art technology for preventing eavesdropping attacks without noise injection. Contrary to the information-oriented methods, the performance degradation in encrypted control systems can be ignored by increasing a key length of cryptosystem [17]. Moreover, for a small key length, appropriate quantizers mitigate the quantization errors due to encryption [18], [19]. Thus, encrypted control is a promising framework for achieving the superior security and control performance of cyber–physical systems. In fact, various encrypted control methods have been developed recently by using partially, somewhat, and (levelled) fully homomorphic encryption [20]–[29]. Moreover, their feasibility has been verified through implementation to a drone [30], fog-computing environment [31], and field-programmable gate array [32]. However, the security level of encrypted control systems has not been analyzed and quantified.

B. Contribution

This study considers an attack scenario that an adversary would like to know a system matrix of a stochastic closed-loop system with an encrypted controller by using collected encrypted-data. Under this scenario, we aim to answer the following questions.

1) What is the optimal controller to make the identification accuracy within a certain value?

2) What is the optimal key length needed to secure the closed-loop system within a life span of the system?

To this end, we introduce two novel security quantities, sample identifying complexity and sample deciphering time. This type of quantification is not reported in any papers on cryptography. The sample identifying complexity is derived as a lower bound for the total variance, i.e., the inverse of precision, of Bayesian estimation by an adversary. The sample deciphering time is computation time for breaking encrypted data without a secret key to obtain a data set for the estimation. The security in this study is defined based on these quantities. Roughly speaking, we say an encrypted control system is secure if the adversary cannot identify the system matrix with a certain precision within a life span of the system. The formal definition of the security will be described later.

The sample deciphering time is introduced in two cases with static-key encryption and dynamic-key encryption. Static-key encryption is traditional public-key encryption of which the key pair is identical throughout the communication. In contrast, a key pair in dynamic-key encryption [33] is updated at a short time interval, e.g., a sampling period. Although dynamic-key encryption would improve the security level of encrypted control systems, its security has not yet been proved. We extend the dynamic-key encryption scheme in [33] and provide a security proof of the extended scheme.

Using the security quantities, we formulate a design problem of optimal key length and controller. The optimal controller is designed to maximize the sample identifying complexity. In other words, the controller maximizes the difficulty of the system identification. More interestingly, such a controller is provided as the standard stochastic cheap controller improving the stability degree of a closed-loop system. This fact means, in controller design, there is no tradeoff between the security level and the control performance.

After designing the optimal controller, we design the optimal key length to secure an encrypted control system. The optimal key length is obtained as the minimum key length to make the sample deciphering time longer than the system’s life span. This key length is beneficial for reducing implementation costs of an encrypted control system while keeping the security level because the size of key length has a tradeoff between ciphertext strength and computation costs of encryption and decryption algorithms.

C. Outline

Section II summarizes notations and a definition of homomorphic encryption. The ElGamal encryption, an example of a multiplicative homomorphic encryption scheme, is also introduced. Section III describes the attack scenario considered in this study. We define the security of encrypted control systems and formulate a design problem of the optimal key length and controller. Section IV proposes sample identifying complexity and sample deciphering time. They are used to understand the relationships among a key length, controller, and the number of samples for system identification. Section V provides the solution to the problem based on the security quantities. Additionally, we show how the security quantities can be used for other design problems in encrypted control systems. Section VI demonstrates the validity of the proposed method by numerical simulations. Section VII concludes this article and presents some remarks on the results of this study.

II. PRELIMINARIES

A. Notation

The sets of real numbers, integers, security parameters, public keys, secret keys, plaintexts, and ciphertexts are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathcal{S}$, $\mathcal{K}_p$, $\mathcal{K}_s$, $\mathcal{M}$, and $\mathcal{C}$, respectively. We define the sets of integers $\mathbb{Z}^+ := \{ z \in \mathbb{Z} | 0 \leq z \}$ and $\mathbb{Z}_n := \{ z \in \mathbb{Z} | 0 \leq z < n \}$. The set of $n$-dimensional real column-vectors is denoted by $\mathbb{R}^n$, and that of $m$-by-$n$ real-valued matrices is denoted by $\mathbb{R}^{m \times n}$. The $i$th element of a vector $x \in \mathbb{R}^n$ is denoted by $x_i$, and the $\ell_2$ norm and the maximum norm of $v$ are denoted by $\|v\|_2$ and $\|v\|_\infty$, respectively. The $i$th column vector and $(i, j)$ entry of a matrix $M \in \mathbb{R}^{m \times n}$ are denoted by $M_i$ and $M_{ij}$, respectively. The permanent and column stack vector of $M$ are defined by $\|M\|_{\text{per}} := \max_{i,j} \{ |M_{ij}| \}$ and $\text{vec}(M) := [M_{11}^\top \cdots M_{ij}^\top]^\top$, respectively. The cardinality of a set $\mathcal{A}$ is denoted by $|\mathcal{A}|$. The Gaussian distribution with a mean $\mu$ and a variance-covariance matrix $\Sigma$ is denoted by $\mathcal{N}(\mu, \Sigma)$. The probability density function of $\mathcal{N}(\mu, \Sigma)$ is denoted by $f(x; \mu, \Sigma)$.

**Definition 1:** Let $\mathcal{A}$ be a finite set and $X$ be a random variable. If $P_r(X = a) = 1/|\mathcal{A}|, \forall a \in \mathcal{A}$, then we say $X$ follows the discrete uniform distribution over $\mathcal{A}$ and is denoted as $X \sim \mathcal{U}(\mathcal{A})$. 
Definition 2 (Negligible function [34]): We say a function \( \epsilon : \mathbb{Z}^+ \setminus \{0\} \to \mathbb{R} \) is negligible if for every positive integer \( c > 0 \), there exists \( N \in \mathbb{Z} \) such that \( |\epsilon(n)| < n^{-c} \) holds for all \( n > N \).

B. Homomorphic Encryption and Its Example

This section describes the definition and example of homomorphic encryption to introduce the encrypted-control framework. One can refer [35] for the detailed survey of homomorphic encryption.

A public-key encryption scheme is a triplet (Gen, Enc, Dec), where Gen : \( \mathcal{S} \to \mathcal{K}_e \times \mathcal{K}_d : k \mapsto (pk, sk) \) is a key generation algorithm, Enc : \( \mathcal{K}_p \times \mathcal{M} \to \mathcal{C} : (pk, m) \mapsto c \) is an encryption algorithm, Dec : \( \mathcal{K}_s \times \mathcal{C} \to \mathcal{M} : (sk, c) \mapsto m \) is a decryption algorithm, \( k \) is a security parameter, e.g., a key length, and \( (pk, sk) = \text{Gen}(k) \) is a pair of public key and secret key. Enc and Dec perform elementwise for a vector and a matrix. Public-key encryption schemes must satisfy Dec(sk, Enc(pk, m)) = m for all \( m \in \mathcal{M} \) and \( (pk, sk) \) generated by Gen.

Definition 3: We say (Gen, Enc, Dec) is multiplicative homomorphic encryption if Dec(sk, c \( \otimes \) c') = mm' for all \( m, m' \in \mathcal{M} \) and \( c, c' \in \mathcal{C} \) satisfying Enc(pk, m) = c and Enc(pk, m') = c', where \( \otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C} \) is a binary operation over \( \mathcal{C} \). Similarly, additive homomorphic encryption is defined with \( \oplus : \mathcal{C} \times \mathcal{C} \to \mathcal{C} \).

An example of multiplicative homomorphic encryption includes the ElGamal encryption [36]. Its algorithms are Gen : \( k \mapsto (pk, sk) = ((p, q, g, h), s) \), Enc : \( (pk, m) \mapsto c = (g^q \mod p, mh' \mod p) \), and Dec : \( (sk, (c_1, c_2)) \mapsto c_1^{-s} c_2 \mod p \), where \( q \) is a \( k \) bit prime, \( p = 2q + 1 \) is a safe prime, \( g \) is a generator of a cyclic group \( \mathcal{G} := \{g^i \mod p \mid i \in \mathbb{Z}_q\} = \mathcal{M} \subset \mathbb{Z}_p \setminus \{0\} \) such that \( g^q \mod p = 1 \), \( h = g^s \mod p \), \( \mathcal{C} = \mathcal{G}^2 \), and \( r, s \sim \mathcal{U}(\mathbb{Z}_q) \). Additionally, multiplicative homomorphism is Dec(sk, Enc(pk, m) \* Enc(pk, m') \mod p) = mm' \mod p, where * is the Hadamard product.

III. ATTACK SCENARIO AND PROBLEM SETTING

Consider a plant described by the discrete-time stochastic linear system

\[
x_{t+1} = A_p x_t + B_p u_t + w_t
\]

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, and \( w \in \mathbb{R}^n \) is a i.i.d. random variable following the Gaussian distribution \( \mathcal{N}(0, L^{-1}) \) with the zero vector \( 0 \) and a precision matrix \( L \). Assume that \( (A_p, B_p) \) is controllable, and the initial state is given by \( x_0 \sim \mathcal{N}(0, L^{-1}) \). A state-feedback controller

\[
u_t = F x_t
\]

which is installed on a computer over a network, e.g., cloud, is employed for stabilizing (1), where a feedback gain \( F \) is to be designed. Note that output-feedback controllers can also be considered although we use a state-feedback controller for the simplicity of discussion.

The networked control system with (1) and (2) has risks of eavesdropping attacks because the plant and controller communicate with each other via network links. This study considers the encrypted control proposed in [20] as a secure control framework against the attacks. An encrypted control system includes an encrypter Enc and decrypter Dec in its feedback loop; see Fig. 1. Note that a sensor (encrypter) and an actuator (decrypter) in this study are assumed to be installed on a unified computer of plant side. An encrypted controller of (2) with multiplicative homomorphic encryption of Definition 3 is defined as

\[
(c_F, c_{x_t}) \mapsto u_{t} = \begin{bmatrix} c_{F_1} \oplus c_{x_{t,1}} & \cdots & c_{F_{1,n}} \oplus c_{x_{t,n}} \\ \vdots & \ddots & \vdots \\ c_{F_{m,1}} \oplus c_{x_{t,1}} & \cdots & c_{F_{m,n}} \oplus c_{x_{t,n}} \end{bmatrix}
\]

where \( c_F = \text{Enc}(pk, F) \), and \( c_{x_t} = \text{Enc}(pk, x_t) \). An input is restored as

\[
u_t = \begin{bmatrix} \sum_{j=1}^{n} \text{Dec}(sk, c_{U_{j,1}}) \\ \vdots \\ \sum_{j=1}^{n} \text{Dec}(sk, c_{U_{j,n}}) \end{bmatrix}
\]

and it approximately equals an input of (2) if quantization errors caused by the encryption are sufficiently small. Thus, the dynamics of the encrypted control system is obtained as

\[
x_{t+1} = A x_t + w_t, \quad A := A_p + B_p F
\]

By using an encrypted control framework, conventional controllers can be used while their gains and signals over network links are encrypted.

