UNIVERSITY OF CALIFORNIA

Los Angeles

Encrypted Lyapunov-Based Model Predictive Control Design for Security to Cyber-Attacks

A thesis submitted in partial satisfaction of the
requirements for the degree Master of Science
in Chemical Engineering

by

Atharva Vijay Suryavanshi

2023

ABSTRACT OF THE THESIS

Encrypted Lyapunov-Based Model Predictive Control Design for Security to Cyber-Attacks

by

Atharva Vijay Suryavanshi
Master of Science in Chemical Engineering
University of California, Los Angeles, 2023
Professor Panagiotis D. Christofides, Chair

In recent years, cyber-security of networked control systems has become crucial, as these systems are vulnerable to targeted cyber-attacks that compromise the stability, integrity and safety of these systems. In this work, secure and private communication links are established between sensor-controller and controller-actuator elements using semi-homomorphic encryption to ensure cyber-security in model predictive control (MPC) of nonlinear systems. Specifically, Paillier cryptosystem is implemented for encryption-decryption operations in the communication links. Cryptosystems, in general, work on a subset of integers. As a direct consequence of this nature of encryption algorithms, quantization errors arise in the closed-loop MPC of non-linear systems. Thus, the closed-loop encrypted MPC is designed with a certain degree of robustness to the quantization errors. Furthermore, the trade-off between the accuracy of the encrypted MPC and the computational cost is discussed. Finally, a two-state multi-input multi-output continuous stirred tank reactor (CSTR) example is employed to demonstrate the implementation of the proposed encrypted MPC design.

The thesis of Atharva Vijay Suryavanshi is approved.

Samanvaya Srivastava

Carlos Gilber Morales-Guio

Panagiotis D. Christofides, Committee Chair

University of California, Los Angeles

2023

Contents

List of Figures

ACKNOWLEDGMENTS

I would like to thank my advisor Professor Panagiotis D. Christofides for his guidance and support during the course of my research.

I would like to thank Professor Samanvaya Srivastava and Professor Carlos Gilber Morales-Guio for reviewing my thesis and contributing to my Master's thesis committee.

I would like to thank the National Science Foundation and the Department of Energy for providing financial support for this research.

This work was submitted with the same title for publication in the AIChE Journal, and is co-authored by Aisha Alnajdi, Mohammed Alhajeri, Fahim Abdullah and Professor Panagiotis D. Christofides. I would like to acknowledge their contributions to my thesis and extend my profound gratitude for their support and help.

Chapter 1

Introduction

Integration of cyber-secure strategies in physical networked control systems, to ensure secure and safe operation, has become crucial due to increased threats of targeted cyber-attacks. In these control systems, cloud computing has been extensively used to manage large amounts of data and to satisfy high computational power requirements. However, these advantages do not come without threats. Communication via unsecure networks between different components of the networked control systems, as well as computations using sensitive data on outsourced platforms, can lead to the threats of data manipulation and data interception, which would ultimately lead to jeopardizing the stability, integrity and profitability of the physical process. The severity and the destructive capabilities of these cyber-attacks can be understood from the recent series of attacks on industrial plants, such as the 2015 BlackEnergy malware attack on the Ukrainian electric power grid [1] and the 2021 cyber-attack on the Colonial oil pipeline system that lead to its shutdown, which consequently lead to a tremendous increase in gasoline prices [2]. Another prominent example is that of the Stuxnet worm, which manipulated the data in the communication links connected to programmable logic controllers (PLC) [3, 4]. Clearly, cyber-attacks on physical control systems are extremely dangerous as they can jeopardize physical processes via digital manipulations [5] and, hence, it is important to develop cyber-secure architectures for control systems.

To combat cyber-security challenges in the context of information technology, i.e., the software component of the plant, chemical and manufacturing have implemented multi-factor authentication, firewall isolation, and elaborate cyber protection protocols over the last decade. However, in the field of operation technology, which ensures the uninterrupted operation of robots, industrial control systems, supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), etc., efforts to address cyber-security had started around 2010 but only gained momentum around 2017 due to the increase in intelligent, targeted cyber-attacks, attracting many industrial process operation and automation groups. With the increasing convergence of information technology and operation technology in the Industry 4.0 framework, cyber-security of the operation technology domain is considered a central component of the secure and safe operation of the chemical sector. As a result, standards developing organizations such as the National Institute of Standards and Technology (NIST) [6] have developed fundamental cybersecurity research road maps, which are frameworks aimed to detect and mitigate the impact of cyber-attacks, that have influenced the security protocols of several industries. Their road map designates five areas for cyber-security practitioners and researchers to focus on, including but not limited to security by design, such as multi-tier controllers, and advanced threat detection. While there has been a growing amount of research in some of the key areas such as the development of machine learning-based detectors for advanced threat detection [7, 8, 9, 10], recovery of the process states following a cyber-attack [11], design of two-tier controllers [12] and cyberattack-resilient controllers for nonlinear systems [13, 14], the establishment of secure remote access protocols in the chemical sector remains an important, fundamental research issue. While secure remote access can be ensured in a number of ways, an emerging example is the use of encrypted control systems, whose primary objective is to preserve privacy with respect to the confidential system states, control inputs, controller parameters and model data.

The earliest examples of encrypted control systems were proposed in 2015 and comprised of linear control laws that were mostly applied to discrete-time, linear systems. The crux of such encrypted control systems, where the data was encrypted from the sensor up to the actuator, was "homomorphism". Homomorphic encryption indicates a special class of cryptographic algorithms (cryptosystems) that allows mathematical operations to be carried out on the encrypted data or "ciphertext". This allows for the calculations of the control law to be carried out in the encrypted or ciphertext space, with only the encrypted control action being sent to the actuator, where it can be decrypted to yield the "plaintext" data, thereby minimizing exposure of the plaintext control action to any attackers. A cryptosystem can be additively homomorphic, which means that addition operations may be carried out in the ciphertext space, and/or multiplicatively homomorphic, which allows multiplications in the encrypted space. In addition, a cryptosystem that is both additively and multiplicatively homomorphic is known as a fully homomorphic encryption, although their applicability in control systems is limited by their high computational demands and the power and memory restraints in control system hardware. Hence, the earliest encrypted control systems used linear control laws and partially homomorphic cryptosystems, specifically the ElGamal cryptosystem [15] and Rivest-Shamir-Adleman (RSA) cryptosystem [16], to demonstrate a proof of concept for encrypted control. However, linear control laws, especially based in the cloud, are severely restricted in terms of industrial applications. Instead, it is far more relevant and motivated to use encryption and remote servers for computationally expensive optimization-based control systems such as model predictive control [17].

Since its conceptualization, model predictive control (MPC) has been widely used in chemical industries to ensure closed-loop stability, while optimizing yield and other performance metrics. The key advantages of MPC include its ability to handle multiple inputs, outputs, multi-variable interactions between them, and state and input constraints by solving an optimization problem that minimizes a desired objective function of the inputs and predicted outputs using a process model and accounting for real-time measurement feedback. The optimization problem is solved over a finite time horizon at every sampling period of the MPC to compute the optimal control action, which guarantees the stability and boundedness of the trajectories of the system at all times.

The development of an encrypted MPC framework is, therefore, highly desirable for the chemical sector, due to the ubiquitous nature of MPC in this field. In this vein, in [18], a cyber-secure architecture for a linear system was designed by implementing the RSA cryptosystem to encrypt the controller parameters and the signals, while encrypted control actions were calculated in the controller using the multiplicative homomorphism property of the RSA cryptosystem. In [19, 20, 21], encrypted MPC for linear systems were proposed such that the additive homomorphism property of Paillier cryptosystem allowed linear computations in the encrypted space that were required to calculate encrypted MPC control actions. The main limitation of the aforementioned advances is that the property of homomorphism only allows for additive or multiplicative operations, which implies we can not perform the nonlinear optimization calculations required for MPC in the encrypted space. However, in a chemical plant setting, the nonlinear MPC computations may be carried out in an edge computer in a secure control room, which can be remotely accessed by the sensors and actuators via the network. As such, the goal is to use encryption to establish secure links from the sensors and actuators to the physically secure control room. The importance of the sensor-controller and the controller-actuator links have been highlighted in several recent works. Ref [22] investigated the effect of the control system parameters on the closed-loop stability and detectability of a multiplicative sensor–controller communication link attack with respect to a type of residual-based detection schemes, finally proposing a mechanism of parameter switching of the control system to retain attack detectability without deteriorating closed-loop performance too aggressively. To balance the above trade-off, in [23], a framework for active attack detection using the controller parameter switching of [22] was developed, where one set of controller parameters corresponds to conventional controller design criteria, while the other set of controller parameters maximizes cyber-attack detectability. Due to the possibility of controller parameter switching leading to excitement of the process, leading to false alarms, [24] proposed a switching condition to reduce the triggering of false alarms. Based on our review of the literature on encrypted MPC, to the best of our knowledge, the use of encryption in nonlinear MPC has not been addressed in the systems engineering literature, which warrants the construction of such a framework.

In this work, we develop a Lyapunov-based encrypted MPC scheme for nonlinear systems in which secure communication channels are established between the sensor-controller and the controller-actuator links under the assumption that we have a secure controller. The rest of this manuscript is organized as follows: in Chapter 2, the class of nonlinear systems considered and details of the Paillier cryptosystem and the quantization process are provided. In Chapter 3, the proposed encrypted MPC scheme is described, and its closed-loop stability results are derived. In Chapters 4 to 6, the proposed encrypted MPC is applied to a reactor with recycle and a reactor operating at an unstable point, respectively, in order to investigate the effectiveness, closed-loop stability results, the robustness of the designed controller to quantization errors, and the computational cost associated with different quantization parameters. Finally, the conclusions are summarized in Chapter 7.

Chapter 2

Preliminaries

2.1 Notation

The notation $|\cdot|$ is used to denote the Euclidean norm of a vector. x^T denotes the transpose of x. The notation $L_fV(x)$ denotes the standard Lie derivative $L_fV(x) := \frac{\partial V(x)}{\partial x} f(x)$. Set subtraction is denoted by "\", i.e., $A \backslash B := \{x \in \mathbb{R}^n \mid x \in A, x \notin B\}$. $\mathbb{R}, \mathbb{N}$, and $\mathbb{Z}$ denote the set of real numbers, natural numbers, and integers, respectively. In addition, $\mathbb{Z}_M$ and $\mathbb{Z}_M^*$ denote the additive and multiplicative group of integers modulo M, respectively. The function $f(\cdot)$ is of class $\mathcal{C}^1$ if it is continuously differentiable in its domain. A continuous function $\alpha : [0, a) \rightarrow [0, \infty)$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and is zero only when evaluated at zero.

2.2 Class of Systems

In this work, we focus on continuous-time nonlinear systems of nonlinear first-order ordinary differential equations (ODEs) with inputs, which is of the form,

$$\dot{x} = F(x, u) = f(x) + g(x)u \tag{2.1}$$

where $x = [x_1, x_2, \ldots, x_n] \in \mathbb{R}^n$ is the state vector and $u \in \mathbb{R}^m$ is the manipulated input vector. The inputs to the process are bounded, that is, $u \in U$ where the set $U \subset \mathbb{R}^m$ is defined as $U := \{u \in U | u_{\min,i} \leq u_i \leq u_{\max,i}, \quad \forall\ i = 1, 2, \cdots, m\}$. $u_{\min,i}$ and $u_{\max,i}$ are physical bounds and define the minimum and maximum value that each manipulated input can attain. $f(\cdot)$ is a sufficiently smooth vector function and $g(\cdot)$ is a sufficiently smooth matrix function. Without loss of generality, it is assumed $f(0) = 0$ and, hence, the origin is a steady state of the nonlinear system of eq. (2.1). Throughout this paper, the initial time is assumed to be zero (i.e., $t_0 = 0$). Furthermore, we will use the following notation: the space of continuous functions mapping the interval $[a, b]$ to the space $\mathbb{R}^n$ is given by $C([a, b], \mathbb{R}^n)$. The norm of a continuous function $\phi \in C([a, b], \mathbb{R}^n)$ is given by $\| \cdot \|$ which is defined as $\|\phi\| = \max\limits_{a \leq s \leq b} |\phi(s)|$. Set subtraction is denoted as: $A \setminus B := \{x \in \mathbb{R}^n | x \in A, x \notin B\}$. $\mathcal{C}^1$ denotes the class of continuously differentiable functions. The set of piecewise constant functions with a period Δ is denoted by $S(\Delta)$.

2.3 Stabilization via Lyapunov-based Feedback Control

We assume that there exists a feedback controller $u = \Phi(x) \in U$ which can render the origin of the system of eq. (2.1) exponentially stable in the sense that there exists a continuously differentiable control Lyapunov function $V(x)$ such that the following inequalities hold for all $x \in D$, where D is an open neighborhood around the origin [25, 26]:

$$c_1|x|^2 \leq V(x) \leq c_2|x|^2, \tag{2.2a}$$

$$\frac{\partial V(x)}{\partial x} F(x, \Phi(x)) \leq -c_3|x|^2, \tag{2.2b}$$

$$\left| \frac{\partial V(x)}{\partial x} \right| \leq c_4|x| \tag{2.2c}$$

where c_1, c_2, c_3 and c_4 are positive constants. The approach in Ref. [27] can be used to construct one such stabilizing controller. Additionally, on the basis of the Lipschitz property of $F(x, u)$ and the bounded nature of u, there exist positive constants M_F, L_x, and $L_x^{'}$ such that the following inequalities hold for all $x, x' \in D$ and $u \in U$:

$$|F(x,u)| \leq M_F \tag{2.3a}$$

$$|F(x,u) - F(x',u)| \leq L_x|x - x'| \tag{2.3b}$$

$$\left|\frac{\partial V(x)}{\partial x}F(x,u) - \frac{\partial V(x')}{\partial x}F(x',u)\right| \leq L_x^{'}|x - x'| \tag{2.3c}$$

For the nonlinear system of eq. (2.1), the closed loop stability region is characterized as a level set of the Lyapunov function V. This stability region Ω_ρ is defined as $\Omega_\rho := \{x \in D|V(x) \leq \rho\}$, where $\rho > 0$.

2.4 Paillier cryptosystem

In this paper, we use the Paillier cryptosystem [28] for encryption and decryption of both process measurements, x, that are sent to the control system and of the control actions, u, that are calculated by the control system and sent to the control actuators. Paillier cryptosystem is a partially homomorphic encryption scheme that allows addition operations in the encrypted message space. The security guarantees of Paillier encryption rely on a standard cryptographic assumption called Decisional Composity Residuocity (DCR) [28, 18, 19, 29]. Paillier encryption has been widely used, especially in the context of linear MPC, due to its additive homomorphism property greatly reducing the communication load and number of decryptions required in linear MPC, as compared to, for example, a multiplicative homomorphic algorithm such as the ElGamal cryptosystem [29]. Paillier cryptosystem encrypts plaintext messages from a subset of $\mathbb{N}$, and the public key of encryption decides the cardinality of such a subset. The first step in the encryption process is the generation of public and private keys. A public key is used to encrypt integer messages into ciphertexts. A private key is used to decrypt ciphertexts and obtain the original integer message. The public and private keys of the Paillier cryptosystem are generated as follows:

1. Randomly choose two large random prime integers p and q such that $\gcd(pq, (p-1)(q-1)) = 1$ where $\gcd(i, j)$ is a function that returns the greatest common divisor of $i, j \in \mathbb{N}$.

2. Compute $M = pq$ and $\lambda = \operatorname{lcm}(q-1, p-1)$, where $\operatorname{lcm}(i, j)$ refers to the least common multiple of the integers i, j.

