Resilient Encryption of Cloud-Based Control Systems

Resiliente Verschlüsselung von cloudbasierten Regelungssystemen

vom Fachbereich Elektrotechnik und Informationstechnik
der Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
zur Verleihung des akademischen Grades

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

genehmigte Dissertation

von

Moritz Fauser

geboren in Neuwied

D386

Tag der mündlichen Prüfung:	28.11.2024
Dekan des Fachbereichs:	Prof. Dr.-Ing. Daniel Görges
Prüfungskommission	
Vorsitzender:	Prof. Dr.-Ing. habil. Norbert Wehn (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau)
Berichterstattende:	Prof. Dr. Ping Zhang (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau)
	Prof. Dr. Moritz Schulze Darup (Technische Universität Dortmund)

Abstract - Cloud-based control systems leverage cloud computing to provide scalable services and real-time resource access over the internet. However, they face vulnerabilities such as eavesdropping and manipulation. This thesis addresses the challenge of securing cloud-based control systems using homomorphic encryption (HE) schemes. A resilient homomorphic encryption (RHE) scheme is developed to ensure signal confidentiality during transmission while enabling control law evaluation directly on ciphertexts. Different from the existing HE schemes, the RHE scheme can neutralize attacks on ciphertexts, allowing the controller to access true sensor data and the actuators to receive true control inputs, even under attack. Based on the RHE scheme, approaches for attack prevention in the post-quantum era, network load reduction and attack detection are proposed. To counter potential quantum computer threats, a post-quantum secure resilient homomorphic encryption (PQS-RHE) scheme is introduced, enhancing resilience against quantum vulnerabilities. For reducing network load, the RHE scheme is extended using the Chinese remainder theorem (CRT), resulting in a multi-slot homomorphic encryption (MS-RHE) scheme. This enables multiple plaintexts to be encrypted into a single ciphertext, reducing the number of transmissions while maintaining ciphertext size. Theoretical and practical analyses of cloud-based control systems secured by the RHE scheme, the PQS-RHE scheme, and the MS-RHE scheme are conducted. Additionally, an attack detection mechanism compatible with the RHE scheme is presented, providing a effective defence against ciphertext manipulation.

Zusammenfassung - Cloudbasierte Regelungssysteme nutzen Cloud-Computing-Technologien, um skalierbare Dienste und Echtzeitzugriff auf Ressourcen über das Internet bereitzustellen. Trotz dieser Vorteile bleibt ihre Sicherheit eine Herausforderung, da solche Systeme anfällig für Abhör- und Manipulationsangriffe sind. Um diese Risiken zu minimieren, widmet sich diese Arbeit der Sicherung cloudbasierter Regelungssysteme durch homomorphe Verschlüsselungsverfahren (HV). Ein zentraler Beitrag ist die Entwicklung eines Resilienten Homomorphen Verschlüsselungsverfahrens (RHV), das die Vertraulichkeit der übertragenen Signale gewährleistet und gleichzeitig die Berechnungsvorschrift des Reglers mit Chiffretexten durchführt. Im Vergleich zu bestehenden HV bietet das RHV den Vorteil, Angriffe auf verschlüsselte Daten zu neutralisieren. Dadurch stellt es sicher, dass der Regler weiterhin die echten Sensordaten erhält und die Aktoren korrekte Steuerungssignale empfangen, selbst unter Angriffsbedingungen. Aufbauend auf diesem Ansatz werden weiterführende Methoden entwickelt. Erstens wird ein Post-Quantensicheres Resilientes Homomorphes Verschlüsselungsverfahren (PQS-RHV) entwickelt, das gegen Bedrohungen durch Quantencomputer schützt und so die Sicherheit des Systems in der Post-Quanten-Ära gewährleistet. Zweitens wird zur Reduzierung der Netzwerklast das Verfahren durch den Einsatz des Chinesischen Restsatzes (CR) erweitert, was zur Einführung des Multi-Slot Resilienten homomorphen Verschlüsselungsverfahrens (MS-RHV) führt. Dieses erlaubt die Verschlüsselung mehrerer Signale in einem einzigen Chiffretext und reduziert so die Anzahl der Übertragungen ohne die Größe der Chiffretexte zu erhöhen. Schließlich werden theoretische und praktische Analysen durchgeführt, um die Effektivität der mit RHV, PQS-RHV und MS-RHV gesicherten Systeme zu bewerten. Ergänzend wird ein mit dem RHV kompatibler Angriffserkennungsmechanismus vorgestellt, der Manipulationen an Chiffretexten detektiert.

Contents

List of Figures

1 Introduction

1.1 Motivation

Cloud-based control systems become a wide spread solution to take advantage of the cloud computing technology. Since data can be outsourced and processed in a cloud, controller parameters and the data from sensors can be configured and monitored over the internet. Moreover, the amount of cloud storage and processing power can be adjusted on demand. Thus, cloud-based control systems bring much improvements in terms of flexibility and scalability and have been realized in a wide range of industry applications, such as process control, energy management, building automation and manufacturing (Givehchi et al., 2014; Faruque and Vatanparvar, 2015; Siderska and Jadaan, 2018). However, the benefits of cloud-based control systems come with several risks, like processing sensitive data over a public network and storing it in a cloud hosted by a third party can leave it vulnerable to eavesdropping and manipulation. The configuration of computing services and resources in the cloud is managed by cloud users according to their own security requirements (National Security Agency, 2020). Tasks such as threat detection, handling internal incidents, and patching/updating customer cloud environments are the responsibility of the customers. Thus, for instance, a malicious adversary can target the vulnerabilities of an unpatched web application to compromise the cloud architecture and obtain sensitive data stored in the cloud platform. Furthermore, an adversary could attempt to access the control network connected to the cloud resources with the aim of manipulating the data flow within the control system so that the data are changed in an unauthorized manner or data are not accessible when needed. Therefore, protecting the sensitive data in a cloud-based control system is not solely the responsibility of the cloud provider, cloud users must also take measures to safeguard their own data to reduce the risks related to confidentiality, integrity and availability.