We consider an attack scenario to identify the dynamics of the encrypted control system. The dynamics must be secret even though an adversary eavesdrops and deciphers the ciphertexts because he/she would exploit it as an initial step for executing more sophisticated attacks, such as stealth attacks. As a result, the total security level of encrypted control systems can be improved by preventing the identification attack. The worst scenario for a defender is a Bayesian estimation of the dynamics, i.e., \( A \) in (3), with deciphered data because the estimation is the best in terms of the variance of estimator. This attack is formulated as follows.

Definition 4: An adversary follows the protocol in the following.

1) Given \( T \in \mathbb{Z}^+ \), collect \( D_{\text{Enc}} := \{\text{Enc}(pk, x_t)\}_{t=0}^T \) by eavesdropping attacks.
2) \( D := \{ x_t \}_{t=0}^T \) by breaking the ciphertexts in \( D_{\text{Enc}} \) using a computer of which performance is \( \Upsilon \) floating-point operations per second (FLOPS).

3) Choose a prior probability \( p(A) = f(\text{vec}(A); \mu, \Lambda^{-1}) \) based on his/her knowledge about a target control system. Then, estimate a posterior probability \( p(A|D) = f(\text{vec}(A); \tilde{\mu}(T), \Lambda^{-1}(T)) \) by Bayesian estimation with \( p(A) \) and \( D \).

An adversary aims to identify a system matrix \( A \) as a posterior probability \( p(A|D) \), and an estimation \( \hat{A} \) is given by \( \text{vec}(\hat{A}) = \tilde{\mu}(T) \).

Is the encrypted control system secure under what conditions in these settings? In this article, the system is said to be secure if identification of \( A \) with a certain precision is impossible within a given period. In particular, the security in the attack scenario is defined as follows, where we use the fact that the trace of a variance–covariance matrix can be used for a measure of the precision of the estimation since it represents the total variance:

**Definition 5:** Let \( \tau_c \) be a life span that represents a period until system (1) is replaced and \( \gamma_c \) be an acceptable variance against adversary’s estimation. Define

\[
\tau(T, k) := \text{time for executing step 2) in Definition 4.}
\]

The encrypted control system in Fig. 1 is said to be secure if there does not exist \( T \in \mathbb{Z}^+ \) satisfying

\[
\mathbb{E} \left[ \text{tr}(\hat{A}^{-1}(T)) \right] < \gamma_c \land \tau(T, k) \leq \tau_c
\]  

(4)

where \( \hat{A}(T) \) is defined in Definition 4. If not, the system is said to be insecure.

In Definition 5, \( \tau_c \) and \( \gamma_c \) are the design parameters while the key length \( k \) and the controller \( F \) are the implicit decision variables. As \( \gamma_c \) is taken larger for protecting the system during a longer period, the key length \( k \) would be longer [37]. Although the longer \( k \) is beneficial for ciphertext strength, it is not desirable in terms of implementation costs because the online computation costs of \( \text{Enc} \) and \( \text{Dec} \) with longer \( k \) have to be larger [38]. In other words, the choice of a longer key length increases economic costs since a high performance computer is required for keeping the real-time operation of the control system. Since there is such a tradeoff, we will design \( F \) for making the key length as short as possible. Later, we will show that the ease of identification relates to the stability of \( A \) in (3). This implies that the choice of a good controller \( F \) can make the key length \( k \) shorter while making the precision of identification within the tolerance \( \gamma_c \). In this light, we consider the following design problem for ensuring the dynamical system security.

**Problem 1:** Consider the encrypted control system in Fig. 1 under the attack scenario in Definition 4. Find \( F \) and a minimum \( k \in (0, \infty) \) such that the system is securely defined in Definition 5.

An essential question behind Problem 1 is how the key length \( k \), controller \( F \), and the number of deciphered samples \( T \) relate to the security. The factors \( k \) and \( T \) are often taken into account in cryptography [34] and sample complexity of computational learning theory [39], respectively. Unlike this, we have to explicitly consider the controller gain as well as those two factors because the system of our interest has dynamics. In view of this, Problem 1 lies in between cryptography, learning theory, and control theory. In the next section, we analyze the relation among \( k, T, F \), and the security.

**Remark 1:** Additive homomorphic encryption can also be used instead of using multiplicative homomorphic encryption. In such a case, an encrypted controller is defined as \( (F, c_{x_t}) \mapsto c_{u_t} = [F_{11}c_{x_{t,1}} \oplus \cdots \oplus F_{1n}c_{x_{n,1}}, \cdots, F_{mn}c_{x_{n,m}}] \) and an input is given by \( u_t = \text{Dec}(sk, c_{u_t}) \).

Note that the encrypted controller has an uncrypted parameter \( F \), unlike the one with multiplicative homomorphic encryption.

**Remark 2:** Although most algorithms to recover \( D \) from \( D_{\text{Enc}} \) would include integer operations rather than floating-point operations, the computational ability for integer operations in this study is assumed to be quantified by FLOPS.

**Remark 3:** So far, we have assumed that an adversary can exactly recover \( D \) from \( D_{\text{Enc}} \) without quantization errors caused by the encryption. In practice, \( \text{Enc} \) and \( \text{Dec} \) in Fig. 1 have to be equipped with an encoder \( \text{Ecd} : \mathbb{R} \rightarrow M \) and decoder \( \text{Dcd} : M \rightarrow \mathbb{R} \) that convert real numbers \( (F, x_t) \) to a plaintext space because the most existing homomorphic encryption schemes rely on arithmetic operations over integers. Therefore, quantization errors are always involved in the deciphered samples. However, for simplifying the following arguments, we do not consider the error, which is the worst-case scenario for the defender. The details of the quantization error analysis are described in Appendix A.

**Remark 4:** An adversary of this study is assumed to estimate a system matrix \( A \) in (3). One may think that considering an estimation attack for a controller gain \( F \) in (2) is also important. The attack can be treated as solving simultaneous equations for \( F \) with \( N \) independent data sets of \( x \) and \( u \). In such a case, the encrypted control system is said to be secure if \( \tau(N, k) \leq \tau_c \) is satisfied.

### IV. Sample Identifying-Complexity Curve and Sample Deciphering-Time Curve

This section introduces two novel quantities referred to as sample identifying-complexity curve and sample deciphering-time curve to clearly understand the relationship among \( k, T, F \), and the security.

#### A. Sample Identifying-Complexity Curve

We introduce the following lemma that connects the notion of the security in Definition 5 to the dynamics of (3).

**Lemma 1:** Consider the system in Fig. 1 under the attack in Definition 4. Suppose \( A \) in (3) is Schur. Then, the parameters of a posterior probability \( p(A|D) \) in Definition 4 are described as

\[
\hat{A}(T) = \Lambda + \sum_{t=0}^{T-1} (x_t \otimes I) L(x_t \otimes I)^\top,
\]

(5)

\[
\hat{\mu}(T) = \hat{A}^{-1}(T) \left( \Lambda \mu + \sum_{t=0}^{T-1} (x_t \otimes I) L x_{t+1} \right).
\]

(6)
Besides, the following relations hold:

\[
\text{tr}(\hat{\Lambda}^{-1}(T)) \geq \frac{n^2}{\text{tr}(\Lambda) + \text{tr}(L) \sum_{t=0}^{T-1} ||x_t||^2},
\]

(7)

\[
\mathbb{E}\left[\text{tr}(\hat{\Lambda}^{-1}(T))\right] \geq \gamma(T, F) := \frac{n^2}{\text{tr}(\Lambda) + \text{tr}(L) \sum_{t=0}^{T-1} \text{tr}\left(\sum_{i=0}^{t} A^i L^{-1}(A^i)\right)},
\]

(8)

**Proof:** See Appendix C.  

Note here that the term \( \sum_{i=0}^{t} A^i L^{-1}(A^i) \) is the weighted finite-time controllability gramian of (3). Lemma 1 shows that the quantification \( \mathbb{E}[\text{tr}(\hat{\Lambda}^{-1}(T))] \) in (4) can be bounded from below by using the trace of the gramian. We refer to the bound \( \gamma \) as sample identifying-complexity curve due to the acknowledgment that the curve captures the complexity of the identification of \( \text{vec}(A) \) with \(|\mathcal{D}| = T + 1 \) samples. It should be noted here that the system trajectory \( x_t \) explicitly depends on the controller gain \( F \). Thus, the curve is a function of \( T \) and \( F \). We can see the following two observations from (8).

1) Dependency of \( F \): The sample identifying complexity is larger if \( F \) makes the stability degree measured by the trace of the controllability gramian smaller. This is natural because as the system is more stable, the amount of information, i.e., the system output driven by the initial state and external input \( w \), can be less, thereby making the identification more difficult.

2) Dependency of \( T \): The sample identifying complexity is larger if the number of deciphered samples is lesser. This implies that the identification is difficult for the adversary by decreasing leaked data samples.

Fig. 2(a) depicts the schematic picture of the curve \( \gamma(T, F) \). Although \( F \) is an \( m \)-by-\( n \) matrix, in the figure, larger \( F \) implies the one making \( A \) in (3) more stabilized.

When a sample size \( T \) is sufficiently large, the summation terms in (5) and (6) should be much larger than the terms \( \Lambda \) and \( \Lambda \mu \), respectively. Then, the estimates \( \hat{\Lambda} \) and \( \hat{\mu} \) satisfy the following relation to an estimation error.

**Corollary 1:** If a sample size \( T \) is sufficiently large, then \( \hat{\Lambda}(T) \) in (5) satisfies

\[
\mathbb{E}\left[||A - \hat{A}||_F^2\right] = \mathbb{E}\left[\text{tr}(\hat{\Lambda}^{-1}(T))\right]
\]

(9)

where \( \text{vec}(\hat{A}) = \hat{\mu}(T) \), and \( \hat{\mu}(T) \) is given by (6).