3. Choose a random integer g such that, $g \in \mathbb{Z}^*_{M^2}$ where $\mathbb{Z}^*_{M^2}$ is the multiplicative group of integers modulo M^2.

4. Define $L(x) = (x-1)/M$.

5. Check the existence of the following modular multiplicative inverse: $u = (L(g^\lambda \text{mod} M^2))^{-1} \text{mod } M$.

6. If the inverse does not exist, go back to step 4 and choose a different value of g.

7. If the inverse exists, we have the public key (M, g) and the private key (λ, u).

Once the keys are obtained, the data $m \in \mathbb{Z}_M$, which can either be quantized states or quantized inputs, is encrypted as follows:

$$E_M(m, r) = c = g^m r^M \bmod M^2 \tag{2.4}$$

where $r \in \mathbb{Z}_M$ is a random integer and c is the ciphertext obtained after encryption of m. To decrypt a ciphertext $c \in \mathbb{Z}_{M^2}$, it is required to calculate:

$$D_M(c) = m = L(c^\lambda \bmod M^2) u \bmod M \tag{2.5}$$

Remark 1. In this study, as the data is decrypted before being used in the MPC calculation, the advantage of the homomorphic property of Paillier cryptosystem is not retained. However, we use Paillier cryptosystem not due to its homomorphism but rather to avoid the computational burden of more advanced encryption algorithms such as AES, whose applicabililty is limited by power and memory constraints on process control hardware.

2.5 Quantization

Paillier cryptosystem encrypts numbers from a subset of $\mathbb{N}$. This subset is given by the set $\mathbb{Z}_M$. Hence, it is important to map real number data (state measurements from the process, and inputs calculated by the controller), which are in the form of floating point numbers, to the set $\mathbb{Z}_M$ in order to encrypt and decrypt signals in the sensor-controller and controller-actuator links. Quantization functions are used to map this real number data to the set $\mathbb{Z}_M$ [19]. For this purpose, we consider signed fixed-point numbers in the base 2. The quantization parameter l_1 denotes the number of total bits and d denotes the number of fractional bits. Based on these quantization parameters, a set $\mathbb{Q}_{l_1,d}$ is constructed which contains rational numbers from -2^{l_1-d-1} to $2^{l_1-d-1} - 2^{-d}$ with the rational numbers separated from each other by a resolution of 2^{-d}. A rational number q in the set $\mathbb{Q}_{l_1,d}$ can be represented as: $q \in \mathbb{Q}_{l_1,d}$ such that, $\exists \beta \in \{0,1\}^{l_1}$ and $q = -2^{l_1-d-1}\beta_l + \sum_{j=1}^{l_1-1} 2^{j-d-1}\beta_i$. Given a real number data point a, the function $g_{l_1,d}$ that maps a to the set $\mathbb{Q}_{l_1,d}$ is given by the equation,

$$\begin{aligned} g_{l_1,d} &: \mathbb{R} \rightarrow \mathbb{Q}_{l_1,d} \\ g_{l_1,d}(a) &:= \arg \min_{q \in \mathbb{Q}_{l_1,d}} |a - q| \end{aligned} \tag{2.6}$$

which finds the quantized rational number closest to the real number data point. Subsequently, using a bijective mapping $f_{l_2,d}$ [19], we map the quantized data to a set of integers that is a subset of the message space $\mathbb{Z}_M$. The bijective mapping is defined as:

$$\begin{aligned} f_{l_2,d} &: \mathbb{Q}_{l_1,d} \rightarrow \mathbb{Z}_{2^{l_2}} \\ f_{l_2,d}(q) &:= 2^d q \bmod 2^{l_2} \end{aligned} \tag{2.7}$$

Encryption of integer plaintext messages is carried over the set $Z_{2^{l_2}}$ and the ciphertexts are decrypted into the same set $Z_{2^{l_2}}$. The ciphertexts are decrypted at the controller and at the actuator to obtain the integer plaintext messages corresponding to the quantized states and quantized inputs, respectively. Hence, it is important to map the decrypted plaintext messages to the set $\mathbb{Q}_{l_1,d}$. The inverse mapping $f^{-1}_{l_2,d}$ is defined as:

$$f^{-1}_{l_2,d} : \mathbb{Z}_{2^{l_2}} \rightarrow \mathbb{Q}_{l_1,d} \tag{2.8}$$

$$f^{-1}_{l_2,d}(m) := \frac{1}{2^d} \begin{cases} m - 2^{l_2} & \text{if } m \geq 2^{l_2-1} \\ m & \text{otherwise} \end{cases} \tag{2.9}$$

Chapter 3

Encrypted MPC Design

In the proposed closed-loop design of fig. 3.1, signals $x(t)$ from the sensor are encrypted and sent to the model predictive controller (MPC). Before nonlinear computations are performed, the encrypted data is decrypted to obtain quantized states $\hat{x}(t)$. At time t, the plant model in the MPC is initialized using the quantized states $\hat{x}(t)$. The MPC calculates the optimized inputs $u(t)$, and these inputs are encrypted before being sent to the actuator. These encrypted inputs are further decrypted and the quantized inputs $\hat{u}(t)$ are applied to the process.

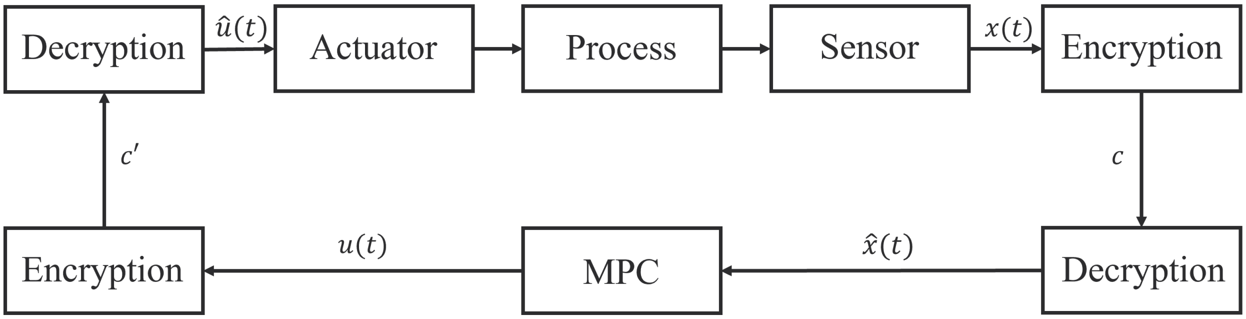

Figure 3.1: Schematic of closed-loop system under encrypted MPC.

Two sources of errors are identified in the above closed loop design. There is a state quantization error in the sensor-controller communication link, and there is also an input quantization error in the controller-actuator communication link. These quantization errors arise as a direct consequence of mapping the state and input data from $\mathbb{R}$ to $\mathbb{Q}_{l_1,d}$. Based on the mapping of eq. (2.6), these quantization errors are bounded such that:

$$|x(t) - \hat{x}(t)| \leq \eta_1 \, 2^{-d} \tag{3.1a}$$

$$|u(t) - \hat{u}(t)| \leq \eta_2 \, 2^{-d} \tag{3.1b}$$

where $\eta_1, \eta_2 > 0$, and d is the quantization parameter of the mapping of eq. (2.6). Given the quantization error in the input applied to the process, the nonlinear system of eq. (2.1) in the closed-loop design of fig. 3.1 takes the form,

$$\begin{aligned} \dot{x} = F(x, \hat{u}) &= f(x) + g(x)\hat{u} \\ &= f(x) + g(x)(u + e_2) \end{aligned} \tag{3.2}$$

where $e_2 = \hat{u}(t) - u(t)$ and

$$|e_2| \leq \eta_2 \, 2^{-d} \tag{3.3}$$

Secondly, there is an error in the computed control action, as the controller receives the quantized state $\hat{x}$ instead of the actual state x. For the stabilizing control law $u = \Phi(x) \in U$, this error in the control action is bounded as:

$$|\Phi(\hat{x}) - \Phi(x)| \leq L_1 |\hat{x} - x| \leq L_1^{'} 2^{-d} \tag{3.4}$$

Taking into account the above errors, we perform a closed-loop stability analysis for the proposed encrypted control system using first the Lyapunov-based controller and then the MPC.

3.1 Closed-loop stability of encrypted control

The presence of quantization errors in the sensor-controller and controller-actuator communication links requires us to characterize a new closed-loop stability region $\Omega_{\hat{\rho}}$ embedded in Ω_ρ (i.e., $\hat{\rho} < \rho$). The following result establishes that the controller $\Phi(x) \in U$ can stabilize, in a sense to be made precise below, the origin of the nonlinear system of eq. (3.2) under an encrypted controller.

Theorem 1. *Consider the nonlinear system of eq.* (3.2) *under encrypted control, with the initial state $x_0 \in \Omega_{\hat{\rho}}$ and with the stabilizing control law $u = \Phi(x) \in U$. Then, the origin of the closed-loop system of eq.* (3.2) *under encrypted control is rendered practically stable for all $x_0 \in \Omega_{\hat{\rho}}$ in the sense that the closed-loop state $x(t)$ remains in Ω_ρ for all times and that the following inequalities hold:*

$$\dot{V} \leq -c_5|x|^2 \quad \forall |x| \geq \frac{c_4 2^{-d}(\gamma_1 + \gamma_2)}{c_3\theta} = \mu \tag{3.5a}$$

$$\limsup_{t\to\infty} |x| \leq b \tag{3.5b}$$

where d is the quantization parameter, $c_3, c_4, \gamma_1, \gamma_2, b > 0$, $0 < \theta < 1$ and $c_5 = (1-\theta)c_3$.

Proof. Based on the nonlinear system of eq. (3.2), the time derivative of V can be written as:

$$\begin{aligned}
\dot{V} &= \frac{\partial V}{\partial x} F(x, \hat{u}) \\
&= \frac{\partial V}{\partial x} F(x, u + e_2) \\
&= \frac{\partial V}{\partial x} F(x, \Phi(\hat{x}) + e_2) \\
&= \frac{\partial V}{\partial x} \left[f(x) + g(x)\big(\Phi(\hat{x}) + e_2\big)\right] \\
&= \frac{\partial V}{\partial x} \left[f(x) + g(x)\big(\Phi(\hat{x}) - \Phi(x) + \Phi(x) + e_2\big)\right] \\
&= \frac{\partial V}{\partial x} \left[f(x) + g(x)\Phi(x) + g(x)\big(\Phi(\hat{x}) - \Phi(x)\big) + g(x)e_2\right] \\
&= \frac{\partial V}{\partial x}\big(f(x) + g(x)\Phi(x)\big) + \frac{\partial V}{\partial x} g(x)\big(\Phi(\hat{x}) - \Phi(x)\big) + \frac{\partial V}{\partial x} g(x) e_2
\end{aligned} \tag{3.6}$$

Based on eq. (2.2b), it follows that

$$\dot{V} \leq -c_3|x|^2 + \frac{\partial V}{\partial x}g(x)\big(\Phi(\hat{x}) - \Phi(x)\big) + \frac{\partial V}{\partial x}g(x)e_2 \tag{3.7}$$

Applying the inequalities of eq. (2.2c), eq. (3.3) and eq. (3.4), it follows that

$$\begin{aligned}\dot{V} &\leq -c_3|x|^2 + c_4\gamma_1|x|2^{-d} + c_4\gamma_2|x|2^{-d} \\ &\leq -c_3|x|^2 + c_4|x|2^{-d}(\gamma_1 + \gamma_2) \\ &\leq -(1-\theta)c_3|x|^2 - \theta c_3|x|^2 + c_4 2^{-d}(\gamma_1 + \gamma_2)|x|\end{aligned} \tag{3.8}$$

Therefore, if the condition of eq. (3.5a) on $|x|$ is satisfied i.e., $|x| \geq \frac{c_4 2^{-d}(\gamma_1+\gamma_2)}{c_3\theta} = \mu$, it follows that

$$\begin{aligned}\dot{V} &\leq -(1-\theta)c_3|x|^2 \\ &\leq -c_5|x|^2\end{aligned} \tag{3.9}$$

where $c_5 = (1-\theta)c_3$. Thus, based on eq. (3.9), we have that $\dot{V}$ is negative for all $x \in \Omega_{\hat{\rho}}$ that satisfy the condition of eq. (3.5a).

Based on the fact that $\Omega_{\hat{\rho}}$ is a level set of V and that $\dot{V}$ is negative for all $x \in \Omega_{\hat{\rho}}$, we have that the state of the closed-loop system $x(t)$ stays in $\Omega_{\hat{\rho}}$ for all times. Furthermore, using Theorem 4.18 in Ref. [30], it follows that

$$\limsup_{t\to\infty} |x(t)| \leq b \tag{3.10}$$

where b is a positive constant (which can be expressed as a class $\mathcal{K}$ function of μ). Hence, as the quantization parameter $d \to \infty$, following the definition of μ from eq. (3.5a), $\mu \to 0$ and, therefore, the ultimate bound approaches zero, proving that larger values of the quantization parameter d results in a smaller error between the state and input trajectories of the encrypted control system and the non-encrypted control system. This proves that the closed-loop states of the nonlinear system of eq. (3.2) are uniformly ultimately bounded under the stabilizing controller $u = \Phi(x) \in U$ for sufficiently large d. □

3.2 Encrypted Lyapunov-based MPC

In this section, a feedback MPC is formulated for the closed-loop design of the nonlinear system of eq. (2.1) with secure sensor-controller and controller-actuator communication links. Control actions will be implemented on the nonlinear system in a sample-and-hold fashion with a sampling period of Δ [31, 32]. The proposed MPC formulation is as follows:

$$\mathcal{J} = \min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u(t))dt \tag{3.11a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u(t)) = f(\tilde{x}) + g(\tilde{x})u \tag{3.11b}$$

$$u(t) \in U, \; \forall \, t \in [t_k, t_{k+N}) \tag{3.11c}$$

$$\tilde{x}(t_k) = \hat{x}(t_k) \tag{3.11d}$$

$$\dot{V}(\hat{x}(t_k), u) \leq \dot{V}(\hat{x}(t_k), \Phi(\hat{x}(t_k))), \text{ if } \hat{x}(t_k) \in \Omega_{\hat{\rho}} \backslash \Omega_{\rho_{\min}} \tag{3.11e}$$

$$V(\tilde{x}(t)) \leq \rho_{\min}, \; \forall \, t \in [t_k, t_{k+N}), \text{ if } \hat{x}(t_k) \in \Omega_{\rho_{\min}} \tag{3.11f}$$

where the predicted state trajectory is denoted by $\tilde{x}$, the set of piecewise constant functions with period Δ is denoted by $S(\Delta)$ and the number of sampling periods in the prediction horizon is denoted by N. The Lyapunov-based MPC calculates the optimal input sequence $u^*(t|t_k)$ over the entire prediction horizon $t \in [t_k, t_{k+N})$, and the first input of this sequence is sent to the actuator to be applied to the system for all $t \in [t_k, t_{k+1})$. Note that, in the MPC optimization problem of eq. (3.11), the first-principles process model implemented in the MPC uses the quantized states $\hat{x}$ to predict the state trajectory.

In the encrypted Lyapunov-based MPC (LMPC) formulation, eq. (3.11a) integrates the cost function over the entire prediction horizon, and eq. (3.11b) describes the plant-model being used in LMPC. The constraint of eq. (3.11c) denotes the constraints on the control inputs. The constraint of eq. (3.11d) initializes the plant model of eq. (3.11b) with quantized states. If $x(t_k) \in \Omega_{\hat{\rho}} \setminus \Omega_{\min}$, then the Lyapunov constraint of eq. (3.11e) drives the closed-loop state, $x(t_k)$, of the nonlinear system of eq. (3.2) towards the origin. If the closed-loop state $x(t_k)$ gets in the region $\Omega_{\rho_{\min}}$, then the constraint of eq. (3.11f) ensures that this state remains in $\Omega_{\rho_{\min}}$ over the entire prediction horizon.