Indeed, real cases of cyber attack incidents targeting explicit industrial control systems have increased both in number and complexity in recent years. Many of those incidents have been reported, while many are still undisclosed or unattributed (Langner, 2013; Lee et al., 2016; CISA, 2017). For this reason, interest in security for cloud-based control systems has increased the past ten years (Darup et al., 2021). Moreover, the European commission enforces more regulations for the prevention of cyber attacks (see, for instance, RED (2014), CRA (2022) and NIS2-Directive (2022)). Thus, approaches are required to secure cloud-based control systems against cyber attacks.

The current methods used to counteract cyber attacks raise two concerns. First of all, conventional tools provided by cryptography and control are often not sufficient

to protect a cloud-based control system because advanced cyber attacks can bypass their defence mechanisms (Van Dijk et al., 2010; Darup et al., 2021). Secondly, even if there are approaches that can provide one traditional security objective such as confidentiality, integrity or availability, it is not trivial to combine them and achieve more than one security objective. Consequently, novel defence mechanisms are required that achieve multiple security objectives to effectively counter a wide range of cyber attacks.

1.2 Objectives

In this thesis, the focus is on the cyber security of processes that employ the concept of a cloud-based control system. For this purpose, a resilient homomorphic encryption (RHE) scheme has been developed. Based on the RHE scheme, an approach for attack prevention in the post-quantum era, network load reduction and attack detection is presented. Moreover, the proposed encryption schemes have been analyzed and compared to each other to give more insights into cloud-based control systems encrypted by these approaches.

The main contributions of this thesis are as follows.

- Vulnerability and resilience: The vulnerability of homomorphic encryption (HE) schemes to sophisticated cyber attacks, such as covert attacks, is investigated by employing a somewhat HE scheme. To cope with the vulnerability, the RHE scheme is developed by modifying the somewhat HE scheme. Different from the existing HE schemes, the RHE scheme is able to neutralize the effect of an attack injected into the ciphertexts. Thus, the controller can get the true sensor information and the actuators can get the true control input signals even if an attack takes place in the control system. The RHE scheme is homomorphic with respect to the matrix-vector product. By transforming the dynamic output feedback controller into a matrix-vector product, both the signals transmitted over the network and the controller parameters can be encrypted. Thus, an unauthorized access to the sensitive data involved in a cloud-based control system is prevented. It will be shown that the transformation between quantized values and integer values causes no error in the calculation of the matrix-vector product. Finally, the influence of the quantization error caused by the transformation between real values and quantized values on the closed-loop system dynamics considering a dynamic output feedback controller is analyzed and conditions for the stability of the closed-loop system are derived.
- Post-quantum security: As a quantum computer may retrieve the secret key from the divisor in the modulo operation used in the encryption of the RHE scheme, the post-quantum secure resilient homomorphic encryption (PQS-RHE) scheme is proposed. The key idea to obtain the PQS-RHE scheme is twofold. First of all, the divisor in the modulo operations in the PQS-RHE scheme are selected differently from the RHE scheme so that retrieving the secret key from

the ciphertexts can not be achieved by modern cryptographic attacks even if a quantum computer is used. Secondly, in order to keep the homomorphic property, a decomposition technique is integrated into the evaluation process of the encrypted controller. After that it is proven that the PQS-RHE scheme can still neutralize the effect of an additive attack injected into the ciphertexts.

- Reduction of the network load: To reduce the network communication load in encrypted control systems, the RHE scheme is further developed by exploring the Chinese remainder theorem (CRT), which gives the multi-slot homomorphic encryption (MS-RHE). Due to the MS-RHE, multiple plaintexts can be encrypted into a single ciphertext. As the ciphertext in the MS-RHE scheme remains the same size as in the RHE scheme and the amount of ciphertexts transferred over the network is decreased, the network communication load is significantly reduced. It is proven that the MS-RHE scheme still keeps the ability of resilience and additive attacks injected into the ciphertexts can still be neutralized.
- Practical aspects of HE schemes: In order to give more insights into the RHE scheme, the PQS-RHE scheme and the MS-RHE scheme, a cloud-based control system encrypted by those encryption schemes is analyzed theoretically and practically. Moreover, a learning with errors (LWE)-based HE scheme will be considered in the practical investigation. The encryption schemes will be evaluated and compared in terms of requirement on network capacity, the usage of cloud storage and the execution time for evaluating the control law in ciphertexts, which play an important role for the practical applicability of the approaches.
- Attack detection: Since the resilience of the RHE scheme to additive attacks has still its limit, a detection approach is developed to give a twofold protection to cloud-based control systems encrypted by the RHE scheme. By exploiting the symmetric property of the inner product, two residual signals can be formulated. In case that the attack is inside of the resilience range, the first residual signal deviates from zero and a warning is generated. As soon as the attack is outside of the resilience range, the second residual signal deviates from zero and an alarm is triggered. That means, attacks can be prevented from breaking the resilience of the RHE scheme by using the proposed detection approach.