**Proof:** See Appendix D.  

Note that the equalities (8) and (9) show that the sample identifying complexity is a lower bound of a type of estimation error with a sufficiently large sample. Thus, it is reasonable that the difficulty of identifying a system matrix is quantified by the sample identifying complexity.

For the following argument, we show a special case when \( L^{-1} = \sigma^2 I \) and the adversary has no prior information about the system, i.e.,

\[
\text{tr}(\Lambda) = 0.
\]

(10)

Then, the following corollary immediately follows from Lemma 1.

**Corollary 2:** If \( L^{-1} = \sigma^2 I \) and (10) hold, then \( \gamma \) in (8) satisfies

\[
\gamma(T, F) = \frac{n}{\sum_{t=0}^{T-1} \text{tr}\left(\sum_{i=0}^{t} A^i (A^i)^\top\right)}.
\]

(11)

**Proof:** See Appendix E.
The sample identifying-complexity curve connects the relationship between the sample complexity $E[\text{tr}(\hat{\Lambda}^{-1}(T))]$ in Definition 5 and a pair $(T, F)$. Before showing how this is useful for solving Problem 1, we next show a different curve that connects the security to $T$ and a key length $k$.

Remark 5: We have introduced the expectation of a lower bound of $\Lambda^{-1}$ because the computation of the inverse of $\Lambda$, in general, requires a large number of computation resources, and it cannot be computed in advance of the control system's operation. A similar approach can be found in [40]–[43], and the studies employed the inverse of a trace of the Fisher information matrix as a lower bound of the precision of general unbiased estimator for dynamical systems. Unfortunately, the approach is not specialized in our attack scenario, i.e., it would give a loose lower bound of $\text{tr}(\hat{\Lambda}^{-1})$, and the lower bound cannot be computed without the system's operating data.

### B. Sample Deciphering-Time Curve

In this article, we refer to $\tau(T, k)$ in (4) as sample deciphering-time curve due to the acknowledgment that the curve captures the computation time for deciphering the $T + 1$ ciphertexts of $D_{\text{Enc}}$. One might consider that the deciphering time does not depend on the number of samples. This is true in a traditional setup of public-key encryption, referred to as static-key encryption in this article, where the keys used for encrypting all samples are identical [34]. On the other hand, when the keys of individual samples are completely different, in other words, dynamic-key encryption is used [33], the deciphering-time clearly depends on the number of samples. We show an explicit representation of $\tau(T, k)$ for each encryption scheme and show an advantage of the dynamic case in terms of the security in Definition 5.

1) **Static-Key Case:** As a multiplicative homomorphic encryption scheme, this study uses the ElGamal encryption $E$ described in Section II. The security of $E$, i.e., the difficulty of breaking the encryption, is based on the hardness of the discrete logarithm problem (DLP) for $G$ that is defined as follows.

**Definition 6 (Discrete logarithm problem [44]):** Let $G$ be a group with a binary operation $\circ$. The DLP for $G$ is to determine, for any given elements $g, h \in G$, an integer $x$ satisfying

$$g^x = g \circ g \circ \cdots \circ g = h.$$ 

Additionally, the assumption that there does not exist a polynomial-time algorithm to solve the DLP is called the discrete logarithm assumption.

In the field of cryptography, the discrete logarithm assumption is widely believed to be satisfied. The ElGamal encryption achieves indistinguishability against chosen-plaintext attacks (IND-CPA) under the decisional Diffie–Hellman (DDH) assumption [34] that is a variant of the discrete logarithm assumption. The security level of IND-CPA means that an adversary can obtain no information about plaintexts from ciphertexts. Hence, an adversary must solve the DLP for $G$ to obtain $D$ from $D_{\text{Enc}}$. The majority of algorithms for solving the DLP for a finite field $\mathbb{F}_\eta$, with a modulus $\eta$ are subexponential-time algorithms of which computation time is described as

$$L_{c,d}(\eta) = \exp\{d(\ln \eta)^v/(\ln \eta)^{1-v}\}$$

(12)

where $v$ and $d$ are algorithm parameters [44]. For instance, the general number field sieve, the known fastest classical subexponential-time algorithm, has $v = 1/3$ and $d = (64/9)^{1/3}$ in (12) [37]. Thus, we use

$$L(k) := L_{1/3,(64/9)^{1/3}}(2^k)$$

(13)

as the computation time for deciphering a ciphertext of $E$ with a key length $k$ in the following. Note that $G \subset \mathbb{F}_p$, and $L(k)$ satisfies $L(k) \leq L_{1/3,(64/9)^{1/3}}(p)$ since $p \in (2^k, 2^{k+1})$. Therefore, (13) is stricter with a defender than (12).

We next show the sample deciphering time of the static-key encryption. Since a single key pair is used for encrypting all the samples throughout a life span of the encrypted control system, the adversary has to break only one ciphertext for finding the secret key. Once the secret key is found, he/she can decrypt all ciphertexts of $D_{\text{Enc}}$ immediately. Thus, the sample deciphering time in this case can be described as

$$\tau(0, k) = \frac{L(k)}{\Upsilon}$$

(14)

where $\Upsilon$ is defined in Definition 4. For satisfying the second inequality of (4), the key length $k$ will be long because not even one ciphertext can be broken during a given period $\tau_c$. Although it is natural from the ordinary manner in cryptography, the online computation costs of the associated Enc and Dec in Fig. 1 must be heavy, which is not desirable for real-time controls.

Remark 6: The number field sieve is used for solving not only the DLP but also the prime factorization problem. Thus, (14) also enables to estimate the computation times for breaking other encryption schemes, such as Rivest-Shamir-Adleman (RSA) encryption [45] and Paillier encryption [46]. Moreover, we can change $L(k)$ according to any given encryption scheme such as the Lenstra-Lenstra-Lovász (LLL) algorithm for lattice and fully homomorphic encryption, and, therefore, the sample deciphering time can be obtained for any encryption scheme as well.

2) **Dynamic-Key Case:** One way to reduce the online computational costs of Enc and Dec while keeping the sample deciphering time long is to regenerate a secret key at each sampling time. However, this approach is not suitable for real-time controls due to the high computational costs. As an alternative approach, we employ the dynamic-key encryption [33] that is an augmented concept of public-key encryption. The overview is as follows: First, give a key pair by Gen at the initial time. The secret key at time $t + 1$ is computed by a simple updating rule based on a modulus operation with a random number and the secret key at time $t$. At the same time, a public key and ciphertexts of controller parameters are also updated to keep the correctness, i.e., the property that a ciphertext is decrypted correctly, with the new secret key. Due to the time-dependency of this dynamic-key encryption, the adversary would have to break $T + 1$ ciphertexts to collect $D$ from $D_{\text{Enc}}$. However, the security proof of the dynamic-key encryption has not yet been shown. Additionally, the dynamic-key encryption refreshes only
the second element of ciphertext, and so the first element remains the same value. In the following, we extend the dynamic-key encryption in [33] to update all components of ciphertext and provide the security proof of the scheme.

The dynamic ElGamal encryption in this study is constructed as follows.

**Definition 7:** Dynamic ElGamal encryption is a tuple $E_{\text{dyn}} := (\text{Gen, Enc, Dec, } T_K, T_C)$ with the transition maps $T_K : ((p, q, g, h), s) \rightarrow ((p, q, g, pg^s \mod p), s + s' \mod q)$, $T_C : (c_1, c_2) \rightarrow (c_1g^r \mod p, (c_1g^r)^*c_2h^r \mod p)$ where $r', s' \sim U(\mathbb{Z}_q)$.

**Remark 7:** The random number $s'$ needs to be shared secretly between a sensor and an actuator if they are installed on different places. This can be achieved by using a standard symmetric-key encryption scheme, such as advanced encryption standard (AES). Similarly, a plant can transmit $r'$ and $s'$ to an encrypted controller secretly.

In Definition 7, $T_K$ and $T_C$ imply updating rules for a key pair and ciphertext, respectively. $T_C$ of the dynamic ElGamal encryption updates both $c_1$ and $c_2$ unlike the scheme in [33]. We first show that the correctness and multiplicative homomorphism of our encryption scheme are satisfied even though the transition map is modified.

**Proposition 1:** Let $k$ be a key length, $(pk_0, sk_0) = \text{Gen}(k)$, and $c_0 = \text{Enc}(pk_0, m)$. If $(pk_{t+1}, sk_{t+1}) = T_K(pk_t, sk_t)$ and $c_{t+1} = T_C(c_t)$, then

$$\text{Dec}(sk_t, c_t) = \text{Dec}(sk_t, \text{Enc}(pk_t, m)) = m \mod p$$

for all $m \in \mathcal{M}$ and $t \in \mathbb{Z}^+$. Furthermore, the multiplicative homomorphism

$$\text{Dec}(sk_t, c_t \ast \text{Enc}(pk_t, m') \mod p) = mm' \mod p$$

is satisfied for all $m, m' \in \mathcal{M}$ and $t \in \mathbb{Z}^+$. 

**Proof:** See Appendix F.

Due to the homomorphism, the dynamics of the encrypted control system in Fig. 1 with the dynamic-key encryption scheme $E_{\text{dyn}}$ can be regarded as (3) while the key pair and ciphertexts are dynamically updated.

We next show an explicit representation of the sample deciphering-time curve $\tau(T, k)$ when $E_{\text{dyn}}$ is used. To this end, we show a cryptographic property of the transition maps $T_K$ and $T_C$.

**Proposition 2:** Let $k$ be a key length, $(pk_0, sk_0) = \text{Gen}(k)$, $m \in \mathcal{M}$, and $c_0 = \text{Enc}(pk_0, m)$. A key pair and ciphertext are updated by $(pk_{t+1}, sk_{t+1}) = T_K(pk_t, sk_t)$ and $c_{t+1} = T_C(c_t)$, respectively. Suppose an adversary knows $pk_t$, $sk_t$, and $c_t$ and can solve the DLP for $\mathbb{G}$. There exists a negligible function $\epsilon(k)$ such that

$$\Pr(sk_{t+1} = pk_{t+1}) < \epsilon(k) \land \Pr(sk_{t-1} = sk_{t-1}) < \epsilon(k)$$

for all $t \geq 1$, where $sk_{t+1}$ and $sk_{t-1}$ are adversary’s estimations of $sk_{t+1}$ and $sk_{t-1}$, respectively.