The following theorem addresses the closed-loop stability of the nonlinear system of eq. (3.2) under the encrypted LMPC.

Theorem 2. *Consider the system of eq.* (3.2)*, under the closed-loop encrypted LMPC design of eq.* (3.11) *based on the stabilizing controller,* $u = \Phi(x) \in U$*, satisfying the inequalities in eq.* (2.2) *and assume that the initial state* $x_0 \in \Omega_{\hat{\rho}}$*. Let* $\Delta > 0, \epsilon_w > 0 \text{ and } \hat{\rho} > \rho_{\min} > \rho_s$ *satisfy,*

$$\begin{aligned} &-\frac{c_3}{c_2}\rho_s + L_x^{'} M_F \Delta + L_w^{'} \delta \leq -\epsilon_w \\ &\rho_{\min} = \max\{V(x(t+\Delta)) | V(x(t)) \leq \rho_s\} \end{aligned} \tag{3.12}$$

Then, the state of the closed-loop system $x(t)$ *is always bounded in* $\Omega_{\hat{\rho}}$ *and is ultimately bounded in* $\Omega_{\rho_{\min}}$.

Proof. Consider the state $x(t_k) \in \Omega_{\hat{\rho}} \setminus \Omega_{\rho_s}$. The time-derivative of V under the control inputs calculated by the LMPC of eq. (3.11) for the nonlinear system of eq. (3.2) at t_k can be written as:

$$\begin{aligned} \dot{V} &= \frac{\partial V(x(t))}{\partial x} F\big(x(t), u(t_k), e_2\big) \\ \dot{V} &= \frac{\partial V(x(t_k))}{\partial x} F\big(x(t_k), u(t_k)\big) \\ &\quad + \frac{\partial V(x(t))}{\partial x} F(x(t), u(t_k), e_2) \\ &\quad - \frac{\partial V(x(t_k))}{\partial x} F(x(t_k), u(t_k)) \end{aligned} \tag{3.13}$$

for all $t \in [t_k, t_{k+1}]$.

In the encrypted LMPC, the constraint of eq. (3.11e) ensures that, if $x(t_k) \in \Omega_{\hat{\rho}} \setminus \Omega_{\rho_{\min}}$, then the closed-loop state is driven towards the origin at t_{k+1} (to a lower level set of V). Based on the inequality of eq. (2.2b), it follows from eq. (3.13) that:

$$\begin{aligned} \dot{V} \leq -c_3|x(t_k)|^2 + \frac{\partial V(x(t))}{\partial x} F(x(t), u(t_k), e_2) \\ - \frac{\partial V(x(t_k))}{\partial x} F(x(t_k), u(t_k)) \end{aligned} \tag{3.14}$$

Based on the fact that the error, $|e_2| \leq \eta_2 \, 2^{-d} = \delta$ is bounded, the Lipschitz conditions of eq. (2.3), and the inequality of eq. (2.2a), it follows from eq. (3.14) that:

$$\dot{V} \leq -\frac{c_3}{c_2}\rho_s + L_x^{'}|x(t) - x(t_k)| + L_w^{'}\delta \tag{3.15}$$

where $L_w^{'} > 0$. Due to the continuity of $x(t) \; \forall \, t \in [t_k, t_{k+1})$, we can write that $|x(t) - x(t_k)| \leq M_F \Delta \; \forall \, t \in [t_k, t_{k+1})$. Using this bound, it follows from eq. (3.15) that:

$$\dot{V} \leq -\frac{c_3}{c_2}\rho_s + L_x^{'} M_F \Delta + L_w^{'}\delta \tag{3.16}$$

Thus, if $-\frac{c_3}{c_2}\rho_s + L_x^{'} M_F \Delta + L_w^{'}\delta \leq -\epsilon_w$, then $\dot{V} \leq -\epsilon_w$ for any $x(t_k) \in \Omega_{\hat{\rho}} \setminus \Omega_{\rho_s}$. This establishes that the state of the closed-loop system is always bounded in $\Omega_{\hat{\rho}}$, and it ultimately converges to $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$ and then remains there. □

Remark 2. It is important to note that the focus of this work is on the cyber-security of the sensor-controller and controller-actuator communication links in a nonlinear MPC scheme. Other studies such as Ref. [29] use semi-homomorphic encryption schemes to avoid decrypting/encrypting the process states and inputs before and after the MPC block in fig. 3.1, i.e., the data is encrypted from the sensor block to the actuator block, which provides protection against eavesdropping by a cloud provider or neighboring agents. However, such results are restricted to linear controllers with a feedback gain since the complex, numerous computations required in MPC, particularly nonlinear MPC, are not possible to carry out in the encrypted space where only either addition or multiplication may be performed. The proposed encrypted MPC architecture is most valuable in a chemical plant setting, where encryption is required to have secure links from the sensors and actuators to the control room, where the nonlinear MPC calculations are carried out, since the control room itself is physically secure and only communicates with the sensors and actuators via the network.

Chapter 4

Application to a chemical reactor with recycle

4.1 Process description

In this section, we apply the above methodology to a chemical reactor example, specifically the system from Ref. [33] without input or state delays in the process. We demonstrate the encrypted MPC approach on a well-mixed non-isothermal continuous stirred tank reactor (CSTR) with a recycle stream and analyze the effects of encryption on the trajectories and closed loop stability. In the CSTR, an irreversible, second-order, elementary, exothermic reaction occurs, which is given as $A \to B$. The CSTR is equipped with a jacket to remove/supply thermal energy at a rate of Q. A first-principles model can be constructed based on the material and energy balances across the CSTR. Using these balances, we can write the differential equations describing the nonlinear dynamics of the process as:

$$\frac{\mathrm{d}C_A}{\mathrm{d}t} = \frac{(1-\lambda)F}{V}C_A + \frac{\lambda F}{V}C_{A0} - \frac{F}{V}C_A - k_0 \mathrm{e}^{\frac{-E}{RT}} C_A^2 \tag{4.1a}$$

$$\frac{\mathrm{d}T}{\mathrm{d}t} = \frac{(1-\lambda)F}{V}T + \frac{\lambda F}{V}T_0 - \frac{\Delta H}{\rho_L C_p} k_0 \mathrm{e}^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{4.1b}$$

where C_A is the concentration of reactant A, and T is the temperature in the reactor. The inlet feed has a volumetric flow rate of λF, where λ is the fraction with which the outlet stream is split—the fraction λ of the outlet stream being the product stream, whereas the fraction $(1-\lambda)$ of the outlet stream is recycled back to the reactor (recycle stream). The feed temperature is T_0, and the inlet feed containing only A has a concentration of C_{A0}. V is the volume of the reactor, and Q is the rate of heat removal from the reactor. The values and definitions of all the other parameters are reported in Ref. [33]. For the above process, the reactant concentration C_A and the temperature of the reactor T, in deviation terms, are the state variables ($x^T = [C_A - C_{As} \quad T - T_s]$). The inlet feed concentration C_{A0} and the rate of heat removal Q are the manipulated inputs to our process, which are bounded to be in the closed sets: $Q \in [-80.0, 80.0]\ MJ/h$ and $C_{A0} \in [0.5, 7.5]\ kmol/m^3$. We investigate the stable steady state of the CSTR system of eq. (4.1), which is achieved at the point $[C_{As} \quad T_s] = [2.96\ kmol/m^3 \quad 320\ K]$ under manipulated input values of $Q_s = 12.2 MJ/h$ and $C_{A0s} = 4\ kmol/m^3$.

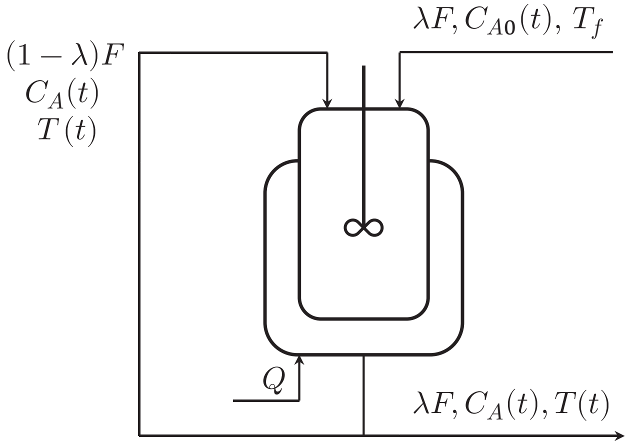

Figure 4.1: Process flow diagram of the CSTR with recycle.

In the encrypted network, secure communications are established between the sensor-controller and controller-actuator links. Before we encrypt the states and inputs, it is important to quantize the data. Using the first quantization function, $g_{l_1,d}(a)$, we map state and input data in real numbers to the set $\mathbb{Q}_{l_1,d}$. The largest value in the set $\mathbb{Q}_{l_1,d}$ is given as $2^{l_1-d-1} - 2^{-d}$, which should always be greater than or equal to the maximum value of permissible inputs and the maximum possible values of the states in the operating region. Similarly, the lowest value in the set $\mathbb{Q}_{l_1,d}$ is given as -2^{l_1-d-1} and, hence, this value should be smaller than the minimum value of permissible inputs and minimum possible values of the states in the operating region. Based on this, we get the minimum value of $l_1 - d$ as 18, and we have to choose the value of l_1 and d accordingly. The rational numbers in the set $\mathbb{Q}_{l_1,d}$ are separated by a resolution of 2^{-d}, which means that the higher the value of d, the lesser is the quantization error and the higher is the computational cost. This relation between the error and the value of d is demonstrated in fig. 4.2, where the function $\sin x$, for $x \in [0, \pi]$ is quantized with $d = 2$ and $d = 4$, resulting in resolutions of 0.25 and 0.0625, respectively. For the purpose of simulations, we vary the values of d from 1 to 8 in increments of 1 and thus, the value of l_1 varies from 19 to 26 in increments of 1. For the second quantization, it is required to have $l_2 > l_1$. Hence, we select the value $l_2 = 29$. Once we have identified values of all the quantization parameters, we quantize the states and inputs, and encrypt them according to the Paillier Encryption algorithm. For the implementation of Paillier Encryption, the "phe" module in Python is used [34]. The first-principles model of eq. (4.1) is used as the process model in the MPC, and the optimization problem is solved using the Python module of the IPOPT software [35]. The dynamic model of eq. (4.1) is simulated numerically using the explicit Euler method with an integration time step of $h_c = 10^{-4}$ hr. The sampling period is $\Delta = 10^{-2}$ hr. The control Lyapunov function $V = x^T P x$ is constructed using the positive definite matrix,

$$P = \begin{bmatrix} 500 & 20 \\ 20 & 1 \end{bmatrix}$$

obtained from extensive simulations. A stabilizing proportional controller is designed to be the lower bound for the LMPC, and the prediction horizon for the LMPC is chosen as $N = 2$. Through extensive simulations, we determine $\rho_{\min} = 0.1$. The LMPC cost function of eq. (3.11a) is chosen to be $L(x,u) = x^T Q_1 x + u^T Q_2 u$, which achieves its minimum value at the origin. Q_1 and Q_2 are the MPC weight matrices that, after carefully tuning, are taken as $Q_1 = \begin{bmatrix} 10 & 0 \\ 0 & 1 \end{bmatrix}$ and $Q_2 = \begin{bmatrix} 0.03 & 0 \\ 0 & 8 \times 10^{-7} \end{bmatrix}$, respectively.

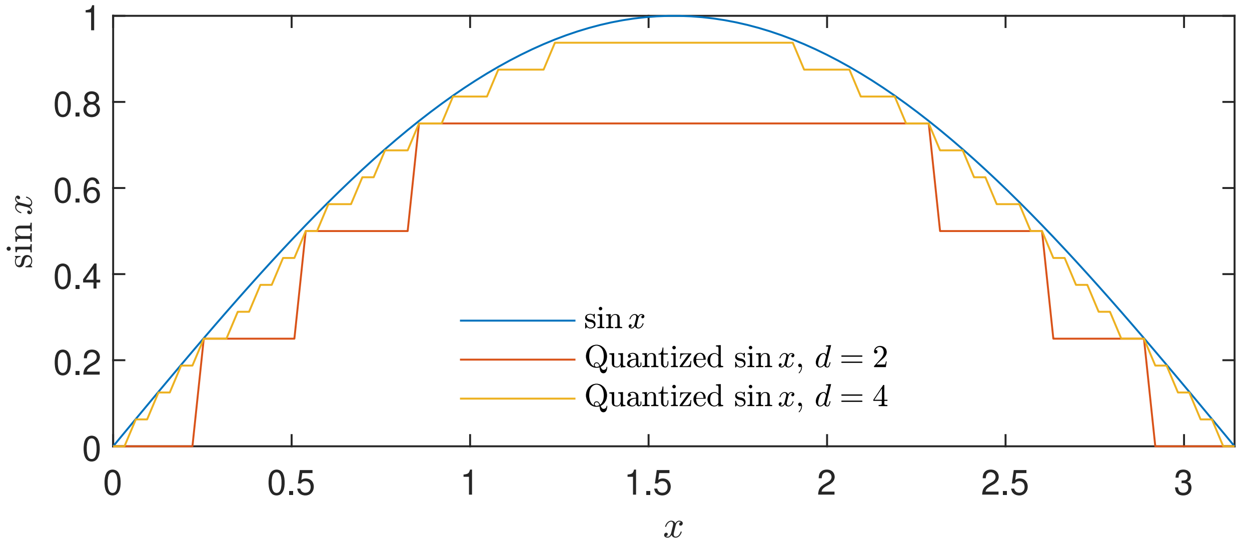

Figure 4.2: Schematic of closed-loop system under encrypted MPC.

4.2 Simulation results

We apply the encrypted LMPC to the CSTR initialized from the point, $x_0 = [-1.7 kmol/m^3 \quad 50K]$, and observe the closed-loop simulation results for values of d between 1 and 8, inclusive. The state and input profiles are shown in figs. 4.3 to 4.10. In figs. 4.3 to 4.5, it can be observed that the state x_1 as well as the input u_1 experience large oscillations when using the encrypted MPC, rendering the encrypted MPC unable to practically stabilize the closed-loop system in the sense of trapping the states in a small neighborhood $\Omega_{\rho_{\min}}$ around the origin. This can be attributed to the large quantization error at values of $d \leq 3$. For $d = 1$, with the quantizated states being separated by a resolution of 2^{-1} or 0.5, it is observed that the dithering in Figure 4 begins when the state x_1 first crosses the threshold of -0.25, causing any values above this to be mapped to zero. A similar behavior is seen in Figure 5 for $d = 2$, where the resolution is higher and the dithering begins when x_1 reaches a value greater than -0.125, implying that $d = 2$ is still smaller than necessary for this system. At $d = 4$, as seen in fig. 4.6, the states under the MPC with and without encryption almost overlap, with the oscillations/dithering in x_1 and u_1 mostly mitigated. At values of $d \geq 5$, the quantization error is sufficiently small, leading to the closed-loop states and manipulated input profiles under MPC with and without encryption being nearly identical, as seen in figs. 4.7 to 4.10. Since the closed-loop states are driven by the encrypted MPC to a neighborhood $\Omega_{\rho_{\min}}$ around the origin, the system is considered to be rendered stable for $d \geq 5$. At increasing values of d, the quantized states and inputs are allowed to assume values from a larger set $\mathbb{Q}_{l_1,d}$, letting the error in eq. (2.6) be reduced further. This leads to the improved closed-loop performance for larger d.