1.3 Organization

In Fig. 1.1, an overview of the dependencies and connections between the chapters is depicted. Chapter 2 gives the notations and the preliminary knowledge that will be used later. Moreover, the cloud-based control system and the case study investigated in this thesis to illustrate the proposed approaches are introduced. In Chapter 3, the vulnerability of the somewhat HE scheme to covert attacks will be investigated and the RHE scheme will be presented. After that it will be proven that the RHE

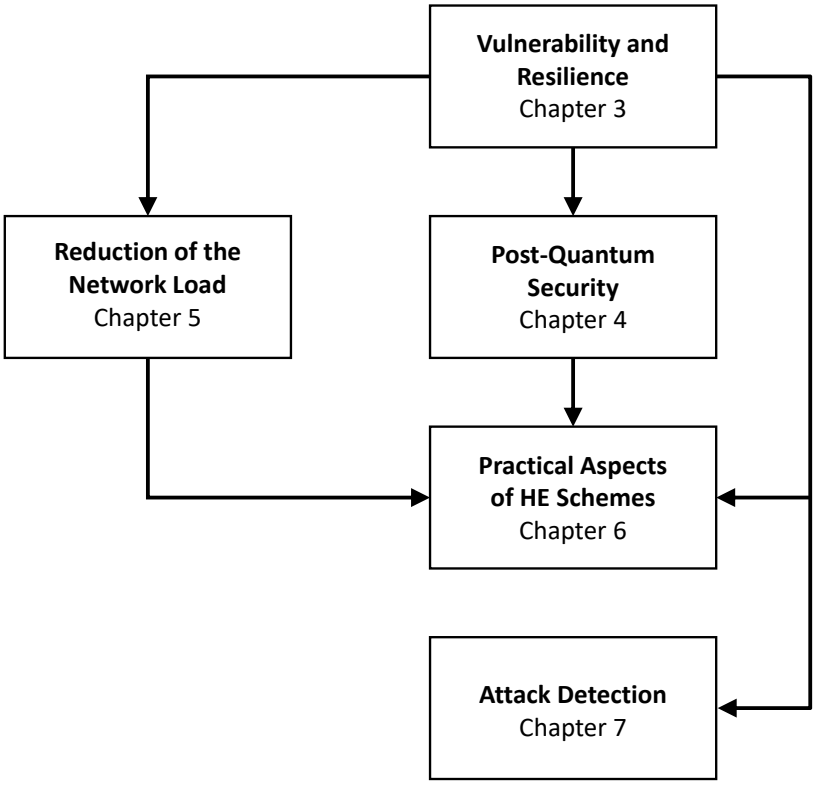

Figure 1.1: Overview of dependencies and connections between the chapters

scheme satisfies indistinguishability under chosen-plaintext attack (IND-CPA). Thus, an adversary can not gain any useful information from the ciphertexts generated by the RHE scheme. The mapping function applied to a control system and the quantization error are analyzed. Moreover, a condition for the stability of the closed-loop system will be derived. An example will be given to show the vulnerability of the somewhat HE scheme to covert attacks and the resilience of the RHE scheme to covert attacks. Chapter 4 introduces the PQS-RHE scheme that modifies the RHE scheme in a way that the ciphertexts generated by the PQS-RHE scheme and the divisor in the modulo operations used in the encryption resist attacks carried out by a quantum computer and thus the PQS-RHE scheme is post-quantum secure. Moreover, it will be proven that the PQS-RHE scheme keeps the ability of resilience. Finally, the main results are validated with a simulation example. Chapter 5 proposes the MS-RHE scheme to reduce the network communication load significantly in encrypted cloud-based control systems. For this purpose, the RHE scheme given in Chapter 3 will be further developed. An analysis shows that the MS-RHE scheme preserve the ability of resilience. Finally, an example will be given to illustrate the cloud-based control system encrypted by the MS-RHE scheme. In Chapter 6, the RHE scheme, the PQS-RHE scheme and the MS-RHE scheme will be analyzed theoretically and practically. In the practical analysis, a LWE-based HE scheme will be considered. The analysis taking into account the requirement on network capacity, usage of cloud storage and the execution time of the encrypted controller. In Chapter 7, a detection approach will be proposed that gives a twofold protection to cloud-based control

systems encrypted by the RHE scheme. A warning signal is triggered as soon as an attack is imposed on the ciphertexts, while an alarm signal is triggered when the attack affects the plaintext obtained after the decryption. Therefore, the RHE scheme can be combined with the proposed detection approach to ensure the integrity of the signals obtained after decryption in case of additive attacks. The thesis is concluded with a summary and an outlook in English, followed by an extended summary in German.

Some results presented in the chapters have been published previously by the author. In Appendix C, a review of the prior publications is provided. Appendix D includes a short CV of the author.

2 Preliminaries

In this section, the notations and some preliminary knowledge that will be used later are given.