**Proof:** See Appendix G.

Proposition 2 implies that if we use the dynamic ElGamal cryptosystem, the probability that an adversary can obtain the secret keys at times $t+1$ and $t-1$ is negligibly small even though he/she knows all information at time $t$ including the information given by solving the DLP for $\mathbb{G}$ as long as the updates of a key pair and ciphertexts are performed secretly. This fact derives the following proposition on the security of our encryption scheme.

**Proposition 3:** $E_{\text{dyn}}$ satisfies IND-CPA at time $t$ under the DDH assumption even though an adversary knows $\{pk_t\}_{t=0}^{t-1}$ and $\{sk_t\}_{t=0}^{t-1}$.

**Proof:** See Appendix H.

From Propositions 2 and 3, an adversary cannot obtain any information about a secret key and plaintext for all time $t$ even though he/she has secret keys at time $t - 1$ and $t + 1$. Thus, he/she must solve the DLP for $\mathbb{G}$ $T+1$ times to collect $D$ from $D_{\text{Enc}}$. Therefore, the computation time for deciphering ciphertexts of $D_{\text{Enc}}$ is linearly increased from $\tau(0, k)$ as a sample size of $D_{\text{Enc}}$ increases if $E_{\text{dyn}}$ is used. Thus, the following lemma is derived.

**Lemma 2:** A sample deciphering-time curve of the encrypted control system in Fig. 1 with $E_{\text{dyn}}$ in Definition 7 is given as

$$\tau(T, k) = \frac{(T + 1)L(k)}{\Upsilon}$$

where $L(k)$ and $\Upsilon$ are defined in (13) and Definition 4, respectively.

Note that the sample deciphering time of the static-key case corresponds to (15) with $T = 0$. It should be noted here that the curve $\tau(T, k)$ monotonically increases as either of $T$ and $k$ increases. A schematic picture of the sample deciphering-time curve is shown in Fig. 2(b).

In conclusion, for the encrypted control system in Fig. 1 with $E_{\text{dyn}}$ in Definition 7, we have introduced the following two curves:

1) $\gamma(T, F)$ in (8) that characterizes the difficulty of identifying the system (3);
2) $\tau(T, k)$ in (15) that quantifies the difficulty of deciphering encrypted samples.

In Section V, we show how these two curves are useful for solving Problem 1.

V. OPTIMAL KEY LENGTH AND CONTROLLER DESIGN

For simplifying the following discussion, we suppose that the assumptions in Corollary 2 hold. From Definition 5 and Corollary 2, the following immediately follows: Given $k$ and $F$, if there does not exist $T$ satisfying

$$\gamma(T, F) < \gamma_c \land \tau(T, k) \leq \tau_c$$

where $\gamma$ and $\tau$ are, respectively, in (11) and (15), and then the encrypted control system in Fig. 1 with $E_{\text{dyn}}$ in Definition 7 and $(k, F)$ is secure. An idea for designing a key length and controller based on the sample identifying-complexity curve $\gamma$ and sample deciphering-time curve $\tau$ is as follows.

1) Controller design: Note from (11) that the identification variance monotonically decreases as the number of samples increases because the finite-time controllability
gramian
\[ W_t := \sum_{i=0}^{t} A^i(A^i)^\top \]  
(17)
is positive definite. Thus, we should design the controller \( F^* \) that maximizes the minimum time step \( T^* \) satisfying\[ \gamma(T^*, F^*) < \gamma_c. \]

2) Key length design: The computation time for deciphering \( |D_{\text{Enc}}| = T^* + 1 \) ciphertexts is \( \tau(T^*, k) \), and the time monotonically increases in a key length \( k \). Considering that a key length is desirable to be as small as possible from the perspective of computational costs, it should be designed as the minimum key length \( k^* \) satisfying\[ \tau(T^*, k^*) > \tau_c. \]
The pair \((k^*, F^*)\) is a solution to Problem 1 since there does not exist \( T \) satisfying (16) with \((k^*, F^*)\). Note here that the controller \( F^* \) simultaneously minimizes the trace of \( W_t \) in (17) of (3). Hence, the controller also improves the stability of the control system, which will be discussed later. In the following, the concrete design processes of \( k^* \) and \( F^* \) are described.

A. Controller Design

Following the controller design step, we design \( F^* \) so that the minimum time step \( T^* \) satisfying the first inequality of (16) is as large as possible. From (7), this design can be solved by making the cost function
\[ J_T := \mathbb{E} \left[ \sum_{t=0}^{T-1} \|x_t\|^2 \right] \]
as small as possible. Since this is a finite-horizon stochastic linear quadratic regulator (s-LQR) design problem, an optimal solution is given as follows.

**Lemma 3:** Consider the system (3) and \( J_T \) in (18). Assume that \( B_p \) is full column rank. Then, the control sequence
\[ u_t = -(B_p^T P_{t+1} B_p)^{-1} B_p^T P_{t+1} A_p x_t, \quad t \in [0, T) \]
(19)
iminizes \( J_T \), where
\[ P_t = A_p^T P_{t+1} A_p - A_p^T P_{t+1} B_p (B_p^T P_{t+1} B_p)^{-1} B_p^T P_{t+1} A_p + I \]
and \( P_T = I \).

**Proof:** See Appendix I.

Although the control (19) is optimal, the resultant controller has to be time-varying. Unfortunately, time-varying controllers are difficult to be used in the encrypted control framework because controller parameters must be encrypted and stored in advance before controller operation due to the difficulty of encrypted controller parameters update. On the other hand, as \( T \rightarrow \infty \), the control law converges to \( u_t = F^* x_t \) with
\[ F^* = -(B_p^T P_{t+1} B_p)^{-1} B_p^T P_{t+1} A_p \]
(20)
where \( P > 0 \) is the solution to the discrete-time algebraic Riccati equation
\[ P = A_p^T P A_p - A_p^T P B_p (B_p^T P B_p)^{-1} B_p^T P A_p + I. \]
Hence, as a suboptimal solution to make \( J_T \) as small as possible, we use the static feedback gain \( F^* \) in (2). It is interesting that the standard stochastic cheap control (19) is a good solution from the perspective of the security. This fact clearly connects the notion of the security and classical control theory. Moreover, the fact means that no tradeoff between the security and the control performance exists in controller design under the adversary of Definition 4. In other words, whenever the defender wants \( F^* \) in (20) for improving closed-loop damping performance, the controller is also a good solution in terms of the security.

Once \( F^* \) is designed, the minimum time step \( T^* \) satisfying the first inequality of (16) can be uniquely determined as follows:
\[ T^* = \arg \min_T E(T), \quad E(T) := \sum_{t=0}^{T-1} \text{tr}(W_t) \]
s.t. \[ E(T) > \frac{n}{\gamma_c} \]
(21)
where \( W_t \) is defined in (17). An illustrative interpretation of this optimization is shown by the red line in Fig. 2(a). It should be noted here that \( T^* \) in (21) can be determined for any controller as long as \( A \) in (3) is Schur. However, \( T^* \) in this case will be larger than the one when \( F^* \) in (20) is used. This choice, as we will show later, induces a longer key length. For tractable computation of \( E(T) \), we introduce the following proposition.

**Proposition 4:** The summation of trace of a finite-time controllability gramian \( E(T) \) in (21) can be computed as
\[ E(T) = \begin{cases} \frac{n_t}{2}, & T = 1, \\ 2n + \text{tr}(A A^\top), & T = 2, \\ 2 E(T - 1) - E(T - 2) + \text{tr}(A^T (A^{T-1})^\top), & T \geq 3. \end{cases} \]

**Proof:** See Appendix I.

Although the computational complexity for computing \( E(T) \) by the definition is more than \( O(T^2) \), that by (21) can be reduced to \( O(T) \), which facilitates the optimization problem (21). The obtained \( T^* \) is used for designing the minimum key length design problem, which is described in the next section.

B. Key Length Design

Suppose that \( T^* \) is given by (21). Following the key length design step, we find a minimum key length \( k^* \) such that the second inequality of (16) does not hold. It follows from the second inequality of (16) and \( \tau(T, k) \) in (15) that the key length minimization can be summarized as
\[ k^* = \arg \min_k L(k) \quad \text{s.t.} \quad L(k) > \frac{\tau_Y T^*}{T^* + 1}. \]
(22)
An illustrative interpretation of this optimization is shown by the red line in Fig. 2(b).

In conclusion, we have the following theorem.

**Theorem 1:** Consider Problem 1 with the assumptions in Corollary 2. The controller \( F^* \) and the minimum key length \( k^* \) are given by (20) and (22), respectively. Then, the encrypted control system in Fig. 1 with the dynamic-key encryption scheme \( E_{\text{dyn}} \) in Definition 7 is secure.

**Proof:** See Appendix K.
Algorithm 1: Optimal design of encrypted control system with dynamic-key encryption.

**Input:** $A_p, B_p, n, \gamma_c, \tau_c, \text{ and } T$.

**Output:** $F^*$ and $k^*$.

1. **# Controller design.**
   - Solve $P = A_p^T P A_p - A_p^T P B_p (B_p^T P B_p)^{-1} B_p^T P A_p$.
   - $F^* = (B_p^T P B_p)^{-1} B_p^T P A_p$.

2. **# Solve optimization problem of (21).**
   - $A \leftarrow A_p + B_p F^*$.
   - $x \leftarrow n, y \leftarrow 0, z \leftarrow 0, T^* \leftarrow 1$.
   - While $x \leq n/\gamma_c$ do
     - $T^* \leftarrow T^* + 1$.
     - $z \leftarrow y$.
     - $y \leftarrow x$.
     - $x \leftarrow 2y - z + \text{tr}(A T^* - 1 (A T^* - 1)^T)$.
   - End while

3. **# Solve optimization problem of (22).**
   - $k^* \leftarrow 1$.
   - While $L(k^*) \leq \tau_c T/(T^* + 1)$ do
     - $k^* \leftarrow k^* + 1$
   - End while

   Return $F^*, k^*$.

A pseudocode of the design algorithm is summarized as Algorithm 1.

C. Other Design Problems

The parameters of a sample identifying-complexity curve $\gamma(T, F)$ and a sample deciphering-time curve $\tau(T, k)$ are a time step $T$, controller $F$, and key length $k$. The optimal key length $k^*$ in Problem 1 is derived under a given controller $F^*$. Similarly, by fixing $T$ or $k$, the curves can be used for formulation of other design problems.

For example, a problem to design a controller gain $F$ under a given key length $k$ is a reverse problem of Problem 1. A degree of freedom in design of $F$ in this problem is restricted by $k$ through the minimum time step $T^*$ satisfying $\tau(T^*, k) > \tau_c$. That is, a defender wants to find $F$ achieving a certain degree of stability of a control system, which is implicitly parameterized by $k$.