Remark 3. Following the results of theorem 1, it is known that the states of the nonlinear system of eq. (2.1) will be bounded in a ball of radius b, which is a class $\mathcal{K}$ function of $\mu = f(d)$, which is an exponentially decreasing function of d provided the modeling errors γ_1 and γ_2 remain the same (i.e., model remains the same). In the reactor system of eq. (4.1), when $d < 5$, it can be inferred that the small value of d causes μ and, hence, b to be large. Specifically, $b > \rho_{\min} = 0.01$ is too large for the states to be maintained in the invariant set $\Omega_{\rho_{\min}}$ as $t \to \infty$. If the stability criterion is less strict and a larger $\rho_{\min}$ is selected, the system can be considered stable under the MPC for $d < 5$. However, this is a process design criterion that must be chosen by domain experts, and our results remain valid for arbitrary values of d and $\rho_{\min}$.

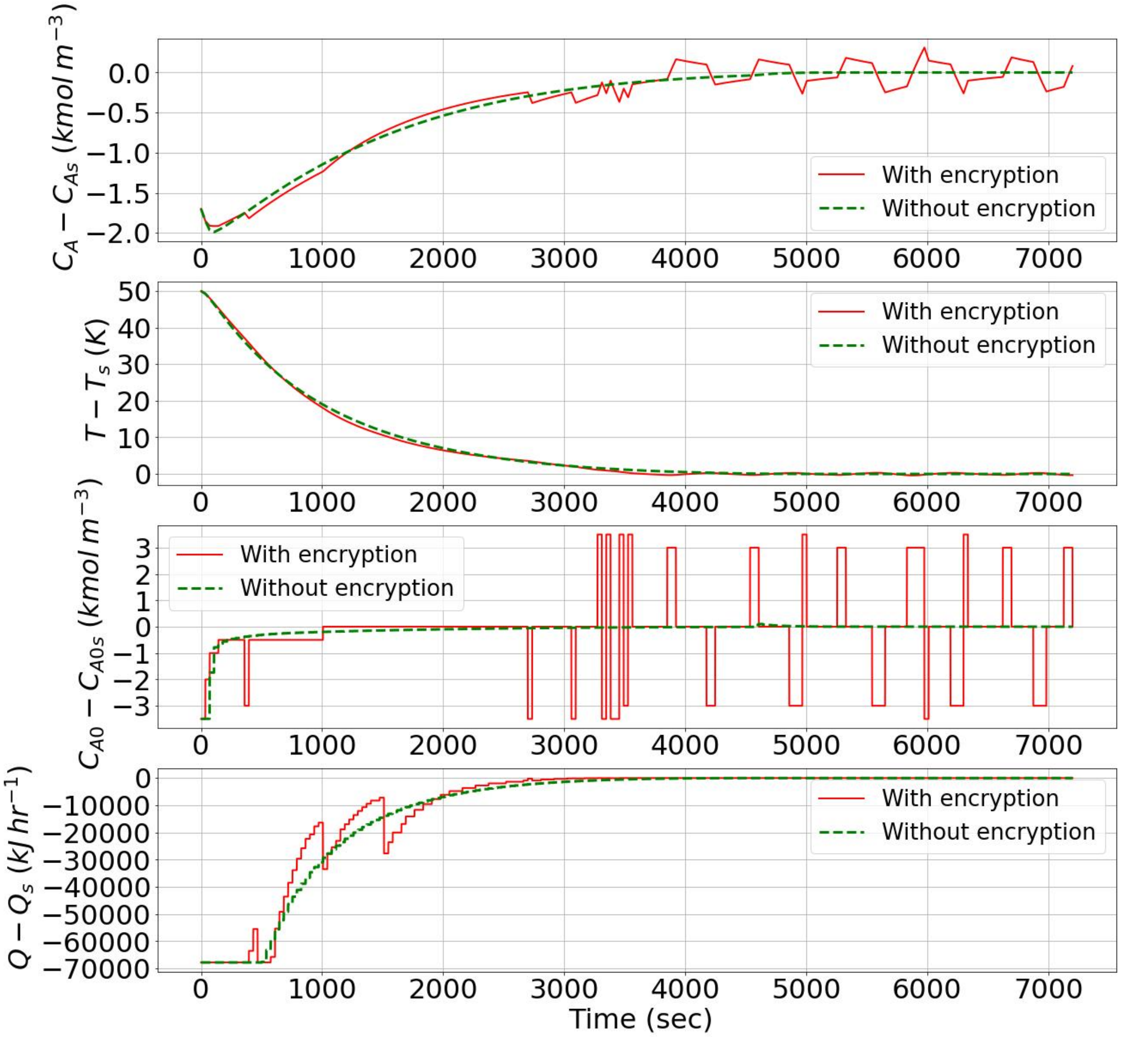

Figure 4.3: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 1$, for the stable steady state.

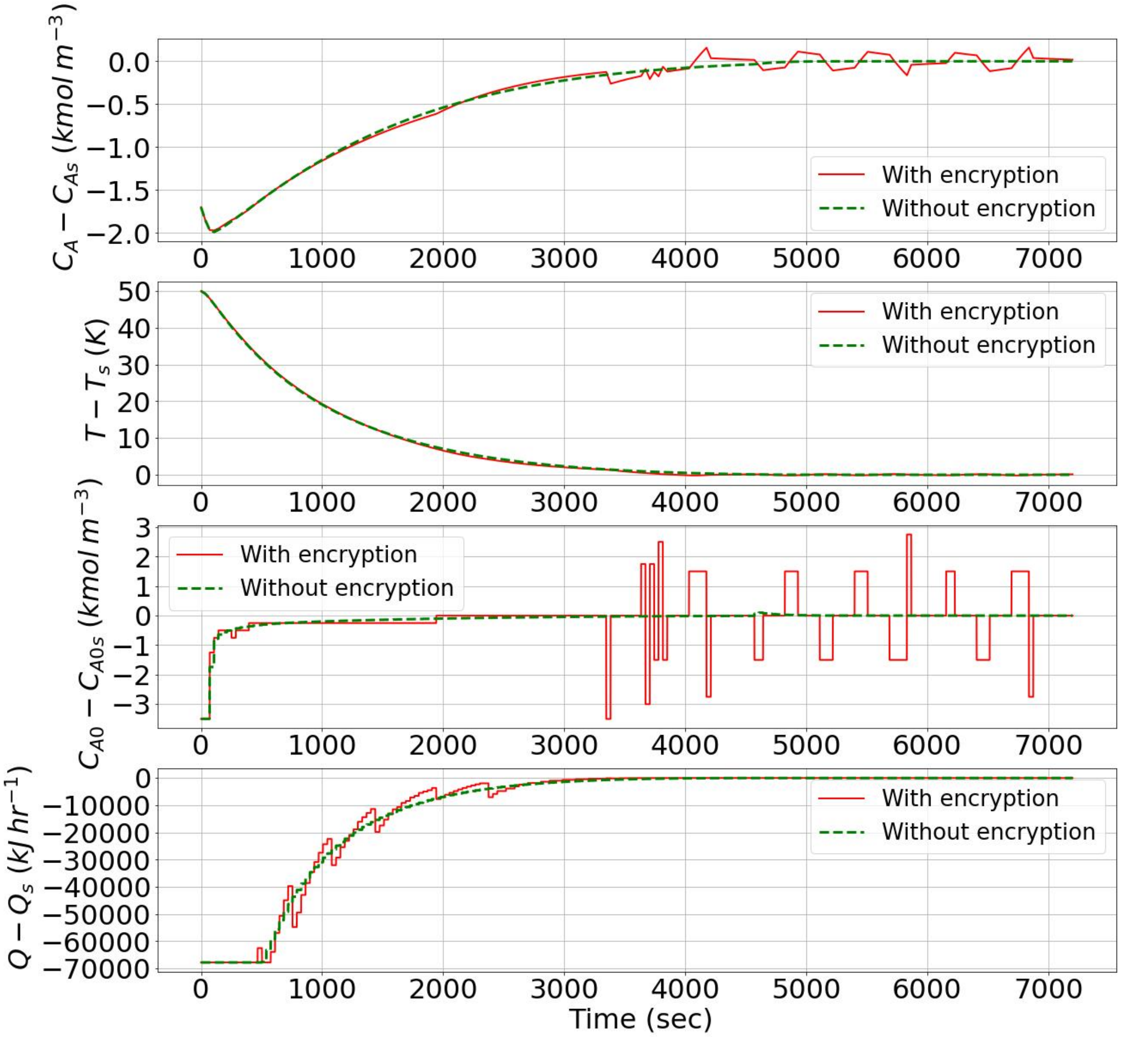

Figure 4.4: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 2$, for the stable steady state.

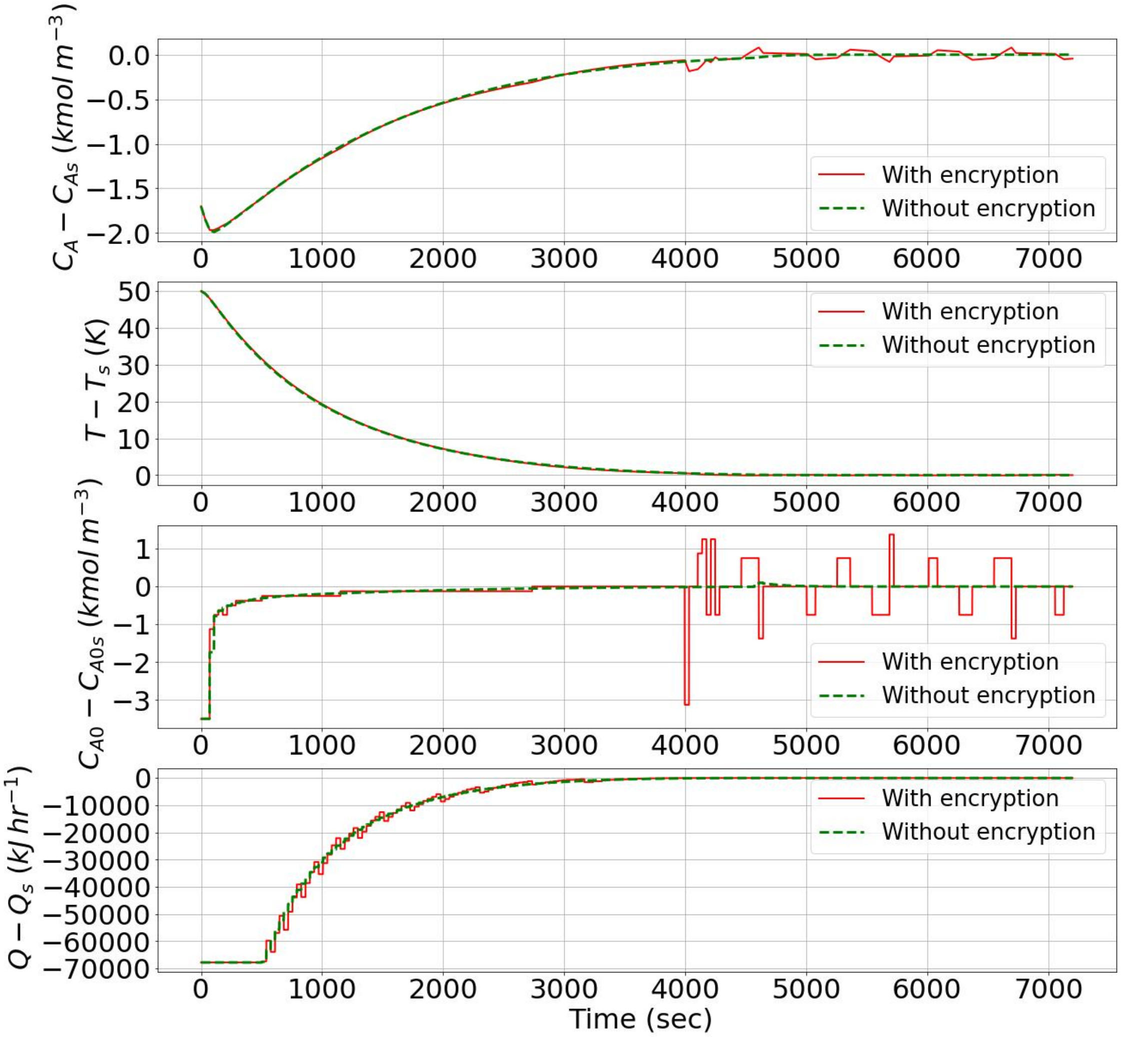

Figure 4.5: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 3$, for the stable steady state.

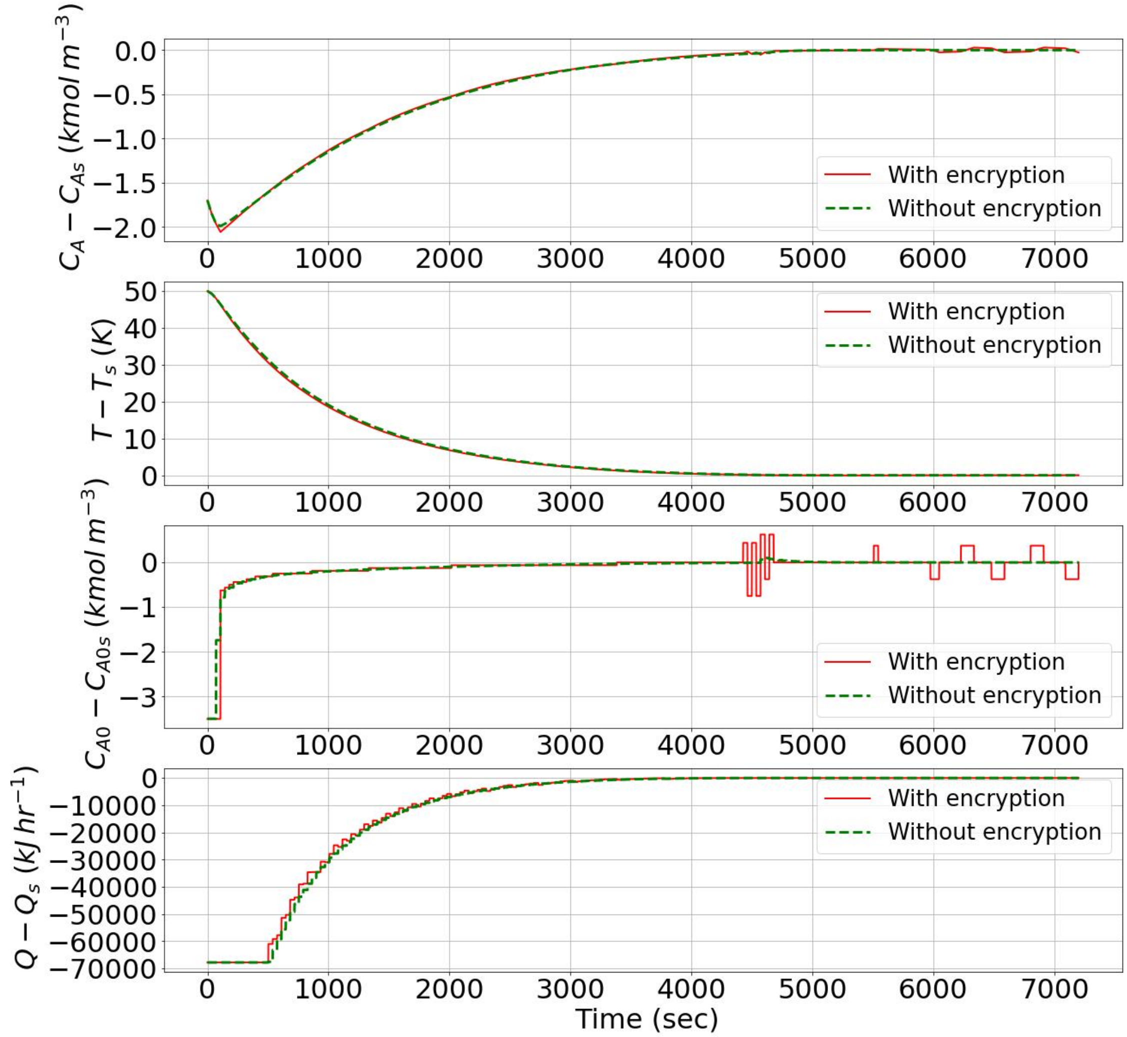

Figure 4.6: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 4$, for the stable steady state.