2.1 Notations

The set of natural numbers, integers and real numbers are denoted, respectively, by $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$. Let $\lfloor\cdot\rfloor$, $\lceil\cdot\rfloor$ and $\lceil\cdot\rceil$ denote the floor operator, rounding operator and the ceiling operator, respectively. Vectors are denoted by lower-case bold letters (e.g. $\boldsymbol{f}$) and matrices are denoted by upper-case bold letters (e.g. $\boldsymbol{F}$). The maximal absolute value of the entries in a matrix $\boldsymbol{F} \in \mathbb{R}^{m\times n}$ and in a vector $\boldsymbol{f} \in \mathbb{R}^{n\times 1}$ are given, respectively, by the maximum norm $\|\boldsymbol{F}\|_{max} = \max_{i,j} |f_{ij}|$ and the infinity norm $\|\boldsymbol{f}\|_\infty = \max_j |f_j|$ (Liu and Yao, 2016). The 1-norm of a vector $\boldsymbol{f}$ is calculated by $\|\boldsymbol{f}\|_1 = \sum_{j=1}^{n} |f_j|$ and let $\|\boldsymbol{f}\|_2$ denote the Euclidean norm determined by $\|\boldsymbol{f}\|_2 = \sqrt{\sum_{j=1}^{n} f_j^2}$. Notice that $\|\boldsymbol{f}+\boldsymbol{w}\|_\infty \leq \|\boldsymbol{f}\|_\infty + \|\boldsymbol{w}\|_\infty$ and $\|\boldsymbol{F}\boldsymbol{w}\|_\infty \leq n\|\boldsymbol{F}\|_{max}\|\boldsymbol{w}\|_\infty$, where $\boldsymbol{w} \in \mathbb{R}^{n\times 1}$. Given two vectors $\boldsymbol{f} = [f_1 \cdots f_n]^T$ and $\boldsymbol{w} = [w_1 \cdots w_n]^T$, the Hadamard product of the vectors $\boldsymbol{f}$ and $\boldsymbol{w}$ is defined as $\boldsymbol{f} \circ \boldsymbol{w} = [f_1 w_1 \cdots f_n w_n]^T$. The Minkowski addition, denoted by $\oplus$, of two sets $\mathcal{F}, \mathcal{W} \subseteq \mathbb{R}$ are defined by $\mathcal{F} \oplus \mathcal{W} = \{f + w \mid f \in \mathcal{F}, w \in \mathcal{W}\}$. The sequence of sets $\mathcal{F}_k$ carried out by the Minkowski addition is denote by $\bigoplus_{k=1}^{K} \mathcal{F}_k = \mathcal{F}_1 \oplus \cdots \oplus \mathcal{F}_K$. The multiplication of a matrix $\boldsymbol{F}$ by a set $\mathcal{W}$ is denoted by $\boldsymbol{F}\mathcal{W} = \{\boldsymbol{F}w \mid w \in \mathcal{W}\}$. The jth entry in the lth vector $\boldsymbol{f}_l \in \mathbb{R}^{n\times 1}$ is denoted by $(f_l)_j$. The Kronecker product of two vectors $\boldsymbol{f}, \boldsymbol{w}$ is defined by $\boldsymbol{f} \otimes \boldsymbol{w} = [f_1\boldsymbol{w}^T \cdots f_n\boldsymbol{w}^T]^T$ (Liu and Yao, 2016). A negligible function, denoted by $\text{negl}(\mu)$, is a function that decreases faster than μ^{-c} for any constant $c > 0$ (Katz and Lindell, 2020).

2.2 System description

The structure under consideration consists of a plant (including sensors and actuators), a controller located in a cloud hosted by a third party that is connected with the plant over a network and a monitoring system to observe the plant behaviour as shown in Fig. 2.1.

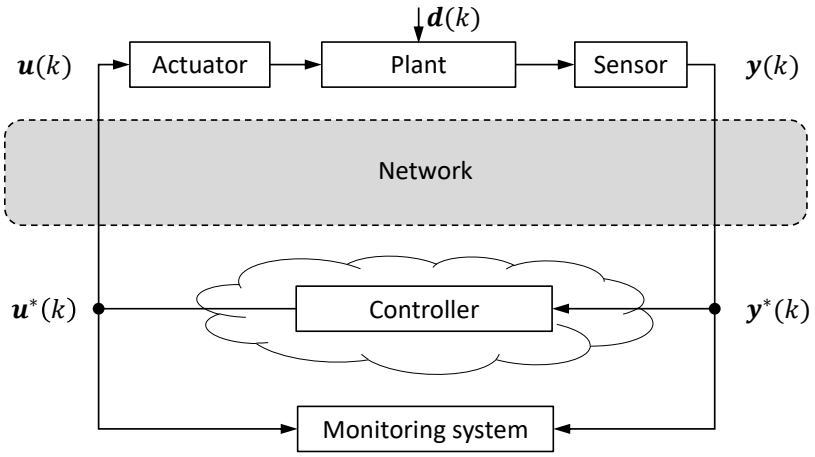

Figure 2.1: Cloud-based control system

The plant is a discrete linear time-invariant (LTI) process described by

$$\begin{aligned} \boldsymbol{x}(k+1) &= \boldsymbol{A}\boldsymbol{x}(k) + \boldsymbol{B}\boldsymbol{u}(k) + \boldsymbol{E}_d\boldsymbol{d}(k) \\ \boldsymbol{y}(k) &= \boldsymbol{C}\boldsymbol{x}(k) + \boldsymbol{D}\boldsymbol{u}(k) + \boldsymbol{F}_d\boldsymbol{d}(k) \end{aligned} \tag{2.1}$$

where $\boldsymbol{x}(k) \in \mathbb{R}^{n_x}$ is the state vector, $\boldsymbol{u}(k) \in \mathbb{R}^m$ is the control input vector, $\boldsymbol{y}(k) \in \mathbb{R}^{b_y}$ is the measured output vector, $\boldsymbol{d}(k) \in \mathbb{R}^{m_d}$ is the unknown disturbance vector, $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{E}_d$ and $\boldsymbol{F}_d$ are matrices of compatible dimensions.