Furthermore, a problem to design $F$ and $k$ under the given time step $T = \tau_c/T_s$ is a variant of Problem 1, where $T_s$ is a sampling time. An adversary in the variant is weaker than the one in Problem 1 because he/she uses all data within the life span for the estimation. Thus, a defender would be required to design a finite-horizon controller maximizing $\gamma(T, F)$ and smaller key length than the solution to Problem 1.

VI. NUMERICAL SIMULATION

Consider (1) with

$$A_p = \begin{bmatrix} 1 & 0.5 \\ 0 & -1.2 \end{bmatrix}, \quad B_p = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad L = \begin{bmatrix} 10^4 & 0 \\ 0 & 10^4 \end{bmatrix}.$$
We next compute the sample deciphering-time curves $\tau(T^*_k, k)$ and $\tau(T^*_k, +1)$ in (15), and $\tau(0, k)$ in (14) for a comparison purpose. Note here that the first (respectively second) represents the time for deciphering $T^*_k + 1$ (respectively $T^*_k + 1$) ciphertexts of the dynamic ElGamal encryption $E_{\text{dyn}}$ in Definition 7 while the third represents that for deciphering any ciphertext of the normal ElGamal encryption $E$. Note that the third case is irrelevant to controllers because the encryption is static-key encryption. Fig. 5 illustrates those three curves for $k$. Let a life span and a computer performance be chosen as $\tau_c = 1.5768 \times 10^9$ s (50 years), which is denoted by the dashed line in the figure, and $\Upsilon = 442 \times 10^{15}$ FLOPS, which is the performance of Fugaku supercomputer. Then, by solving (22), the optimal key length for each cases is determined to be 641, 734, and 1091 bits. This result implies that the simultaneous use of the dynamic-key encryption and the s-LQR optimal controller can drastically reduce the key length while keeping the security level of the encrypted control system, thereby reducing its computation costs.

Finally, we show how the differences of those three key lengths appear in the online computation times. All the computations are done by using MacBook Pro (macOS Big Sur, 2.3 GHz quad-core Intel Core i7, 32 GB 3733 MHz LPDDR4X) with C++. The results are shown in Table I. Fig. 6 depicts the average computation times of $E_{\text{dyn}}$, $F$, and $T_K$. The optimal key length and controller effectively reduced the implementation costs of encrypted control systems while keeping their security level.

**VII. CONCLUSION**

This article addressed a systematic design of encrypted control systems against eavesdropping attacks to construct secure cyber–physical systems. To quantify the security level of encrypted control systems, the novel security notions, sample identifying complexity and sample deciphering time, were proposed. The sample identifying complexity characterizes the difficulty of system identification by means of a controllability gramian of a closed-loop system. Additionally, the sample deciphering time represents the computation time for breaking ciphertexts to collect a data set for the identification. Combining the notions, the optimal key length was determined as the minimum key length enough to prevent the identification with a given precision within a life span of the system. The numerical simulations demonstrated that the optimal key length and controller effectively reduced the implementation costs of encrypted control systems while keeping their security level.

To our best knowledge, this article is the first work to reveal the relationship between the cryptographic security and dynamical systems in a control-theoretic manner. One might think that some papers already related security level and properties of control systems [3], [11]–[15]. However, these studies considered only the control-theoretic aspect of the impact of cyber-attacks, namely resilience, performance degradation, and detectability. In contrast, our approach connected the effect of eavesdropping computation of encrypted control systems includes $n$ times of $E_{\text{enc}}$ and $mn$ times of $E_{\text{dec}}$ on a plant side. Hence, for larger dimensional systems, the proposed design methodology would be helpful for real-time controls while keeping the security level theoretically.
attacks and the characteristics of dynamical systems taking the feasibility of the attacks into consideration in terms of a computation time.

In this article, the precision of adversary’s estimation was evaluated based on a variance, i.e., the second moment about a mean. However, we did not consider the first moment about the origin of the estimation. In fact, although the estimator (6) is a consistent estimator, it is not a non-biased estimator. Hence, the adversary would obtain the estimates including a bias with a precision evaluated by the second moment. This means that the security evaluation of this article is strict with a defender. We will modify the proposed method to consider both the first and second moments.

Moreover, the estimation of system and input matrices of (1) rather than a system matrix of (3) will be considered. This would be achievable by rewriting (1) as

$$\begin{bmatrix} x_{t+1} \\ 0 \end{bmatrix} = \begin{bmatrix} A_p & B_p \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_t \\ u_t \end{bmatrix} + \begin{bmatrix} w_t \\ 0 \end{bmatrix}.$$ 

The equation is the same form of (3), and, thus, the discussions in this article would be extended directly. We will also consider extending the security concepts to be used for more general encrypted control systems, namely dynamic output-feedback controllers and nonlinear plants. This can be achieved, for example, by using the input–output history feedback controller representation [47] and the Koopman operator [48]. The controller representation realizes a dynamic controller as a matrix-vector product form such as (2). The Koopman operator lifts a finite-dimensional nonlinear system to an infinite-dimensional linear system. The proposed scheme can be applied for such systems up to an error due to the truncation of the system dimension.

**APPENDIX**

**A. Quantization in Encrypted Control**

This section describes the properties of quantization errors in encrypted control systems with a linear controller

$$f : (\Phi, \xi) \rightarrow \psi = \Phi \xi$$

where $\Phi \in \mathbb{R}^{\alpha \times \beta}$ is a controller parameter matrix, $\xi \in \mathbb{R}^\beta$ is a controller input vector, which consists of a controller state and plant output, and $\psi \in \mathbb{R}^\alpha$ is a controller output vector, which consists of a controller state update and plant input. In this case, an encrypted controller of (23) with the ElGamal encryption $E$ is given as

$$f_E : (c_\Phi, c_\xi) \rightarrow c_\psi$$ (24)

where $c_\Phi = \text{Enc}(pk, m_\Phi)$, $c_\xi = \text{Enc}(pk, m_\xi)$, $c_{\psi_{ij}} = c_{\Phi_{ij}} \mod p$, and $m_\Phi$ and $m_\xi$ are plaintexts of $\Phi$ and $\xi$, respectively.

For implementation of the encrypted controller (24), $\xi$ and $\Phi$ must be encoded into plaintexts before encryption and be decoded to real numbers after decryption using an encoder and decoder because a plaintext space is not a set of real numbers. This study uses the following encoder $\text{Ecd}_\Delta : \mathbb{R} \rightarrow \mathcal{M}$ and decoder $\text{Dcd}_\Delta : \mathcal{M} \rightarrow \mathbb{R}$ with a sensitivity $\Delta > 0$:

$$\text{Ecd}_\Delta : x \mapsto \bar{x} = \min \left\{ \arg \min_{m \in \mathcal{M}} |x/\Delta + p1_\mathbb{Z}_{<\Delta}(x) - m| \right\},$$

$$\text{Dcd}_\Delta : \bar{x} \mapsto \Delta(\bar{x} - p1_{\mathbb{Z}_{<\Delta}}(\bar{x}))$$

where $\mathbb{R}_{<\Delta} = \{ x \in \mathbb{R} \mid x < 0 \}$, $\mathbb{Z}_{<\zeta} := \{ z \in \mathbb{Z} \mid \zeta < z \}$, and $1_{\mathbb{L}(\cdot)}$ is an indicator function that outputs 1 if its argument belongs to a set $\mathbb{L}$; otherwise, it outputs 0. $\text{Ecd}_\Delta$ and $\text{Dcd}_\Delta$ perform elementwise for a vector and matrix.

Define $\mathbb{Q}_\Delta := \text{Dcd}_\Delta \circ \text{Ecd}_\Delta$. Then $\mathbb{Q}_\Delta : x \mapsto \bar{x} = x + \bar{x}$ can be regarded as a quantizer [19]. A quantization error $\bar{x} = \mathbb{Q}_\Delta(x) - x \in \mathbb{R}$ holds

$$|\bar{x}| \leq \Delta d_{\max}/2$$ (25)

where $d_{\max}$ is the maximum difference between two consecutive elements in the plaintext space. The inequality (25) implies that the quantization error decreases as $\Delta$ decreases. Actually, the following propositions on the relationship between quantization errors and a sensitivity hold.

**Proposition 5:** Given the ElGamal encryption $E$ and $f_E$ in (24). Let $(pk, sk) = \text{Gen}(k)$, $m_\Phi = \text{Ecd}_{\Delta}(\Phi)$, $m_\xi = \text{Ecd}_{\Delta}(\xi)$, $c_\Phi = \text{Enc}(pk, m_\Phi)$, and $c_\xi = \text{Enc}(pk, m_\xi)$. Suppose an overflow and underflow do not occur, that is, $||\mathbb{Q}_{\Delta}(\Phi)/\Delta||_{\max}||\mathbb{Q}_{\Delta}(\xi)/\Delta||_{\infty} \leq q$. If $\Delta_{\Phi} \rightarrow 0$ and $\Delta_{\xi} \rightarrow 0$. Then $f_E$ satisfies

$$f^+ \circ \text{Dcd}_{\Delta_{\Phi}} \circ \text{Dec}(sk, f_E(c_\Phi, c_\xi)) = f(\Phi, \xi) = \psi$$

where $f = f^+ \circ f^*$, and the maps $f^+$ and $f^*$ are a multiplication and addition part of $f$ in (23), respectively [20].