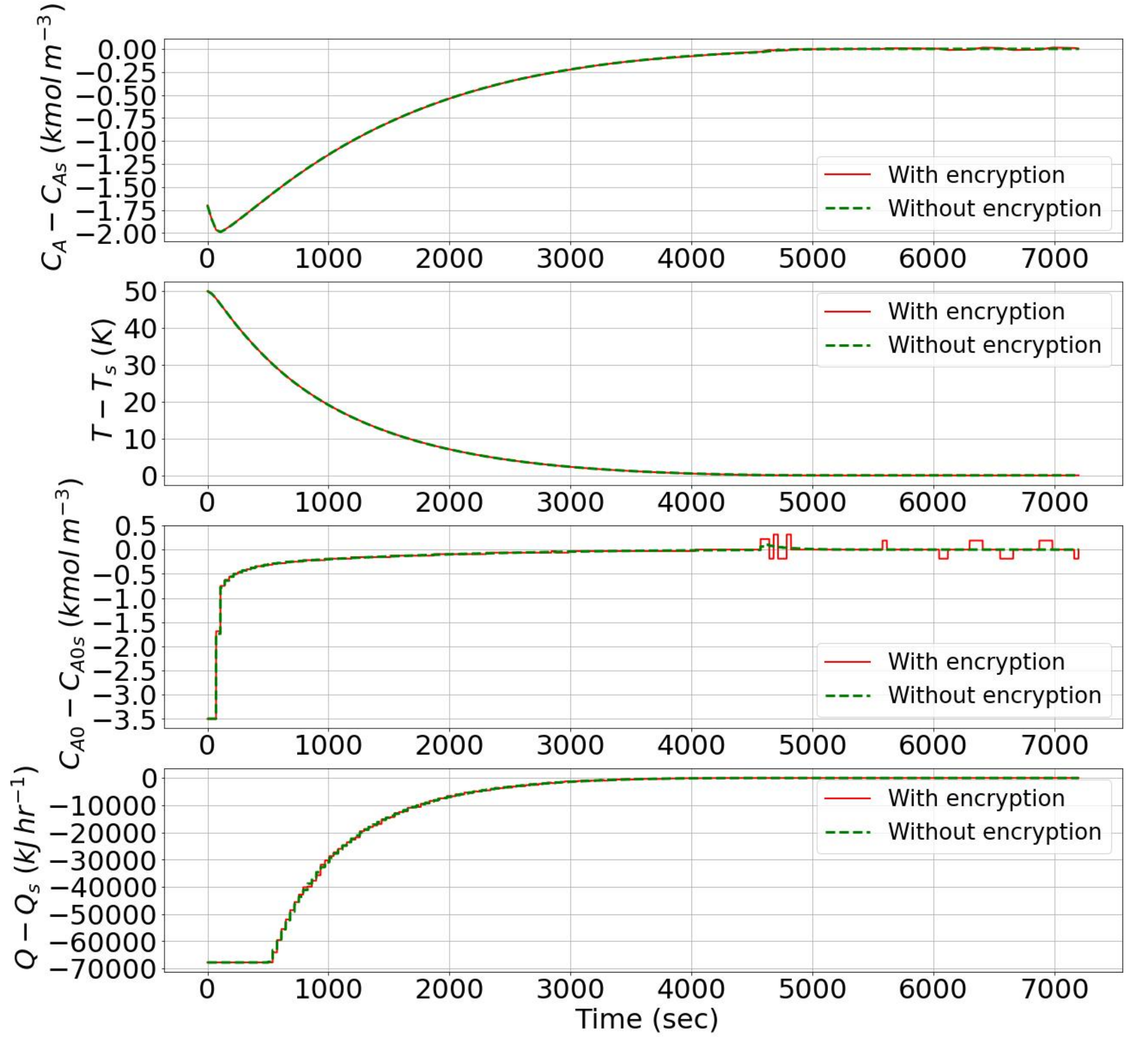

Figure 4.7: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 5$, for the stable steady state.

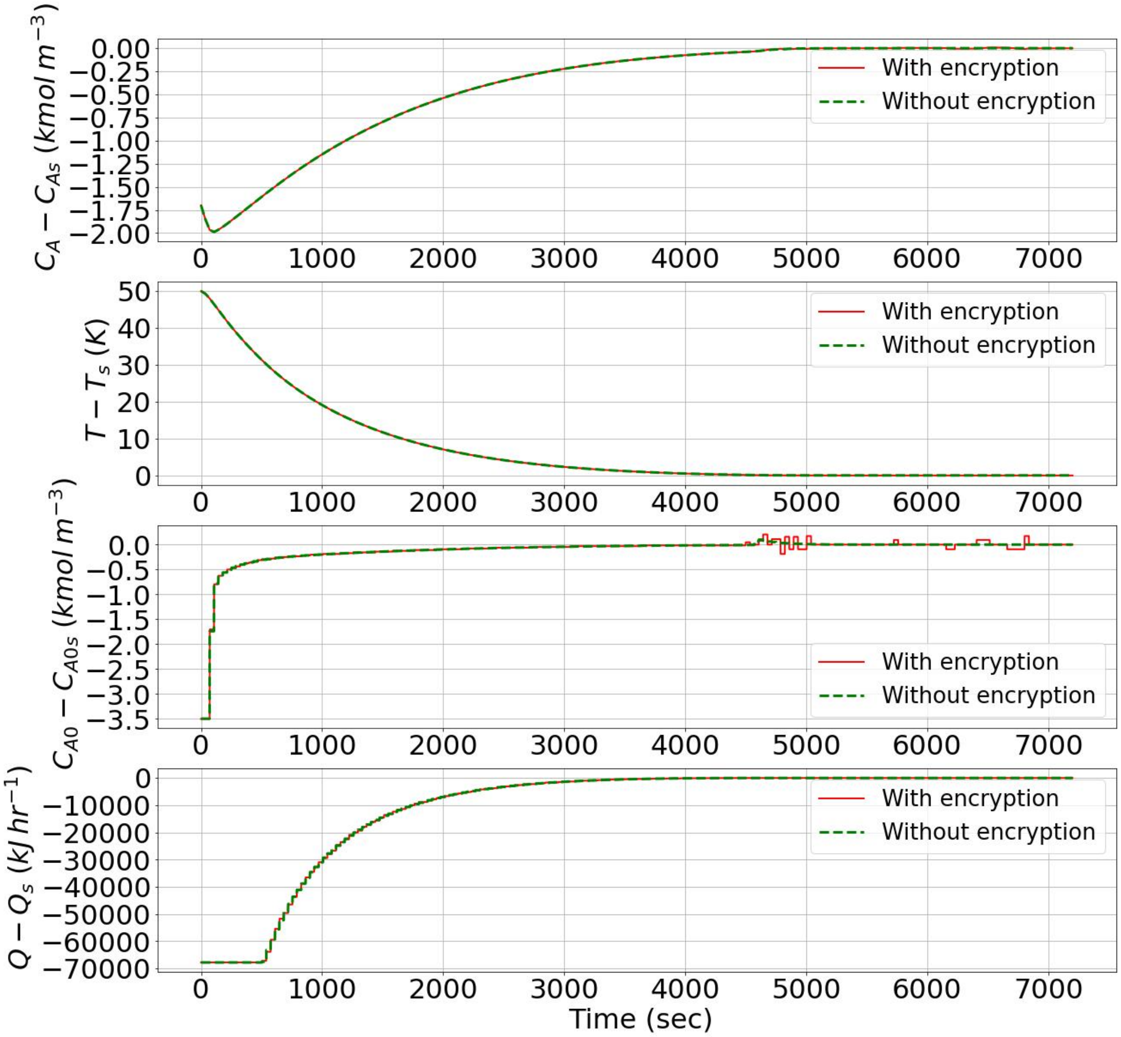

Figure 4.8: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 6$, for the stable steady state.

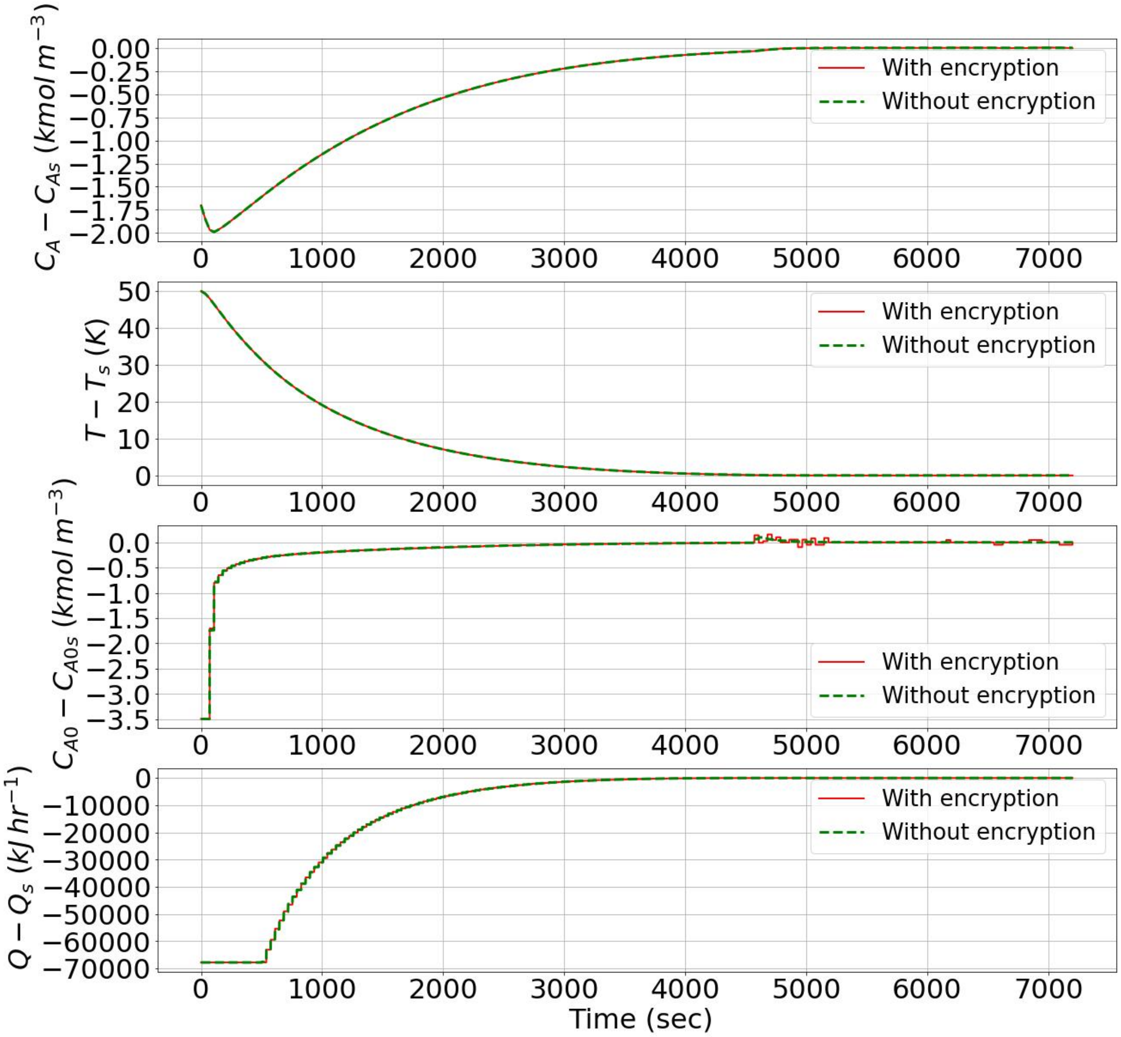

Figure 4.9: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 7$, for the stable steady state.

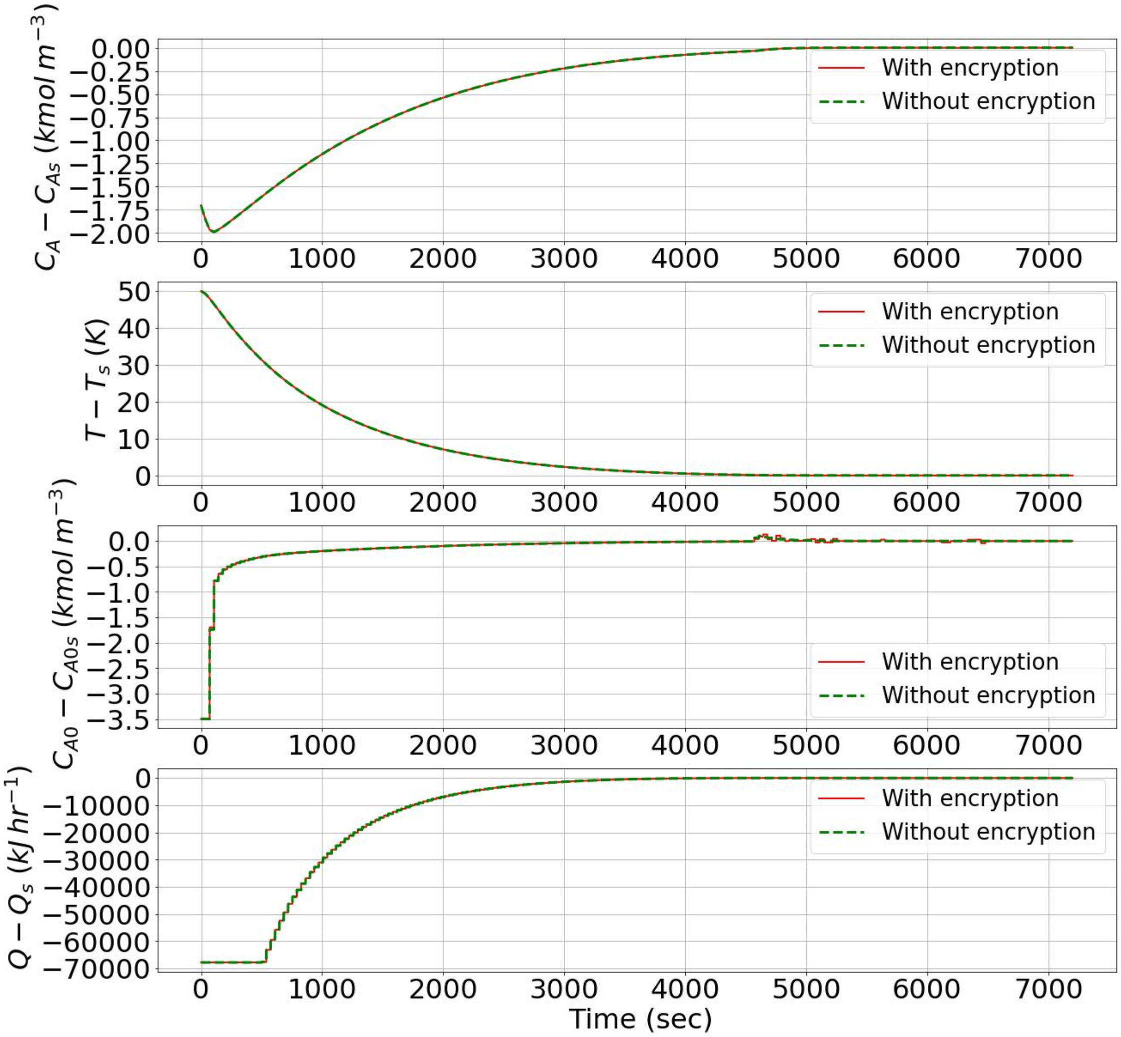

Figure 4.10: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 8$, for the stable steady state.