Assume that the plant in (2.1) communicates over the network with a dynamic output feedback controller described by

$$\begin{aligned} \boldsymbol{x}_s(k+1) &= \boldsymbol{A}_s\boldsymbol{x}_s(k) + \boldsymbol{B}_s\boldsymbol{y}^*(k) \\ \boldsymbol{u}^*(k) &= \boldsymbol{C}_s\boldsymbol{x}_s(k) + \boldsymbol{D}_s\boldsymbol{y}^*(k) \end{aligned} \tag{2.2}$$

where $\boldsymbol{x}_s(k) \in \mathbb{R}^{n_s}$ is the state vector of the controller, $\boldsymbol{u}^*(k) \in \mathbb{R}^m$ is the generated control input vector, $\boldsymbol{y}^*(k) \in \mathbb{R}^{b_y}$ is the received output vector, $\boldsymbol{A}_s$, $\boldsymbol{B}_s$, $\boldsymbol{C}_s$ and $\boldsymbol{D}_s$ are matrices of appropriate dimensions. The controller (2.2) can be equivalently rewritten as

$$\begin{bmatrix} \boldsymbol{x}_s(k+1) \\ \boldsymbol{u}^*(k) \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_s & \boldsymbol{B}_s \\ \boldsymbol{C}_s & \boldsymbol{D}_s \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_s(k) \\ \boldsymbol{y}^*(k) \end{bmatrix} = \boldsymbol{T}\boldsymbol{g}(k), \tag{2.3}$$

where $\boldsymbol{T} \in \mathbb{R}^{\alpha\times\beta}$, $\boldsymbol{g}(k) \in \mathbb{R}^{\beta\times 1}$, $\alpha = n_s + m$ and $\beta = n_s + b_y$.

Assumption 1. *Throughout this thesis, we assume that the controller* (2.2) *guarantee the stability of the closed-loop system.*

Assume that an observer-based fault detection system is used to monitor the cloud-based control system and the residual signal is generated by

$$\begin{aligned} \hat{\boldsymbol{x}}(k+1) &= \boldsymbol{A}\hat{\boldsymbol{x}}(k) + \boldsymbol{B}\boldsymbol{u}^*(k) + \boldsymbol{L}\big(\boldsymbol{y}^*(k) - \hat{\boldsymbol{y}}(k)\big) \\ \hat{\boldsymbol{y}}(k) &= \boldsymbol{C}\hat{\boldsymbol{x}}(k) + \boldsymbol{D}\boldsymbol{u}^*(k) \end{aligned}$$

$$\boldsymbol{r}(k) = \boldsymbol{W}\big(\boldsymbol{y}^*(k) - \hat{\boldsymbol{y}}(k)\big) \tag{2.4}$$

where $\hat{\boldsymbol{x}}(k) \in \mathbb{R}^{n_s}$ is the estimated state vector, $\hat{\boldsymbol{y}}(k) \in \mathbb{R}^{b_y}$ is the estimated output vector, $\boldsymbol{r}(k) \in \mathbb{R}^{n_r}$ is the residual vector, $\boldsymbol{L}$ and $\boldsymbol{W}$ are matrices of appropriate dimensions. An alarm is triggered based on the following decision logic

$$\begin{cases} \|\boldsymbol{r}\|_2 \leq \delta_r \Rightarrow \textit{nominal} \\ \|\boldsymbol{r}\|_2 > \delta_r \Rightarrow \textit{attacked}, \end{cases} \tag{2.5}$$

where the threshold δ_r is selected based on the disturbances in the plant (2.1).

2.3 Case study: Quadruple-tank system

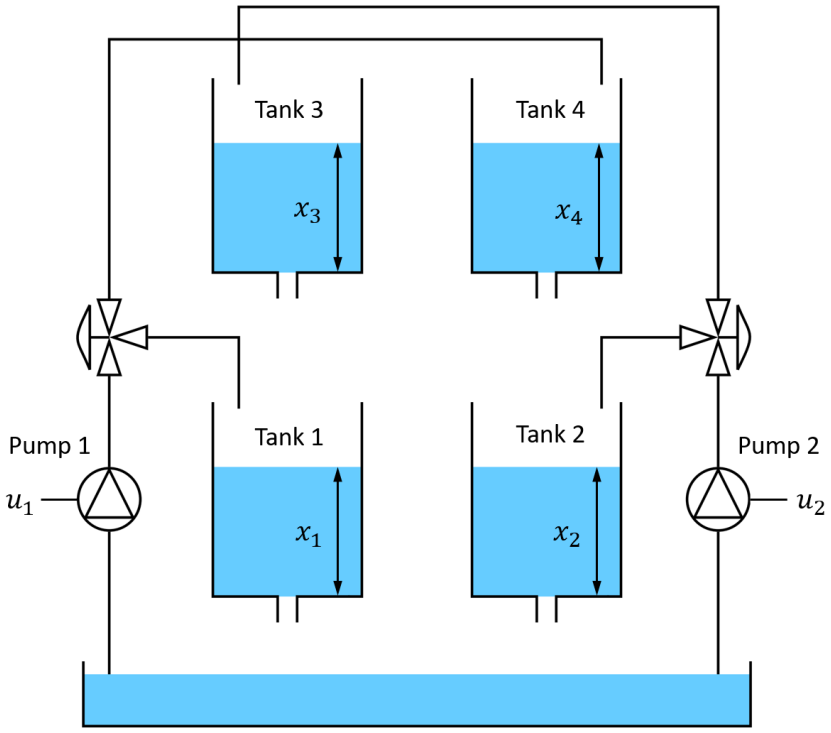

Figure 2.2: Quadruple-tank system according to Johansson (2000)