**Proof:** From the multiplicative homomorphism of $E$, we have $f^+ \circ \text{Dcd}_{\Delta_{\Phi}} \circ \text{Dec}(sk, f_E(c_\Phi, c_\xi)) = f^+ \circ \text{Dcd}_{\Delta_{\Phi}} \circ f^*(m_\Phi, m_\xi)$. Regardless of the signs of $\Phi_{ij}$ and $\xi_{ij}$, when an overflow and underflow do not occur, then the $(i, j)$ entry of $\text{Dcd}_{\Delta_{\Phi}} \circ f^*(m_\Phi, m_\xi)$ is given as

$$\Delta_{\Phi} \xi_{ij} = (\Phi_{ij}/\Delta_{\Phi} + \delta_{\Phi_{ij}})(\xi_{ij}/\Delta_{\Phi} + \delta_{\xi_{ij}}) = \Psi_{ij} \xi_{ij},$$

where $\Psi_{ij} = \Phi_{ij} + \Phi_{ij} \xi_{ij} + \Phi_{ij} \xi_{ij}, \Phi_{ij} = \Delta_{\Phi} \delta_{\Phi_{ij}} = \mathbb{Q}_{\Delta_{\Phi}}(\Phi_{ij}) - \Phi_{ij}$, and $\xi_{ij} = \Delta_{\xi} \delta_{\xi_{ij}} = \mathbb{Q}_{\Delta_{\xi}}(\xi_{ij}) - \xi_{ij}$. From (25), we obtain

$$\left| \Psi_{ij} \right| \leq \left| \Delta_{\Phi} d_{\max}/2 + \left| \Phi_{ij} \right| \Delta_{\xi} d_{\max}/2 + \Delta_{\Phi} \Delta_{\xi} d_{\max}/4.$$ Therefore, $f^+ \circ \text{Dcd}_{\Delta_{\Phi}} \circ f^*(m_\Phi, m_\xi) = \Psi_{ij} \xi_{ij} = \psi = \Delta_{\Phi} \rightarrow 0$ and $\Delta_{\xi} \rightarrow 0$ because of $\Psi_{ij} \rightarrow 0$.

**Proposition 6:** Let $k$ be a key length of the ElGamal encryption. Suppose $\max(||\Phi||_{\max}, ||\xi||_{\infty})$ exists. Then, there exist sensitivities $\Delta_{\Phi}(k)$ and $\Delta_{\xi}(k)$ satisfying $||\mathbb{Q}_{\Delta_{\Phi}}(\Phi)/\Delta_{\Phi}(k)||_{\max}||\mathbb{Q}_{\Delta_{\xi}}(\xi)/\Delta_{\xi}(k)||_{\infty} \leq q$ such that

$$\lim_{k \rightarrow \infty} \Delta_{\Phi}(k) = 0 \quad \text{and} \quad \lim_{k \rightarrow \infty} \Delta_{\xi}(k) = 0.$$ 

**Proof:** Let $\Delta_{\Phi} = \mathbb{Q}_{\Delta_{\Phi}}(\Phi)$, $\mathbb{Q}_{\Delta_{\Phi}}(\Phi)$, $\xi = \mathbb{Q}_{\Delta_{\xi}}(\xi)$, and $D = \max(||\Phi||_{\max}, ||\xi||_{\infty})$. Then, the inequality $||\mathbb{Q}_{\Delta_{\Phi}}(\Phi)/\max||_{\infty}/||\mathbb{Q}_{\Delta_{\Phi}}(\xi)/\Delta_{\Phi}(k)||_{\infty} \leq q \leq k$ can be deformed as

$$(\Delta_{\Phi} - \max) 2^{-k} = D(2^{-k} - d_{\max}/2)$$

Therefore, $||\mathbb{Q}_{\Delta_{\Phi}}(\Phi)/\max||_{\infty}/||\mathbb{Q}_{\Delta_{\Phi}}(\xi)/\Delta_{\Phi}(k)||_{\infty} \leq \Delta_{\Phi} - \max$ $d_{\max}/2$. By definition, every element in a plaintext space of the ElGamal encryption is quadratic residue modulo
p. The author of [49] shows that the number of consecutive quadratic nonresidues modulo p is at most $O(p^2 + \delta)$ for large $p$ and any positive number $\delta$. This means $d_{\text{max}} \leq 2\left(\frac{1}{2} + o(1)\right)(k+1)$ since $p \in (2^k, 2^{k+1})$, and $\lim_{k \to \infty} 2\left(\frac{1}{2} + o(1)\right) - d_{\text{max}}/2 \geq \lim_{k \to \infty} (2\left(\frac{1}{2} + o(1)\right) - 2\left(\frac{1}{2} + o(1)\right)(k+1) = \infty$. Therefore, $\Delta(k) = \Delta_x(k) \to 0$ as $k \to \infty$.

Proposition 5 shows that an output of $f_\varepsilon$ exactly matches one of $f$ if the sensitivities are zero as long as $\text{Ecd}_\Delta$ and $\text{Dcd}_\Delta$ do not cause an overflow and underflow. Proposition 6 guarantees that such sensitivities exist when a key length is sufficiently large. If a key length is relatively small, then quantization errors cannot be ignored. The quantization errors would degrade the precision of adversary’s estimation of $A$ in (3), that is, the number of data needs to be increased in order to keep the precision of the estimation.

B. Technical Lemmas

This section introduces two technical lemmas used for proofs in the following appendices.

Lemma 4: Let $v \in \mathbb{R}^n$ and $M \in \mathbb{R}^{n \times n}$. Then

$$\text{tr}((v \otimes I)M(v \otimes I)^\top) = \text{tr}(M\|v\|^2).$$

Proof:

$$\text{tr}((v \otimes I)M(v \otimes I)^\top) = \text{tr}\left(\begin{bmatrix} v_1 I & \cdots & m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_n I & \cdots & m_{n1} & \cdots & m_{nn} \end{bmatrix} \begin{bmatrix} v_1 I & \cdots & v_n I \end{bmatrix}\right),$$

$$= \text{tr}(\text{diag}(m_{11}v_1^2, \ldots, m_{nn}v_n^2)),$$

$$= (m_{11} + \cdots + m_{nn})(v_1^2 + \cdots + v_n^2) = \text{tr}(M\|v\|^2).$$

This completes the proof.

Lemma 5: Let $M \in \mathbb{R}^{m \times n}$ be a full column rank matrix, and $P \in \mathbb{R}^{m \times m}$ be a positive definite matrix. Then $M^\top PM$ is positive definite and invertible.

Proof: For any nonzero vector $x \in \mathbb{R}^n$

$$x^\top(M^\top PM)x = (Mx)^\top P(Mx) > 0.$$ Therefore, $M^\top PM$ is positive definite, and this also means that it is invertible.

C. Proof of Lemma 2

Proof: From Bayes’ theorem, the probability density functions in Definition 4 hold $p(A/D) = p(D/A)p(A)/p(D) \propto p(D|A)p(A)$. Additionally

$$p(D|A) = p(x_t) \prod_{t=0}^{T-1} p(x_{t+1}|x_t),$$

$$= p(x_0) \prod_{t=0}^{T-1} f(x_{t+1}; (x_t \otimes I)^\top \text{vec}(A), L^{-1})$$

where $Ax_t = (x_t \otimes I)^\top \text{vec}(A)$. It follows that

$$\ln p(A|D)$$

$$= \ln p(D|A) + \ln p(A) + \text{const},$$

$$= \sum_{t=0}^{T-1} \ln f(x_{t+1}; (x_t \otimes I)^\top \text{vec}(A), L^{-1})$$

$$+ \ln f(\text{vec}(A); \mu, \Lambda^{-1}) + \ln p(x_0) + \text{const},$$

$$= -\frac{1}{2} \sum_{t=0}^{T-1} (x_{t+1} - (x_t \otimes I)^\top \text{vec}(A))^\top L (x_{t+1} - (x_t \otimes I)^\top \text{vec}(A))$$

$$- \frac{1}{2} \ln(\text{vec}(A)^\top \Lambda \text{vec}(A) - 2 \text{vec}(A)^\top \hat{\Lambda} \mu) + \text{const},$$

where

$$\tilde{\Lambda} = \Lambda + \sum_{t=0}^{T-1} (x_t \otimes I)L(x_t \otimes I)^\top,$$

$$\tilde{\mu} = \Lambda^{-1} \left(\Lambda \mu + \sum_{t=0}^{T-1} (x_t \otimes I)Lx_{t+1}\right).$$

That is, $p(A/D) = f(\text{vec}(A); \mu, \Lambda^{-1})$. Furthermore, it follows from Lemma 4 that

$$\text{tr}(\tilde{\Lambda}^{-1}) \geq n^2 \text{tr}(\Lambda)^{-1} = n^2 \left(\text{tr}(\Lambda) + \text{tr}(L) \sum_{t=0}^{T-1} \|x_t\|^2\right)^{-1}. $$

The solution of (3) is $x_t = \sum_{i=0}^{t} A^i w_{t-i-1}$ for all $t \geq 0$, where $w_{-1} := x_0$. Therefore, the sample-identifying complexity curve $\gamma(T, F)$ is given as

$$\gamma(T, F) = \mathbb{E} \left[ n^2 \left(\text{tr}(\Lambda) + \text{tr}(L) \sum_{t=0}^{T-1} \|x_t\|^2\right)^{-1}\right],$$

$$= n^2 \left(\text{tr}(\Lambda) + \text{tr}(L) \sum_{t=0}^{T-1} \text{tr} \left(\sum_{i=0}^{t} A^i \Sigma(A^i)^\top\right)\right)^{-1},$$

where

$$\mathbb{E} \left[\|x_t\|^2\right] = \text{tr} \left(\mathbb{E} \left[\sum_{i=0}^{t} A^i w_{t-i-1} \left(\sum_{i=0}^{t} A^i w_{t-i-1}\right)^\top\right]\right),$$

$$= \text{tr} \left(\sum_{i=0}^{t} A^i \mathbb{E} \left[w_{t-i-1} w_{t-i-1}^\top\right] (A^i)^\top\right),$$

$$= \text{tr} \left(\sum_{i=0}^{t} A^i \Sigma(A^i)^\top\right).$$
This completes the proof.

D. Proof of Corollary 1

Proof: When a sample size $T$ is sufficiently large, the estimates $\hat{\Lambda}$ and $\hat{\mu}$ are given by

\[
\hat{\Lambda} \approx \sum_{t=0}^{T-1} (x_t \otimes I) L(x_t \otimes I)^T,
\]

\[
\hat{\mu} \approx \text{vec}(A) + \hat{\Lambda}^{-1} \left( \sum_{t=0}^{T-1} (x_t \otimes I)Lw_t \right)
\]

where $x_{t+1} = Ax_t + w_t = (x_t \otimes I) \text{vec}(A) + w_t$. Hence

\[
E \left[ \|A - \hat{A}\|_F^2 \right] = E \left[ \| \text{vec}(A) - \hat{\mu} \|_2^2 \right]
\]

\[
= E \left[ \left\| \hat{\Lambda}^{-1} \left( \sum_{t=0}^{T-1} (x_t \otimes I)Lw_t \right) \right\|_2^2 \right],
\]

\[
= E \left[ \text{tr} \left( \hat{\Lambda}^{-1} \left( \sum_{t=0}^{T-1} (x_t \otimes I)Lw_t \right) w_t^\top L^\top (x_t \otimes I)^\top \right) \right],
\]

\[
= E \left[ \text{tr} \left( \hat{\Lambda}^{-1} \left( \sum_{t=0}^{T-1} (x_t \otimes I)L(x_t \otimes I)^\top \right) \right) \right],
\]

\[
= E \left[ \text{tr} \left( \hat{\Lambda}^{-1} \right) \right].
\]

This completes the proof.