Chapter 5

Application to a chemical reactor operating at an unstable steady-state

5.1 Process description

We implement the proposed encrypted LMPC to the chemical process studied in Ref. [26] i.e., a jacketed, perfectly mixed CSTR in which the irreversible, second-order, elementary, exothermic reaction $A \to B$ takes place. The following mass and energy balances describe the transient operation of the nonisothermal CSTR:

$$\frac{\mathrm{d}C_A}{\mathrm{d}t} = \frac{F}{V}\left(C_{A0} - C_A\right) - k_0 \mathrm{e}^{\frac{-E}{RT}} C_A^2 \tag{5.1a}$$

$$\frac{\mathrm{d}T}{\mathrm{d}t} = \frac{F}{V}\left(T_0 - T\right) + \frac{-\Delta H}{\rho_L C_p} k_0 \mathrm{e}^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{5.1b}$$

where the symbols carry the same denotations as chapter 4. Parameter values are enlisted in Ref. [26]. The state variables are the concentration of A and reactor temperature, C_A and T, respectively, in deviation terms i.e., $x^T = [C_A - C_{As} \quad T - T_s]$. The inlet feed concentration C_{A0} and the rate of heat removal Q are the manipulated inputs to our process, which are bounded to be in the closed sets: $Q \in [-80.0, 80.0]\ MJ/h$ and $C_{A0} \in [0.5, 7.5]\ kmol/m^3$. We are interested in operating the CSTR at its unstable steady state, $[C_{As} \quad T_s] = [1.95 kmol/m^3 \quad 402K]$, corresponding to inputs of $Q_s = 0MJ/h$ and $C_{A0s} = 4kmol/m^3$.

The control objective is to maintain the operation of the CSTR at its unstable steady state under the encrypted LMPC using the quantized states and inputs in computations and actuation. For the Pallier encryption algorithm, we choose $l_1 - d$ and l_2 to be 20 and 31, respectively. The sampling time Δ and integration time step h_c are chosen to be 10^{-2} hr and 10^{-4} hr, respectively. The positive definite matrix P in the control Lyapunov function $V = x^T P x$ for this system is taken as

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix}$$

based on extensive simulations. A prediction horizon of $N = 2$ is used in the LMPC. With respect to stability under the LMPC, we choose $\rho_{\min} = 2$ as the criterion for the states having reached stability and use a contractive constraint of the form $\dot{V} \leq -kV$ for eq. (3.11e), where $k = 0.15$. The weight matrices Q_1 and Q_2 in the LMPC cost function are chosen as $Q_1 = \begin{bmatrix} 10000 & 0 \\ 0 & 1 \end{bmatrix}$ and $Q_2 = \begin{bmatrix} 3 \times 10^{-7} & 0 \\ 0 & 1 \end{bmatrix}$, respectively.

5.2 Simulation results

The proposed encrypted LMPC is applied to the nonisothermal CSTR operating near its unstable steady state. Specifically, the initial condition is $x_0 = [-1.69\ kmol/m^3 \quad 73\ K]$, and values of d between 1 and 7, inclusive, are studied. The state and input profiles are shown in figs. 5.1 to 5.7. From the results of closed-loop encrypted MPC simulations, it can be observed that, for some small value of the quantization parameter, d, the encrypted MPC is not able to stabilize the nonlinear system around a small neighborhood around the origin. Instead, we observe the oscillations of states around a point other than the unstable steady state. Based on fig. 5.1, this may be attributed to the large quantization error in the input applied to the system. While the MPC calculates an exact fixed-point value, the quantization with a low resolution withholds the systems from applying this input. In particular, since $d = 1$, the manipulated C_{A0} that can be applied to the system oscillates between the values of 2.0 $kmol/m^3$ and 2.5 $kmol/m^3$. Thus, for systems being operated at an unstable equilibrium, it is possible that the encrypted MPC cannot practically stabilize the system for $d \leq d_{\text{critical}}$, and it is important to identify this critical value of the quantization parameter. For the nonlinear system of eq. (5.1), we have $d_{\text{critical}} = 1$, as evidenced by the removal of oscillations and approach to the steady state once d is increased from 1 to 2 in fig. 5.2. Additionally, for $d > d_{\text{critical}}$, as the value of the quantization parameter d increases, we see improvement in MPC performance in the sense that we achieve faster convergence of states to a small neighborhood, $\Omega_{\rho_{\min}}$, around the origin and also less controller effort is required to reach the steady state. The MPC performance improved because the quantization error significantly decreases with the increase in d. However, this improvement in performance comes at a computational cost, which is discussed in the subsequent section. It is important to note that, if the computational resources are limited, the MPC performance that can be achieved is also limited but one must ensure that the chosen value of quantization parameter d is larger than the critical value, d_{critical}.

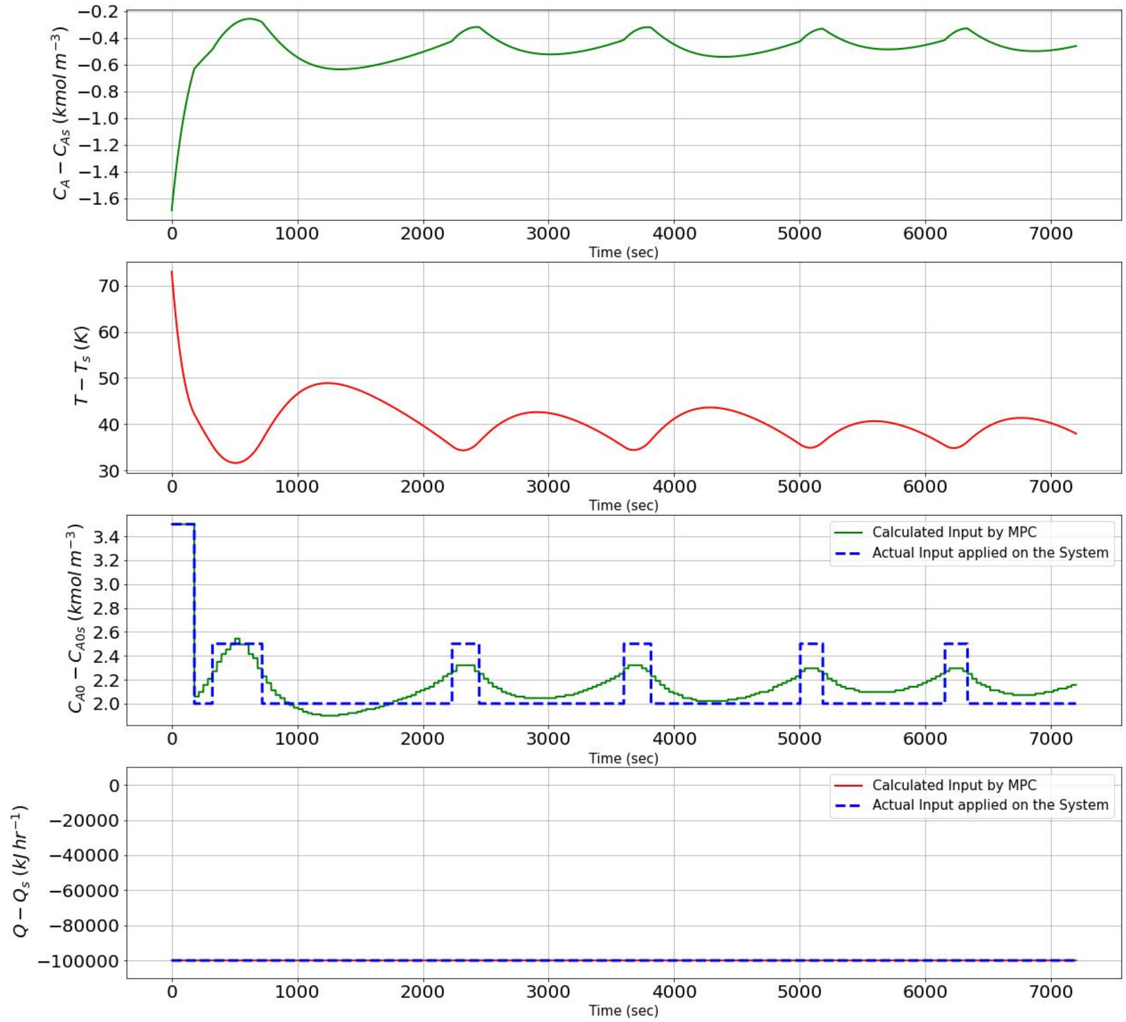

Figure 5.1: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 1$, for the unstable steady state.

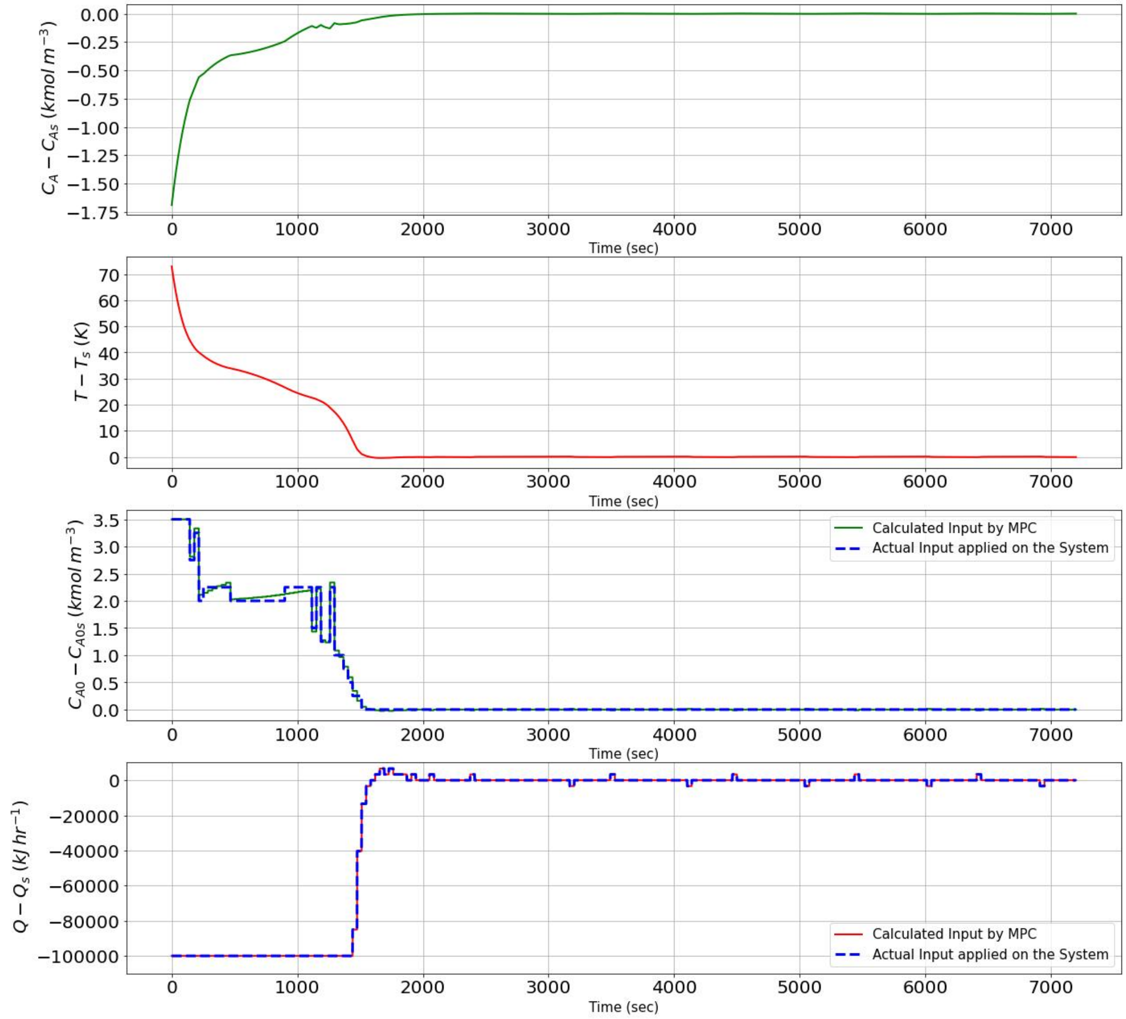

Figure 5.2: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 2$, for the unstable steady state.

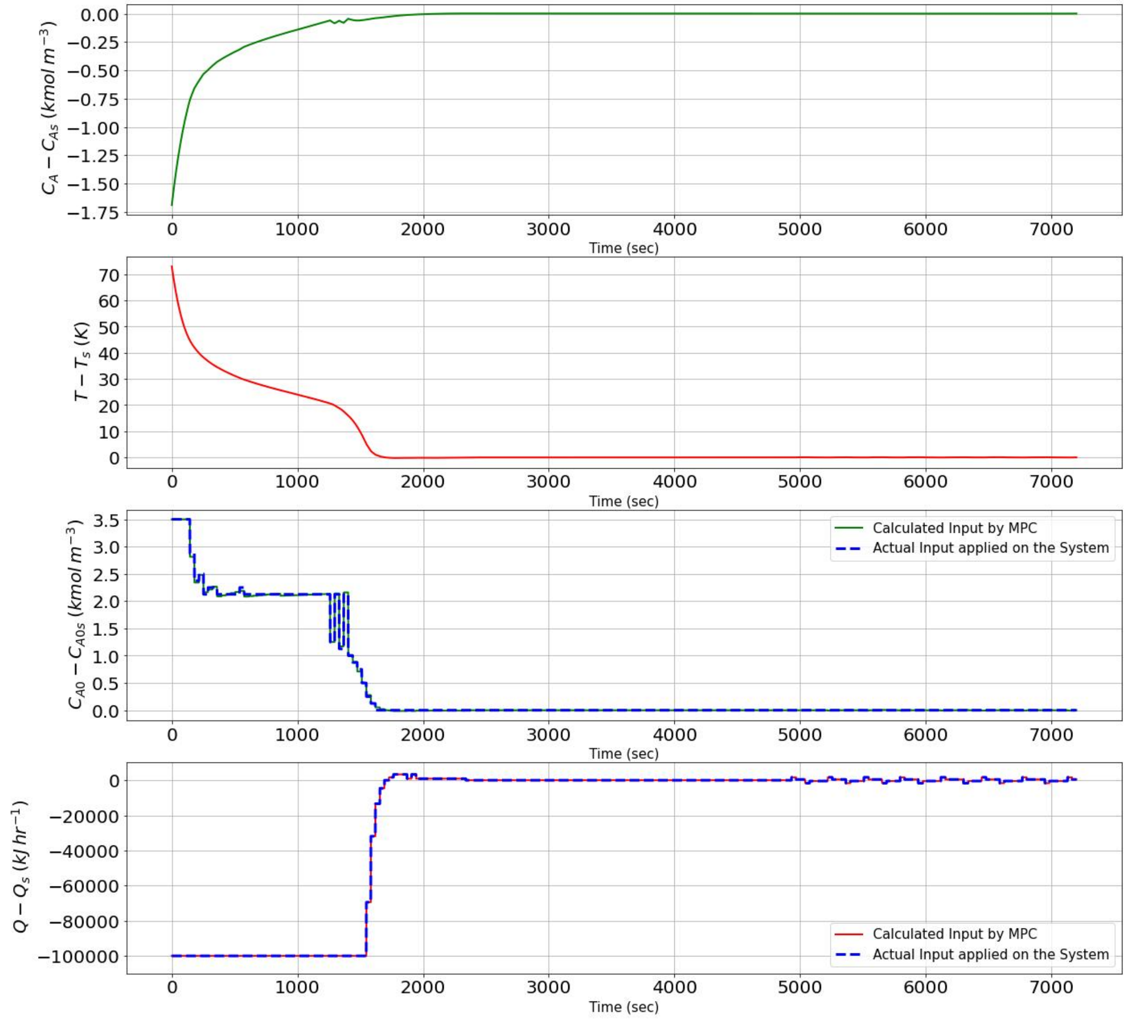

Figure 5.3: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 3$, for the unstable steady state.