The proposed approaches are demonstrated with the help of the quadruple-tank system given in Johansson (2000), which is a well-established benchmark for the study of cyber security (Teixeira et al., 2012; Kim et al., 2016; Romagnoli et al., 2019). The nonlinear continuous-time plant model given by Johansson (2000) is linearized at the working point $\boldsymbol{x} = [x_1 \;\; x_2 \;\; x_3 \;\; x_4]^T = [12.6 \;\; 13 \;\; 4.8 \;\; 4.9]^T cm$. The states $\boldsymbol{x}(k)$ in the model are the liquid levels in the tanks, the control inputs $\boldsymbol{u}(k) = [u_1(k) \;\; u_2(k)]^T$ are the pressure in the pumps. The sampling time is $T = 1$ second. The plant is

described by (2.1) with

$$\boldsymbol{A} = \begin{bmatrix} 0.9843 & 0 & 0.0251 & 0 \\ 0 & 0.9891 & 0 & 0.0176 \\ 0 & 0 & 0.9747 & 0 \\ 0 & 0 & 0 & 0.9823 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 0.0478 & 0.0010 \\ 0.0005 & 0.0348 \\ 0 & 0.0776 \\ 0.0554 & 0 \end{bmatrix}$$

$$\boldsymbol{C} = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{bmatrix}, \boldsymbol{D} = \boldsymbol{O}, \boldsymbol{E}_d = \begin{bmatrix} \boldsymbol{B} & \boldsymbol{O} \end{bmatrix}, \boldsymbol{F}_d = \begin{bmatrix} \boldsymbol{O} & \boldsymbol{I} \end{bmatrix} \tag{2.6}$$

where the matrix $\boldsymbol{I}$ and the matrix $\boldsymbol{O}$ denote, respectively, an identity matrix and a zero matrix of compatible dimensions.

To stabilize the system, the parameters of the controller (2.3) are selected as

$$\begin{aligned} \boldsymbol{A}_s &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \ \boldsymbol{B}_s = \begin{bmatrix} -0.0625 & 0 \\ 0 & -0.01563 \end{bmatrix} \\ \boldsymbol{C}_s &= \begin{bmatrix} -0.032 & 0 \\ 0 & 0.0192 \end{bmatrix}, \ \boldsymbol{D}_s = \begin{bmatrix} -1 & 0 \\ 0 & 0.3 \end{bmatrix} \end{aligned} \tag{2.7}$$

The observer gain $\boldsymbol{L}$ and the weighting matrix $\boldsymbol{W}$ are selected with the well-established unified approach given by Ding (2013) as

$$\boldsymbol{L} = \begin{bmatrix} 0.0262 & 0.0006 \\ 0.0006 & 0.0195 \\ 0.0126 & 0.0297 \\ 0.0293 & 0.0090 \end{bmatrix}, \boldsymbol{W} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.8}$$

The disturbances $\boldsymbol{d}(k)$ are random variables normally distributed with the mean value $\varphi = 0$ and the standard deviation $\sigma = 0.001$, which leads to the threshold $\delta_r = 0.03$.

2.4 A stealthy cyber attack on cloud-based control systems

In this section, the cloud-based control system under a cyber attack will be introduced. Moreover, it will be shown how a cyber attack remains stealthy in the cloud-based control system even if a classical monitoring system is used.

2.4.1 Cloud-based control system under attack

In Fig. 2.3, a cloud-based control system under a cyber attack is shown. The attack signals imposed on the measured output signals $\boldsymbol{y}(k)$ and the control input signals $\boldsymbol{u}^*(k)$ are denoted, respectively, by $\boldsymbol{a}_1(k) \in \mathbb{R}^{b_y}$ and $\boldsymbol{a}_2(k) \in \mathbb{R}^m$. After the attack signals $\boldsymbol{a}_1(k), \boldsymbol{a}_2(k)$ are injected into the network, there is

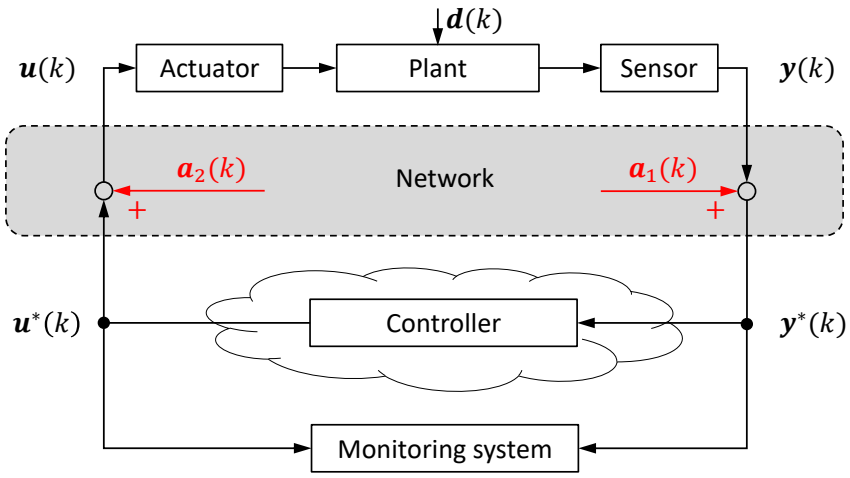

Figure 2.3: Cloud-based control system under cyber attack

$$\begin{aligned} \boldsymbol{y}^*(k) &= \boldsymbol{y}(k) + \boldsymbol{a}_1(k) \\ \boldsymbol{u}(k) &= \boldsymbol{u}^*(k) + \boldsymbol{a}_2(k) \end{aligned} \tag{2.9}$$

If there is no cyber attack, then $\boldsymbol{u}(k) = \boldsymbol{u}^*(k)$ and $\boldsymbol{y}(k) = \boldsymbol{y}^*(k)$.