E. Proof of Corollary 2

Proof: From the assumptions, $\text{tr}(L) = n \sigma^{-2}$ and

\[
\text{tr} \left( \sum_{i=0}^{t} A^i \Sigma(A^i)^\top \right) = \sigma^2 \text{tr} \left( \sum_{i=0}^{t} A^i (A^i)^\top \right).
\]

Thus

\[
\gamma(T, F) = n^2 \left\{ \frac{n \sigma^{-2} \sum_{i=0}^{t} A^i (A^i)^\top}{n \sigma^{-2} \sum_{i=0}^{t} A^i (A^i)^\top} \right\}^{-1},
\]

\[
= n \left\{ \frac{\sum_{i=0}^{t} \text{tr} \left( A^i (A^i)^\top \right)}{\sum_{i=0}^{t} \text{tr} \left( A^i (A^i)^\top \right)} \right\}^{-1}.
\]

This completes the proof.

F. Proof of Proposition 1

Proof: Let $(pk_t, sk_t) = ((p, q, g, h_t), s_t)$, $c_t = (c_{1,t}, c_{2,t})$, and $r_t$ be a random number used in the encryption algorithm at time $t$. From the proof of in [33, Th. 1], $\text{Dec}(sk_t, \text{Enc}(pk_t, m)) = m \mod p$ is satisfied. The remaining part $\text{Dec}(sk_t, c_t) = m \mod p$ is obtained by direct calculation as

\[
c_{1,t}^{-s_t} c_{2,t} = (g^{r_{t-1} + r'})^{-s_t} (g^{r_{t-1} + r'})^{s_t} m h_{t-1}^{-r_{t-1} - r_{t-1}'} h_{t-1}' = mg^{-r_{t-1} + r'}(s_{t-1} + s') g^{r_{t-1} + r'}(s_{t-1} + s'),
\]

\[
= m \mod p.
\]

Furthermore

\[
\text{Dec}(sk_t, c_t \ast \text{Enc}(pk_t, m')) \mod p = (c_{1,t} g^{r'})^{-s_t} c_{2,t} m' h_t^r, = c_{1,t}^{-s_t} c_{2,t} m' g^{-s_t r} g^{s_t r}, = m \mod p.
\]

This completes the proof.

G. Proof of Proposition 2

Proof: Let $(pk_t, sk_t) = ((p, q, g, h_t), s_t)$ and $c_t = (c_{1,t}, c_{2,t})$. The adversary cannot calculate $sk_{t+1} = sk_t + s_t'$ and $sk_{t-1} = sk_{t-2} + s_{t-2}'$ even though he/she knows $sk_t = sk_{t-1} + s_t'$, $pk_t = g^{s_{t-1} + s_t}$, $c_{1,t} = g^{c_{2,t} + s_t}$, $c_{2,t} = mg^{r_t + r_{t-1} + s_{t-1}}$, $m = c_{1,t}^{-s_t} c_{2,t}$, and $r_t + r_{t-1} = \log_q c_{1,t}$ as long as $s_t$, $s_{t-1}$, and $s_{t-2}$ are secret.

$s_t$ is randomly updated, i.e., $s_t \sim U(\mathbb{Z}_q)$ [33]. Additionally, $h_t = g^{s_t} \mod U(\mathbb{G})$ because $s_t \sim U(\mathbb{Z}_q)$ and $\mathbb{G}$ is isomorphic to $\mathbb{Z}_q$ [33]. Similarly, $c_{1,t} = c_{1,t-1} g^{r_{t-1}} \mod U(\mathbb{G})$ and $c_{2,t} = c_{1,t-1}^{-s_{t-1}} c_{2,t-1} (g^{s_{t-1} + s_{t-1}})^{r_{t-1} - r_{t}} \mod U(\mathbb{G})$ since $r_t \sim U(\mathbb{Z}_q)$, $g^{r_t} \mod U(\mathbb{G})$, $g^{s_t} \mod U(\mathbb{G})$, and $(g^{s_t} h_t)^{r_t} \mod U(\mathbb{G})$. These facts conclude samples $\{h_t\} \leq \mathbb{Z}_q$, $\{c_{1,t}\} \leq \mathbb{Z}_q$, and $\{c_{2,t}\} \leq \mathbb{Z}_q$ for any time span $T \in [0, \infty)$ are unbiased. Therefore, the best strategy for the adversary to estimate $sk_{t+1}$ and $sk_{t-1}$ is random sampling from $\mathbb{Z}_q$, that is, $\Pr(\text{sk}_{t+1} = \text{sk}_{t+1}) = \Pr(\text{sk}_{t-1} = \text{sk}_{t-1}) = q^{-1}$.

Let $\epsilon(k) = 2^{-(k-1)}$ with a key length $k > 1$. Then, for every positive integers $c > 0$, there exists $N \in \mathbb{Z}$ such that $\epsilon(k) < k^{-c}$ for all $k > N$ because $\epsilon(k)$ and $k^{-c}$ decrease monotonically for $k > 1$ and satisfy $\lim_{k \to \infty} \epsilon(k)/k^{-c} = \lim_{k \to \infty} 2^{k'/2^k} = 0$. Therefore, $\epsilon(k)$ is negligible and satisfies $\Pr(\text{sk}_{t+1} = \text{sk}_{t+1}) = \Pr(\text{sk}_{t-1} = \text{sk}_{t-1}) = q^{-1} < \epsilon(k)$ since $q \in (2^{k-1}, 2^k)$.

H. Proof of Proposition 3

The security of a cryptosystem is formally defined via a game between a challenger and an adversary [50]. The IND-CPA game is described as follows.

1) The challenger generates a key pair and gives the public key to the adversary.
2) The adversary chooses two plaintexts based on his/her knowledge that is only the public key in this case and sends the plaintexts to the challenger.
3) The challenger randomly selects a plaintext from the given plaintexts and returns it to the adversary.
4) The adversary guesses which plaintext was encrypted.

This process can be formulated by using probabilistic polynomial-time algorithms, $A_0$ and $A_1$, as follows.

IND-CPA
1) $(pk, sk) = \text{Gen}(k)$.
2) $(m_0, m_1, \sigma) = A_0(pk)$.
3) $c = \text{Enc}(pk, m_b), b \sim U(\{0, 1\})$.
4) $\tilde{b} = A_1(c, \sigma)$.

The cryptosystem satisfies IND-CPA if the challenger wins the game, that is, the adversary’s advantage $|\Pr(\tilde{b} = \tilde{b}) - 1/2|$ is negligible. We now show the proof of Proposition 3 by reducing
the IND-CPA game of the dynamic ElGamal encryption to IND-CPA of the normal ElGamal encryption.

Proof: Consider the IND-CPA game of the dynamic ElGamal encryption denoted by IND-CPA \(^0\) \(_{\text{dyn}}\).

IND-CPA \(^0\) \(_{\text{dyn}}\)

1. \((pk_0, sk_0) = \text{Gen}(k)\).
2. \((m_0, m_1, \sigma) = A_0(pk_0)\).
3. \(c_0 = \text{Enc}(pk_0, m_b) \sim U(\{0, 1\})\).
4. Set \(t \leftarrow 0\).
5. \((pk_{k+1}, sk_{k+1}) = T_k(pk_t, sk_t)\).
6. \(c_{t+1} = T_c(c_t)\).
7. Set \(t \leftarrow t + 1\), and repeat 5)–7) as needed.
8. \(\hat{b} = A_1(\{c_n\}_{n=0}^t, \{pk_n\}_{n=0}^{t-1}, \{sk_n\}_{n=1}^{t-1}, \sigma)\).

In the modified game IND-CPA \(^0\) \(_{\text{dyn}}\), fix the lines 5) and 6) of IND-CPA \(^0\) \(_{\text{dyn}}\) to \(\text{Enc}(pk_{k+1}, sk_{k+1}) = \text{Gen}(k)\) and \(c_{t+1} = \text{Enc}(pk_{k+1}, sk_{k+1})\), respectively.

IND-CPA \(^1\) \(_{\text{dyn}}\)

1. \((pk_0, sk_0) = \text{Gen}(k)\).
2. \((m_0, m_1, \sigma) = A_0(pk_0)\).
3. \(c_0 = \text{Enc}(pk_0, m_b) \sim U(\{0, 1\})\).
4. Set \(t \leftarrow 0\).
5. \((pk_{k+1}, sk_{k+1}) = \text{Gen}(k)\).
6. \(c_{t+1} = \text{Enc}(pk_{k+1}, sk_{k+1})\).
7. Set \(t \leftarrow t + 1\), and repeat 5)–7) as needed.
8. \(\hat{b} = A_1(\{c_n\}_{n=0}^t, \{pk_n\}_{n=0}^{t-1}, \{sk_n\}_{n=1}^{t-1}, \sigma)\).

From the proof of Proposition 2, this modification does not change any probability in IND-CPA \(^0\) \(_{\text{dyn}}\) since operations of \(T_k\) and \(T_c\) are completely random. Therefore, the difference between the adversary’s advantages in IND-CPA \(^0\) \(_{\text{dyn}}\) and IND-CPA \(^1\) \(_{\text{dyn}}\) is negligible. Furthermore, the modification concludes that \(\{c_n\}_{n=0}^{t-1}, \{pk_n\}_{n=0}^{t-1}, \{sk_n\}_{n=1}^{t-1}\) give no information about \(c_t\) and \(m_b\). Thus, we obtain the equivalent game of IND-CPA \(^1\) \(_{\text{dyn}}\), which is denoted by IND-CPA \(^2\) \(_{\text{dyn}}\).

IND-CPA \(^2\) \(_{\text{dyn}}\)

1. \((pk_0, sk_0) = \text{Gen}(k)\).
2. \((m_0, m_1, \sigma) = A_0(pk_0)\).
3. \(c_0 = \text{Enc}(pk_0, m_b) \sim U(\{0, 1\})\).
4. Set \(t \leftarrow 0\).
5. \((pk_{k+1}, sk_{k+1}) = \text{Gen}(k)\).
6. \(c_{t+1} = \text{Enc}(pk_{k+1}, sk_{k+1})\).
7. Set \(t \leftarrow t + 1\), and repeat 5)–7) as needed.
8. \(\hat{b} = A_1(\{c_n\}_{n=0}^t, \sigma)\).