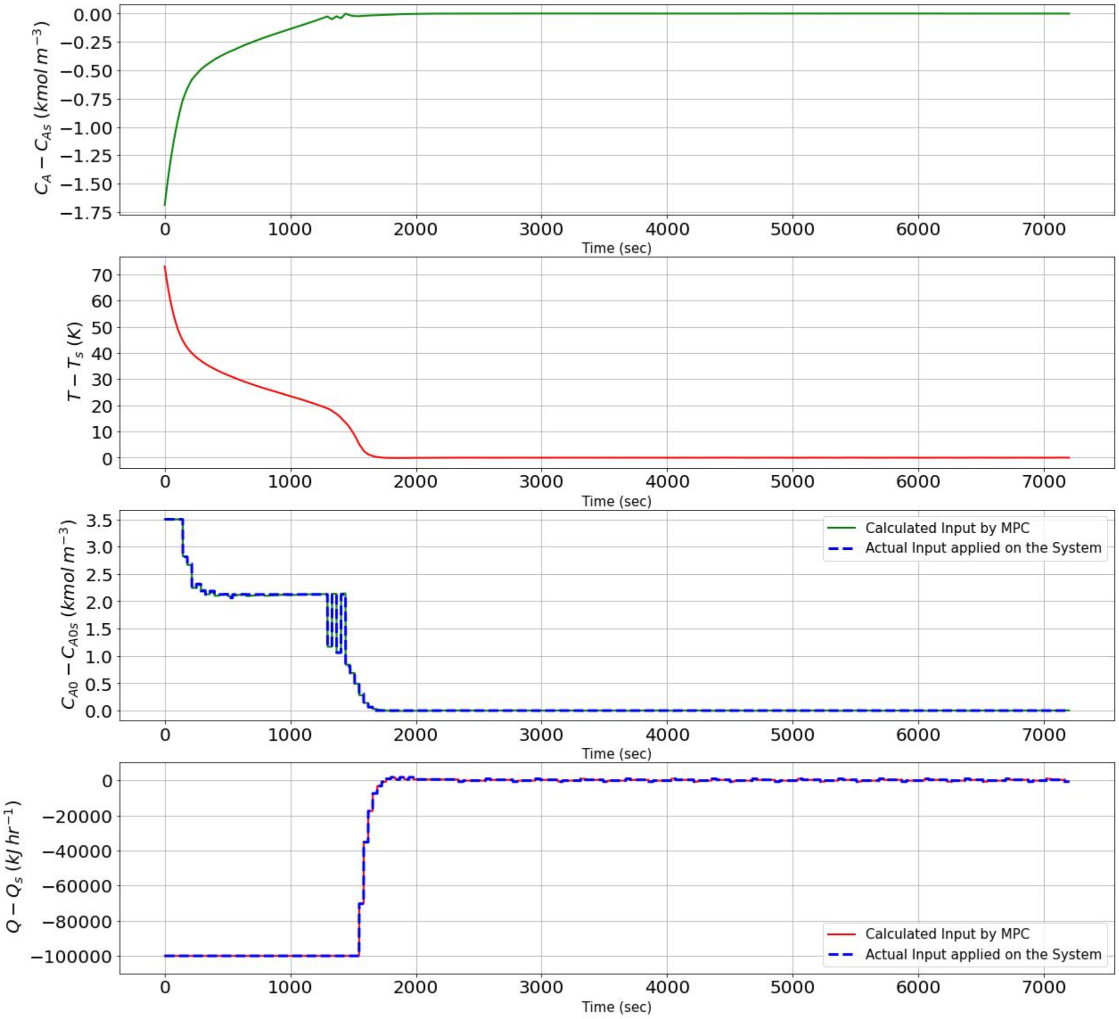

Figure 5.4: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 4$, for the unstable steady state.

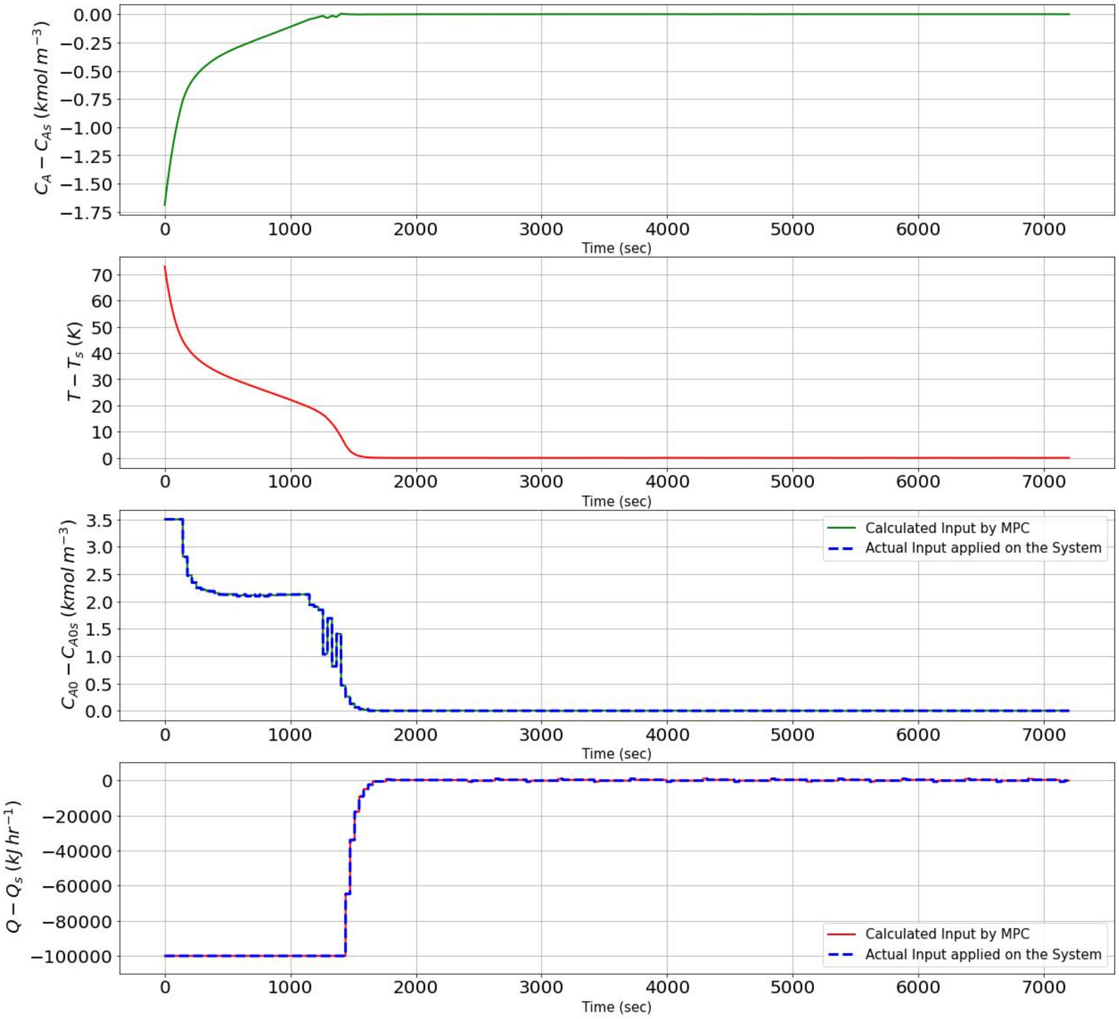

Figure 5.5: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 5$, for the unstable steady state.

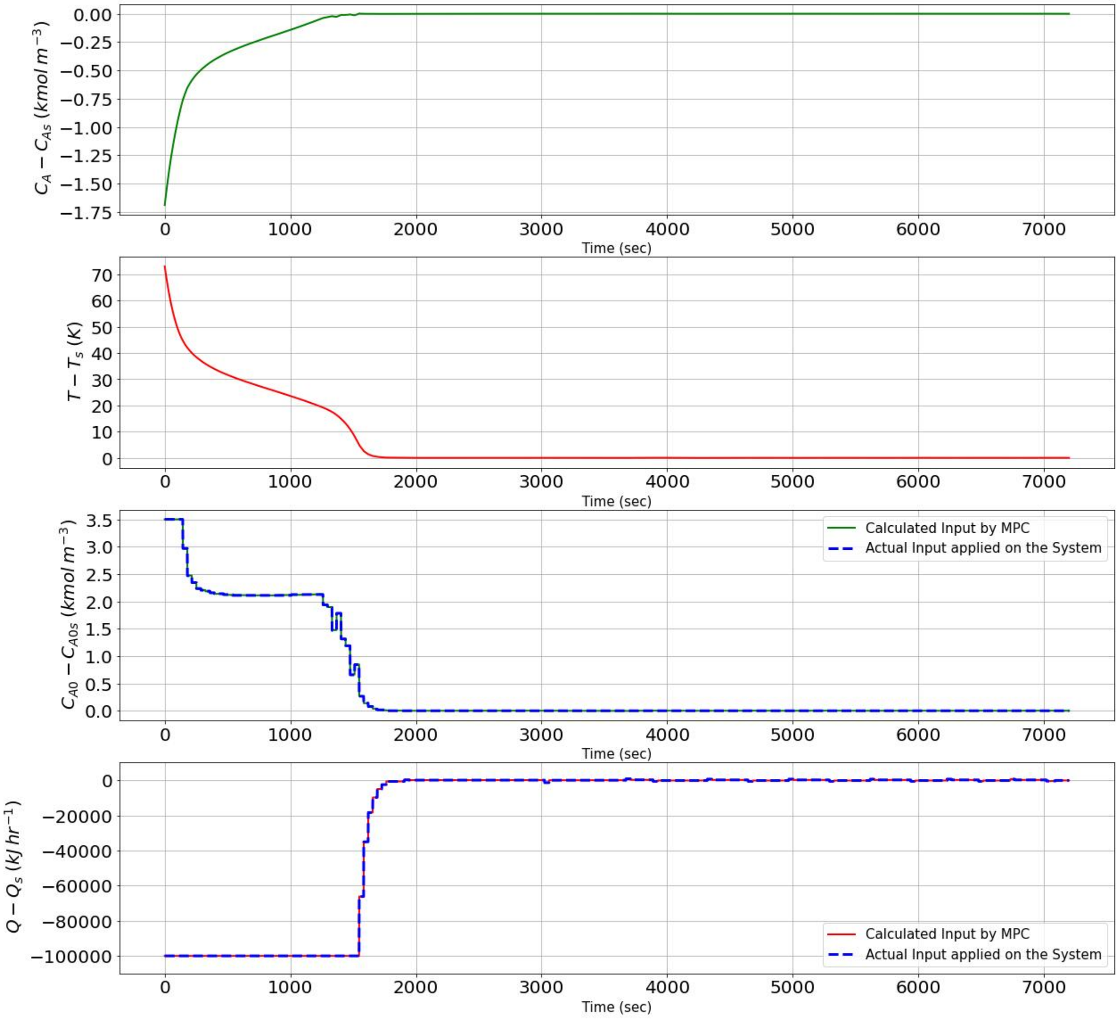

Figure 5.6: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 6$, for the unstable steady state.

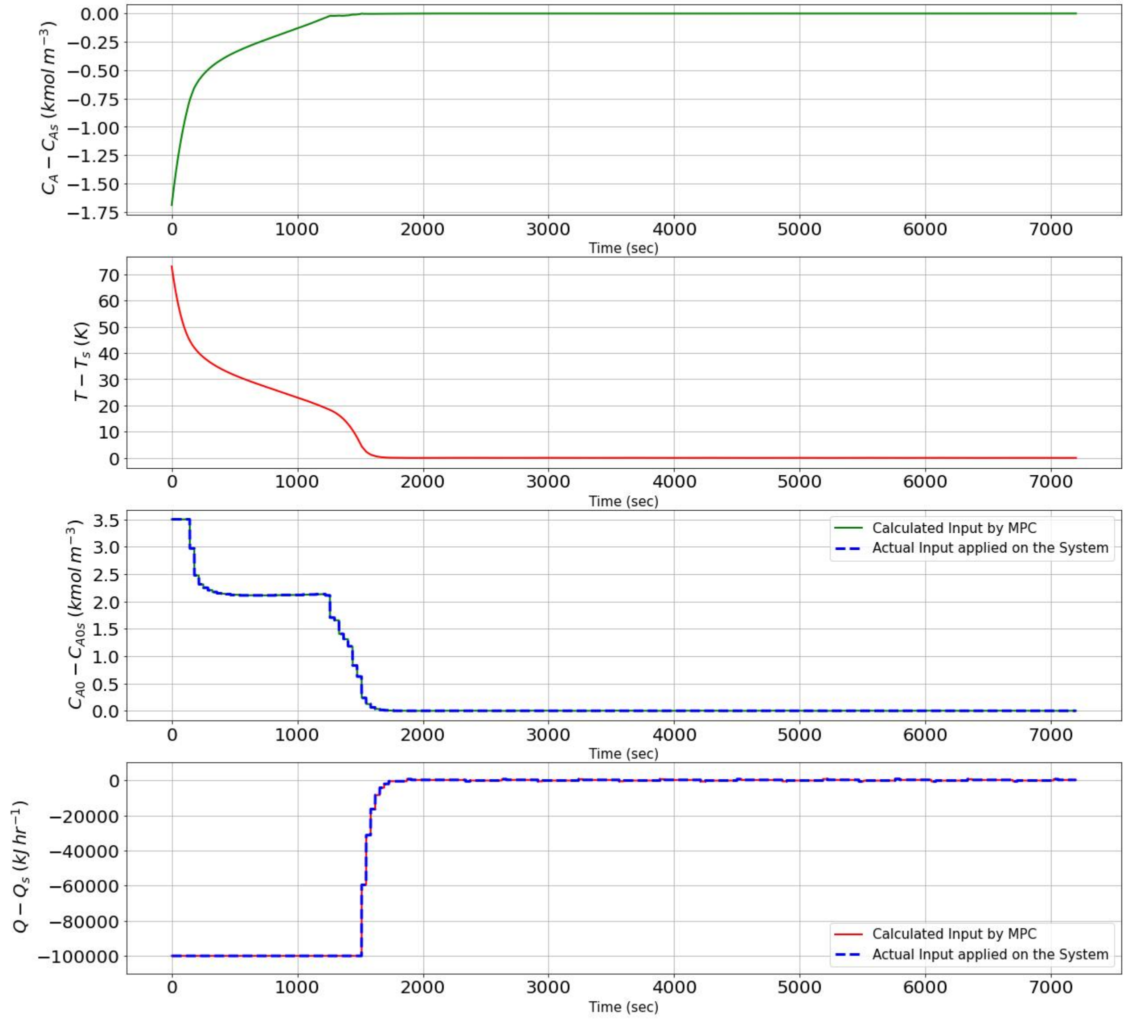

Figure 5.7: State and input profiles of closed-loop simulations under LMPC with encryption (red line) and without encryption (green line), where $d = 7$, for the unstable steady state.