2.4.2 Covert attack

The covert attack has been firstly introduced by Smith (2011). As the covert attack can be imposed on a cloud-based control system without being detected by a conventional monitoring system, the covert attack is a serious threat for cloud-based control systems.

To impose a covert attack on a cloud-based control system, it is required that the adversary has writing access to all the control input signals and sensor output signals and also good knowledge of the plant model. The additive attack signal $\boldsymbol{a}_2(k)$ on the control input signals $\boldsymbol{u}^*(k)$ is designed by the adversary to bring the plant to some predefined state. The additive attack $\boldsymbol{a}_1(k)$ on the sensor output signals $\boldsymbol{y}(k)$ is used to compensate the influence of $\boldsymbol{a}_2(k)$ on the sensor output signals $\boldsymbol{y}(k)$.

Let $\boldsymbol{A}_1(z), \boldsymbol{A}_2(z), \boldsymbol{U}(z)$ and $\boldsymbol{Y}(z)$ denote, respectively, the z-transform of $\boldsymbol{a}_1(k)$, $\boldsymbol{a}_2(k)$, $\boldsymbol{u}(k)$ and $\boldsymbol{y}(k)$. The attack signal $\boldsymbol{a}_1$ is selected according to

$$\boldsymbol{A}_1(z) = -\boldsymbol{G}(z)\boldsymbol{A}_2(z), \tag{2.10}$$

where $\boldsymbol{G}(z) = \boldsymbol{D} + \boldsymbol{C}(z\boldsymbol{I} - \boldsymbol{A})^{-1}\boldsymbol{B}$. Then there is

$$\begin{aligned} \boldsymbol{Y}^*(z) &= \boldsymbol{G}(z)(\boldsymbol{U}(z) + \boldsymbol{A}_2(z)) - \boldsymbol{G}(z)\boldsymbol{A}_2(z) \\ &= \boldsymbol{G}(z)\boldsymbol{U}(z). \end{aligned} \tag{2.11}$$

That means, if the adversary has comprehensive knowledge of the system dynamics $\boldsymbol{G}(z)$, he is able to cancel the influence of the attack $\boldsymbol{a}_2(k)$ on the sensor output signals $\boldsymbol{y}^*(k)$ completely. Therefore, the sensor output signals $\boldsymbol{y}^*(k)$ received by the monitoring system do not contain any information about the attack $\boldsymbol{a}_2(k)$.

2.5 Indistinguishability under chosen-plaintext attack

The indistinguishability under chosen-plaintext attack (IND-CPA) is a default requirement on modern encryption schemes (Katz and Lindell, 2020). Assume that two plaintexts are chosen by an adversary whereby one plaintext will be encrypted and the corresponding ciphertext is available to the adversary. The encryption of the plaintext is carried out randomly, i.e. the adversary does not know which plaintext has been encrypted. An encryption scheme satisfies IND-CPA, if the adversary is not able to distinguish which plaintext has been encrypted. Commonly, the so-called CPA experiment has been exploited to prove that an encryption scheme satisfies IND-CPA, as given below (Katz and Lindell, 2020).

We denote by $\text{IND-CPA}_{\mathcal{A},\mathcal{E}}(\kappa)$ the CPA experiment of the encryption scheme $\mathcal{E} = (KeyGen, Enc, Dec)$ using the security level κ and by $\mathcal{A}$ the adversary who tries to win the CPA experiment. Usually the running time of algorithms employed in encryption schemes is mainly decided by the security level κ in unary representation (i.e. as a string of ones denoted by 1^κ) (Katz and Lindell, 2020). The CPA experiment can be carried out in three steps.

1. A secret key sk is generated by the key generation function $KeyGen(1^\kappa)$ using the security level κ. An integer v is randomly chosen from the set $\{0, 1\}$.
2. The adversary $\mathcal{A}$ chooses a pair of plaintexts $w_i \in \mathcal{M}$, where $i \in \{0, 1\}$ and $\mathcal{M}$ denotes the plaintext space supported by $\mathcal{E}$. Then, the ciphertext $c = Enc(w_v, sk)$ is returned to the adversary $\mathcal{A}$, where v is randomly selected so that the adversary does not know whether w_1 or w_2 is now encrypted.
3. The adversary $\mathcal{A}$ outputs an integer v' from the set $\{0, 1\}$, i.e. the adversary guesses which plaintext w_v has been encrypted by the encryption function $Enc(w_v, sk)$. If $v' = v$, then the adversary $\mathcal{A}$ wins the CPA experiment which is denoted by $\text{IND-CPA}_{\mathcal{A},\mathcal{E}}(\kappa) = 1$.

An encryption scheme $\mathcal{E}$ satisfies IND-CPA, if the success for any adversary $\mathcal{A}$ to win the CPA experiment and guess correctly whether w_1 or w_2 has been encrypted is negligibly better than $1/2$, which is denoted by

$$\Pr[\text{IND-CPA}_{\mathcal{A},\mathcal{E}}(\kappa) = 1] = \frac{1}{2} + negl(\kappa) \tag{2.12}$$

where $negl(\kappa)$ is the negligible function. According to Katz and Lindell (2020), an encryption scheme that satisfies IND-CPA is also resilient to known plaintext attacks (KPA).