IND-CPA \(^2\) \(_{\text{dyn}}\) is clearly the same as IND-CPA because the repetition of 5)–7) does not affect the adversary’s advantage. This fact concludes that the difference between adversary’s advantages in IND-CPA \(^0\) \(_{\text{dyn}}\) and IND-CPA \(^1\) \(_{\text{dyn}}\) is negligible. In addition, the advantage in IND-CPA of the ElGamal encryption is negligible under the DDH assumption. From the above discussions, the dynamic ElGamal encryption satisfies IND-CPA at time \(t\) under the DDH assumption.

I. Proof of Lemma 3

Proof: The problem that minimizes \(J_T\) in (18) is a form of the typical finite-horizon discrete-time s-LQR problem [51]. Hence, the optimal control sequence is given as \(u_t = -(B_p^T P_{t+1} B_p)^{-1} B_p^T P_{t+1} A_p x_t\) if \(B_p^T P_{t+1} B_p\) is invertible, where \(P_t = A_p^T P_{t+1} A_p - A_p^T P_{t+1} B_p (B_p^T P_{t+1} B_p)^{-1} B_p^T P_{t+1} A_p + I,\) and \(P_T = I\).

Proof: The cases of \(T = 1, 2\) can be easily confirmed. For \(T \geq 3\), it follows that

\[
E(T) = E(T - 1) + \sum_{i=0}^{T-2} \text{tr}(A^i(A^i)^T) + \text{tr}(A^{T-1}(A^{T-1})^T),
\]

\[
= E(T - 1) + (E(T - 1) - E(T - 2)) + \text{tr}(A^{T-1}(A^{T-1})^T),
\]

\[
= 2E(T - 1) - E(T - 2) + \text{tr}(A^{T-1}(A^{T-1})^T).
\]

This completes the proof.

K. Proof of Theorem 1

Proof: From (11), (17), and (21), we have the minimum time step \(T^*\) satisfying \(\gamma(T^*, F^*) < \gamma_c\). Then, from (15) and (22), the key length \(k^*\) fulfills \(\tau(K^*, k^*) > \tau_c\). Therefore, the encrypted control system is secure.

REFERENCES

[1] E. A. Lee, “Cyber physical systems: Design challenges,” in Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput., 2008, pp. 363–369.

[2] A. Hamayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security - A survey,” IEEE Internet Things J., vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[3] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, “A systems and control perspective of CPS security,” Ann. Rev. Control, vol. 47, pp. 394–411, 2019.

[4] Z. Wang et al., “Cyber-physical systems for water sustainability: Challenges and opportunities,” IEEE Commun. Mag., vol. 53, no. 5, pp. 216–222, May 2015.

[5] 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.

[6] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, “A tutorial introduction to security and privacy for cyber-physical systems,” in Proc. Eur. Ctrl. Conf., 2019, pp. 968–978.

[7] E. Nekouei, T. Tanaka, M. Skoglund, and K. H. Johansson, “Information-theoretic approaches to privacy in estimation and control,” Annu. Rev. Control, vol. 47, pp. 412–422, 2019.

[8] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in Proc. Theory Cryptogr., 2006, pp. 265–284.

[9] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, “Differential privacy in control and network systems,” in Proc. Conf. Decis. Control, 2016, pp. 4252–4272.
[10] M. U. Hassan, M. H. Rehmani, and J. Chen, “Differential privacy tech-
niques for cyber physical systems: A survey,” IEEE Commun. Surv. Tut.,
vol. 22, no. 1, pp. 746–789, Jan./Mar. 2020.
[11] C. Muruga, I. Shames, J. Ruths, and D. Nelić, “Security metrics and
synthesis of secure control systems,” Automatica, vol. 115, 2020,
Art. no. 108757.
[12] H. Sandberg, A. Teixeira, and K. H. Johansson, “On security indices for
state estimators in power networks,” in Proc. 1st Workshop Secure Control
Syst., 2010.
[13] J. Mišlović, A. Teixeira, K. H. Johansson, and H. Sandberg, “Actuator
security indices based on perfect undetectability: Computation, robustness,
and sensor placement,” IEEE Trans. Autom. Control, vol. 65, no. 9,
pp. 3816–3831, Sep. 2020.
[14] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. D. Persis, “Net-
worked control under DoS attacks: Tradeoffs between resilience and
data rate,” IEEE Trans. Autom. Control, vol. 66, no. 1, pp. 460–467,
Jan. 2021.
[15] A. Cetinkaya, P. Arcaini, H. Ishii, and T. Hayakawa, “A search-based
approach to identifying jamming attacks and defense policies in wireless
networked control,” in Proc. IEEE Conf. Decis. Control, 2020, pp. 5717–
5724.
[16] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, “Encrypted
control for networked systems - An illustrative introduction and current
challenges,” IEEE Control Syst. Mag., vol. 41, no. 3, pp. 58–78, 2021.
[17] K. Kogiso, “Upper-bound analysis of performance degradation in en-
crypted control system,” in Proc. Amer. Control Conf., 2018, pp. 1250–
1255.
[18] M. Kishida, “Encrypted control system with quantiser,” IET Control
Theory Appl., vol. 13, no. 1, pp. 146–151, 2019.
[19] K. Teranishi, N. Shimada, and K. Kogiso, “Stability analysis and dynamic
quantizer for controller encryption,” in Proc. IEEE Conf. Decis. Control,
2019, pp. 7184–7189.
[20] K. Kogiso, and T. Fujita, “Cyber-security enhancement of networked
control systems using homomorphic encryption,” in Proc. IEEE Conf.
Decis. Control, 2015, pp. 6836–6843.
[21] F. Farokhi, I. Shames, and N. Batterham, “Secure and private control using
semi-homomorphic encryption,” Control Eng. Prac., vol. 67, pp. 13–20,
2017.
[22] J. Kim et al., “Encrypting controller using fully homomorphic encryption
for security of cyber-physical systems,” IFAC-PapersOnLine, vol. 49,
no. 22, pp. 175–180, 2016.
[23] M. S. Darup, A. Redder, I. Shames, F. Farokhi, and D. E. Quevedo,
“Towards encrypted MPC for linear constrained systems,” IEEE Control
Syst. Lett., vol. 2, no. 2, pp. 195–200, Apr. 2018.
[24] M. S. Darup, A. Redder, and D. E. Quevedo, “Encrypted cooperative
control based on structured feedback,” IEEE Control Syst. Lett., vol. 3,
no. 1, pp. 37–42, Jan. 2019.
[25] M. B. Alexandru, K. Gatis, Y. Shoukry, S. A. Seshia, P. Tabuada, and G. J.
Pappas, “Cloud-based quadratic optimization with partially homomorphic
encryption,” IEEE Trans. Autom. Control, vol. 66, no. 5, pp. 2357–2364,
May 2021.
[26] A. B. Alexandru, A. Tsiampis, and G. J. Pappas, “Towards private data-
driven control,” in Proc. IEEE Conf. Decis. Control, 2020, pp. 5449–5456.
[27] R. Fritz, M. Fauser, and P. Zhang, “Controller encryption for discrete event
systems,” in Proc. Amer. Control Conf., 2019, pp. 5633–5638.
[28] M. Ristic, B. Noack, and U. D. Hanebeck, “Secure fast covariance
intersection using partially homomorphic and order revealing encryption
schemes,” IEEE Control Syst. Lett., vol. 5, no. 1, pp. 217–222,
Jan. 2021.
[29] J. Stuh and T. Tanaka, “Encrypted value iteration and temporal difference
learning over leveled homomorphic encryption,” in Proc. Amer. Control
Conf., 2021, pp. 2555–2561.
[30] J. H. Cheon et al., “Toward a secure drone system: Flying with real-
time homomorphic authenticated encryption,” IEEE Access, vol. 6,
pp. 24325–24339, 2018.
[31] K. Teranishi, N. Shimada, and K. Kogiso, “Development and examination of
Fog computing-based encrypted control system,” IEEE Robot. Automat.
Lett., vol. 5, no. 3, pp. 4642–4648, Jul. 2020.
[32] J. Tran, F. Farokhi, M. Cantoni, and I. Shames, “Implementing homomor-
phic encryption based secure feedback control,” Control Eng. Prac.,
vol. 97, 2020, Art. no. 104350.
[33] K. Teranishi, N. Shimada, and K. Kogiso, “Stability-guaranteed dynamic
ElGamal cryptosystem for encrypted control systems,” IET Control Theory
Appl., vol. 14, no. 16, pp. 2242–2252, 2020.
Tomonori Sadamoto (Member, IEEE) received the Ph.D. degree in information engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 2015. From 2015 to 2016, he was a Visiting Researcher with the School of Electrical Engineering, Royal Institute of Technology, Stockholm, Sweden. From April 2016 to August 2016, he was a Researcher with the Department of Systems and Control Engineering, Graduate School of Engineering, Tokyo Institute of Technology, Tokyo, Japan. From 2016 to 2018, he was a specially appointed Assistant Professor with the same department. Since 2018, he has been an Assistant Professor with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan.

Dr. Sadamoto was named as a finalist of the European Control Conference Best Student-Paper Award in 2014. He was the recipient of the Research encouragement Award from The Funai Foundation for Information Technology in 2019 and the IEEE Control Systems Magazine Outstanding Paper Award in 2020.

Aranya Chakrabortty (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2008. From 2008 to 2009, he was a Postdoctoral Research Associate with the University of Washington, Seattle, WA, USA. From 2009 to 2010, he was an Assistant Professor with Texas Tech University, Lubbock, TX, USA. Since 2010, he has been with the Electrical and Computer Engineering Department, North Carolina State University, Raleigh, NC, USA, where he is currently a Professor. His research interests are in all branches of control theory with applications to electric power systems.

Dr. Chakrabortty was the recipient of the NSF CAREER Award in 2011. He was named as a University Faculty Scholar by the NC State Provost's office in 2019.

Kimino Kogiso (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in mechanical engineering from Osaka University, Suita, 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 with the Department of Information Systems, Nara Institute of Science and Technology, Nara, Japan, in 2005. Since 2014, he has been an Associate Professor with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan. From 2010 to 2011, he was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA. His research interests include constrained control, control of decision makers, cybersecurity of control systems, and their applications.