Chapter 6

Effect of the quantization parameter and the MPC optimization on computational cost

From fig. 6.1, it is clear that the computational cost increases with an increase in the value of the quantization parameter d. The increase in computational cost with the increase in the magnitude of d is primarily attributed to two reasons. The resolution between the elements of the set $\mathbb{Q}_{l_1,d}$ is equal to 2^{-d}. As the magnitude of d increases, the resolution of the set decreases and, hence, the number of elements in the set increases. Firstly, as a direct consequence of the increase in the number of elements, the computational cost required to construct such a set also increases. Secondly, as the number of elements in the set $\mathbb{Q}_{l_1,d}$ increases, the number of search operations required to map a real number to the set $\mathbb{Q}_{l_1,d}$ increases and, hence, the computational cost associated with it also increases. For the purpose of simulation of the CSTR with a stable steady-state, a normalized computational cost, associated with the quantization parameter d, was calculated for all the cases. This computational cost was a weighted sum of the number of operations required to construct the set $\mathbb{Q}_{l_1,d}$ and the number of search operations required to map real number states and inputs to the set $\mathbb{Q}_{l_1,d}$. The weights depend on the computational time required for the above two kinds of operations. Finally, the computational cost is normalized using the maximum computational cost out of all the cases, which corresponds to the computational cost associated with the case when $d = 8$.

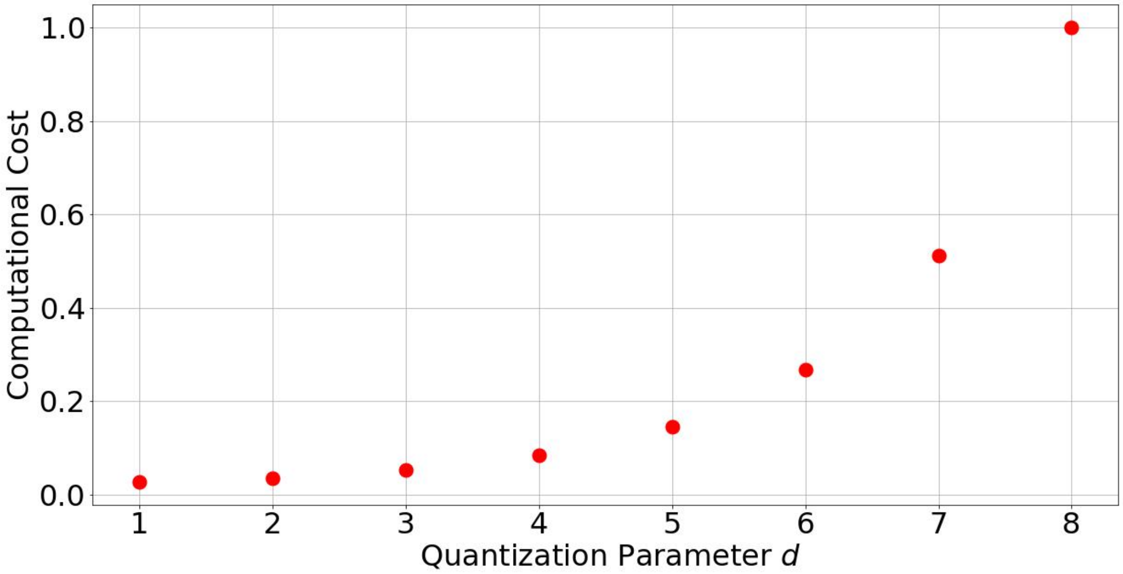

Figure 6.1: Normalized computational cost associated with different values of the quantization parameter d.

It is clear from fig. 6.1 that, if the computational resources are limited, the highest degree of accuracy (with respect to performance in comparison to MPC without encryption) that can be achieved by the encrypted MPC scheme is also limited.

Relative to the MPC problem, the encryption/decryption algorithm requires a significantly larger computational load. Figure 6.2 shows, for $d = 1$, the ratio of the time it takes to perform all the encryption/decryption operations to the time required to solve the MPC optimization problem for every sampling period over the simulation duration. It is observed that the time taken for encryption/decryption is an order of magnitude higher than the time required to solve the MPC for most sampling periods. The ratio is equal to approximately 10 in the first half of the simulation and varies between approximately 6 and 18 for the second half. As the value of d increases, a larger portion of the computational load will be shifted to the encryption/decryption operations because a higher number of binary search operations will be required for encryption/decryption, while the MPC problem remains the same in terms of complexity, leading to even higher ratios in fig. 6.2.

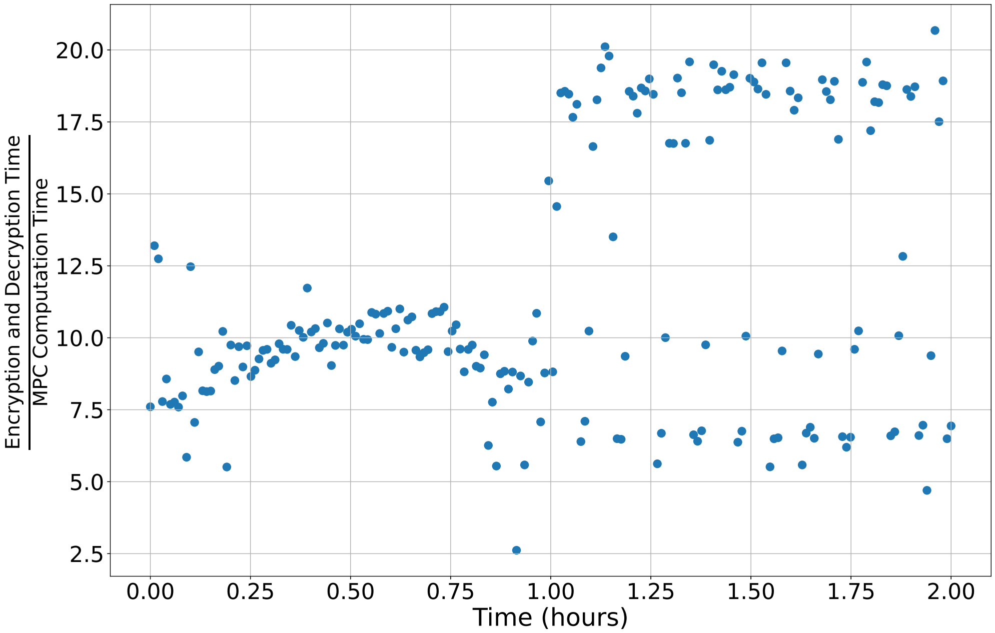

Figure 6.2: Ratio of time required for encryption/decryption operations to the time required for solving the MPC optimization problem, for each sampling period throughout the simulation of the CSTR with the stable steady state when d = 1.

Remark 4. As discussed, a larger value of d improves the accuracy at the cost of increasing the computational burden of both generating the set $\mathbb{Q}_{l_1,d}$ (which is a one-time offline computation carried out before implementing the MPC) and the binary search operations to map floating point numbers to the set (which is an online calculation carried out several times in each sampling period of the MPC). Between these two components of the computational cost, however, the generation of the set $\mathbb{Q}_{l_1,d}$ represents an order of magnitude higher number of computations than the binary search operations required to encrypt/decrypt states and inputs within the simulation duration considered. Since the cost of generating $\mathbb{Q}_{l_1,d}$ increases exponentially with d, it is desirable to use a value of d reasonably above d_{critical} but not excessively large in order to balance robustness and computational costs. Since a value of $d = 8$ was sufficient for the applications considered in this work, this was the maximum value of d studied. However, d can be increased as necessary to represent a greater range of floating point numbers for more complex applications or when operating in a wider region. An appropriate starting point may be to use the standard 32-bit representation of floating or fixed point numbers, which corresponds to $d = 14$ in our framework. This requires the generation of the set $\mathbb{Q}_{32,14}$, which contains 4294967296 numbers in the set. The generation of this set, which is an offline calculation before the online MPC implementation, required 1087 seconds on an Intel i7-10700K 3.80 GHz computer with 64 GB of RAM, which was the machine used for all the simulations in this work. Hence, a local machine is sufficient for end-to-end implementation of the proposed encrypted MPC up to at least $d = 14$, corresponding to 32-bit floating or fixed point numbers. If a higher d is required, for which the generation of the set $\mathbb{Q}_{l_1,d}$ is not computationally tractable in a local machine, only the generation of $\mathbb{Q}_{l_1,d}$ may be carried out offline in a high-performance cluster and saved. Subsequently, the generated $\mathbb{Q}_{l_1,d}$ can be loaded and the encrypted MPC can still be implemented in a local machine due to the much lower processing power required for the binary search operations for encryption/decryption within the MPC, which also scale approximately linearly rather than exponentially with d.

Remark 5. While the quantization errors in this work were not compared to other common sources of errors such as sensor noise and plant-model mismatch, as demonstrated above, for values of d below a certain threshold d_{critical}, the quantization error can be significant enough to cause the process to oscillate without stabilizing within the level set $\Omega_{\rho_{\min}}$, causing the closed-loop system to not be practically stabilizable as per the definition in our work. This effect was seen more strongly in the case of operating a reactor at the unstable steady-state. Therefore, irrespective of the plant-model mismatch or sensor noise levels in a chemical process, the quantization errors in an encrypted MPC cannot be neglected in the controller design stage.

Chapter 7

Conclusion

In this work, we developed a closed-loop encrypted MPC scheme using Paillier cryptosystem for encryption-decryption operations in the sensor-controller and controller-actuator communication links. Quantization errors in the secure communication links were identified, based on which closed-loop stability criteria were derived. The designed Lyapunov-based model predictive control scheme was robust to these quantization errors and ultimately drove the states to a small a neighborhood around the steady state of the nonlinear system. Further, the proposed encrypted MPC scheme was implemented on a continuous stirred tank reactor system with recycle and another reactor operating at an unstable equilibrium point. Specifically, closed-loop simulations were carried out for different values of the quantization parameter d. The state and input profiles were plotted against the case of the unencrypted MPC. Larger values of the quantization parameter d resulted in lesser error between the state and input profiles of the encrypted MPC and of the unencrypted MPC; however, a higher computational cost was associated with larger values of the quantization parameter d.

Bibliography

[1] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research*, page 1–11, Belfast, United Kingdom, 2016.

[2] T. Tsvetanov and S. Slaria. The effect of the colonial pipeline shutdown on gasoline prices. *Economics Letters*, 209:110122, 2021.

[3] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, page 355–366, Hong Kong, China, 2011.

[4] T. M. Chen and S. Abu-Nimeh. Lessons from stuxnet. *Computer*, 44:91–93, 2011.

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

[6] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity (version 1.1). Technical report, National Institute of Standards and Technology, 2018.

[7] L. Huang, X. Nguyen, M. Garofalakis, J. M. Hellerstein, M. I. Jordan, A. D. Joseph, and

N. Taft. Communication-efficient online detection of network-wide anomalies. In *Proceedings of 26th IEEE International Conference on Computer Communications*, pages 134–142, Barcelona, Spain, 2007.

[8] S. Omar, A. Ngadi, and H. H. Jebur. Machine learning techniques for anomaly detection: an overview. *International Journal of Computer Applications*, 79:33–41, 2013.

[9] S. Agrawal and J. Agrawal. Survey on anomaly detection using data mining techniques. *Procedia Computer Science*, 60:708–713, 2015.

[10] Z. Wu, F. Albalawi, J. Zhang, Z. Zhang, H. Durand, and P. D. Christofides. Detecting and handling cyber-attacks in model predictive control of chemical processes. *Mathematics*, 6:173, 2018.

[11] Z. Wu, S. Chen, D. Rincon, and P. D. Christofides. Post cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, 159:248–261, 2020.

[12] S. Chen, Z. Wu, and P. D. Christofides. A cyber-secure control-detector architecture for nonlinear processes. *AIChE Journal*, 66:e16907, 2020.

[13] H. Durand. A nonlinear systems framework for cyberattack prevention for chemical process control systems. *Mathematics*, 6:169, 2018.

[14] H. Durand and M. Wegener. Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods. *Mathematics*, 8:499, 2020.

[15] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[16] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, feb 1978.

[17] J. Richalet, A. Rault, J. Testud, and J. Papon. Model predictive heuristic control: Applications to industrial processes. *Automatica*, 14:413–428, 1978.

[18] K. Kogiso and T. Fujita. Cyber-security enhancement of networked control systems using homomorphic encryption. In *Proceedings of the 54th IEEE Conference on Decision and Control*, pages 6836–6843, Osaka, Japan, 2015.

[19] M. S. Darup, A. Redder, I. Shames, F. Farokhi, and D. Quevedo. Towards encrypted MPC for linear constrained systems. *IEEE Control Systems Letters*, 2:195–200, 2017.

[20] M. S. Darup, A. Redder, and D. E. Quevedo. Encrypted cloud-based MPC for linear systems with input constraints. *IFAC-PapersOnLine*, 51:535–542, 2018.

[21] M. S. Darup. Encrypted MPC based on ADMM real-time iterations. *IFAC-PapersOnLine*, 53:3508–3514, 2020.

[22] S. Narasimhan, N. H. El-Farra, and M. J. Ellis. Detectability-based controller design screening for processes under multiplicative cyberattacks. *AIChE Journal*, 68:e17430, 2022.

[23] S. Narasimhan, N. H. El-Farra, and M. J. Ellis. Active multiplicative cyberattack detection utilizing controller switching for process systems. *Journal of Process Control*, 116:64–79, 2022.

[24] S. Narasimhan, N. H. El-Farra, and M. J. Ellis. A control-switching approach for cyberattack detection in process systems with minimal false alarms. *AIChE Journal*, 68:e17875, 2022.

[25] Z. Wu, A. Tran, D. Rincon, and P. D. Christofides. Machine learning-based predictive control of nonlinear processes. part I: Theory. *AIChE Journal*, 65, e16729, 2019.

[26] Z. Wu, A. Tran, D. Rincon, and P. D. Christofides. Machine learning-based predictive control of nonlinear processes. part II: Computational implementation. *AIChE Journal*, 65, e16734, 2019.

[27] Y. Lin and E. D. Sontag. A universal formula for stabilization with bounded controls. *Systems & control letters*, 16:393–397, 1991.

[28] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the International conference on the theory and applications of cryptographic techniques*, pages 223–238, Berlin, Heidelberg, 1999. Springer.

[29] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas. Encrypted control for networked systems: An illustrative introduction and current challenges. *IEEE Control Systems Magazine*, 41:58–78, 2021.

[30] H. Khalil. *Nonlinear Systems*. Pearson Education. Prentice Hall, 2002.

[31] M. Heidarinejad, J. Liu, and P. D. Christofides. Economic model predictive control of nonlinear process systems using lyapunov techniques. *AIChE Journal*, 58:855–870, 2012.

[32] P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Stabilization of nonlinear systems with state and control constraints using lyapunov-based predictive control. *Systems & Control Letters*, 55, 8:650–659, 2006.

[33] M. Ellis and P. D. Christofides. Economic model predictive control of nonlinear time-delay systems: Closed-loop stability and delay compensation. *AIChE Journal*, 61, 12:4152–4165, 2015.

[34] C. Data61. Python paillier library. https://github.com/data61/python-paillier, 2013.

[35] A. Wächter and L. T. Biegler. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Mathematical programming*, 106, 1:25–57, 2006.