2.6 Chinese remainder theorem

To encrypt multiple plaintexts into a single ciphertext, the Chinese remainder theorem (CRT) plays an important role. It builds the basis of the MS-RHE developed in Chapter 5.

Definition 1 (Chinese remainder theorem (CRT) (Cormen et al., 2001)). *Let $p_1, \cdots, p_\tau$ be pairwise co-prime integers, i.e. the greatest common divisor (GCD) of the pairs (p_i, p_j) satisfies $gcd(p_i, p_j) = 1$, $\forall i, j$, where $i \neq j$, $i, j = 1, 2, \cdots, \tau$ and $\tau \in \mathbb{N}\backslash\{0\}$. Assume that $s_j \in \{0, 1, \cdots, p_j - 1\}$, $j = 1, \cdots, \tau$, are predefined integers. Then, an integer $x \in [0, \pi_\tau)$ with $\pi_\tau = \prod_{j=1}^{\tau} p_j$ can be calculated such that*

$$x \ mod \ p_1 = s_1, \ \cdots, \ x \ mod \ p_\tau = s_\tau \tag{2.13}$$

The integer x that satisfies (2.13) is denoted by $x = \underset{p_1,\cdots,p_\tau}{CRT}(s_1, \cdots, s_\tau)$.

Note that the integer $x = \text{CRT}_{p_1,\cdots,p_\tau}(s_1, \cdots, s_\tau)$ can be calculated with the algorithms given by Pei et al. (1996). If $p_1, \cdots, p_\tau$ are all prime numbers, then they are also pairwise co-prime integers.

2.7 Approximate greatest common divisor problem

In the last decade, the approximate greatest common divisor (AGCD) distribution has been exploited to obtain HE schemes that are secure against modern cryptographic attacks (Van Dijk et al., 2010; Coron et al., 2014; Lepoint, 2014; Cheon et al., 2015; Benarroch et al., 2017; Pereira, 2021). In this section, the AGCD distribution and several variants of the AGCD problem are introduced, which are building the base of the RHE scheme in Chapter 3, the PQS-RHE scheme in Chapter 4 and the MS-RHE scheme in Chapter 5.

Definition 2 (Approximate greatest common divisor (AGCD) distribution (Lepoint, 2014)). *Let ρ, ψ and γ be integers, $0 < \rho < \psi < \gamma$, p is a ψ-bit prime number and q is an integer uniformly chosen from the interval $[0, \lfloor 2^\gamma / p \rfloor]$. The random variable $z = s + rp$ has the AGCD distribution denoted by $\mathcal{D}_{\gamma,\rho}(q, p)$, where s and r are independent random integers uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, q - 1]$.*

Definition 3 (Error-free approximate greatest common divisor (EF-AGCD) problem (Coron et al., 2011)). *Let ρ, ψ and γ be integers, $0 < \rho < \psi < \gamma$, $z_0 = qp$, where p is a ψ-bit prime number and $q \in \{0, 1, \cdots, \lfloor 2^\gamma / p \rfloor\}$ is an integer that can not be factorized into integers smaller than 2^ψ. Assume that N is a large integer value. The EF-AGCD problem is the problem to compute p while having access to z_0 and N independent samples z_i, $i = 1, 2, \cdots, N$, drawn from the distribution $\mathcal{D}_{\gamma,\rho}(q, p)$ given in Definition 2.*

Definition 4 (Decisional EF-AGCD problem (Lepoint, 2014)). *Let the random variable u be an integer from the interval $[0, 2^\gamma - 1]$ and have the uniform distribution $\mathcal{U}_\gamma$. Assume that N is a large integer value. The decisional EF-AGCD problem is the problem of distinguishing between the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ given in Definition 2 and the uniform distribution $\mathcal{U}_\gamma$ while having access to z_0, N independent samples z_i, $i = 1, 2, \cdots, N$, drawn from the distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ and N independent samples u_i, $i = 1, 2, \cdots, N$, drawn from the uniform distribution $\mathcal{U}_\gamma$.*

Until now, there is no probabilistic polynomial time (PPT) algorithm that is able to distinguish between the uniform distribution $\mathcal{U}_\gamma$ and the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ (Lepoint, 2014; Cheon and Stehlé, 2015; Benarroch et al., 2017; Pereira, 2021). Thus, a HE scheme constructed based on the EF-AGCD problem can generate ciphertexts that are computationally indistinguishable from uniformly distributed integers so that the HE scheme satisfies IND-CPA.

Definition 5 (Decisional AGCD problem). *Let the random variable u be an integer from the interval $[0, 2^\gamma - 1]$ and have the uniform distribution $\mathcal{U}_\gamma$. Assume that N is a large integer value. The decisional AGCD problem is the problem of distinguishing between the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ given in Definition 2 and the uniform distribution $\mathcal{U}_\gamma$ while having access to N independent samples z_i, $i = 1, 2, \cdots, N$, drawn from the distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ and N independent samples u_i, $i = 1, 2, \cdots, N$, drawn from the uniform distribution $\mathcal{U}_\gamma$.*

Since the decisional AGCD problem remains hard to solve even if quantum computers become reality (Cheon and Stehlé, 2015; Benarroch et al., 2017; Pereira, 2020; Cominetti and Simplicio, 2020), an HE scheme which is based on the decisional AGCD problem can be regarded as quantum secure.

For the selection of the parameters in the MS-RHE scheme, the batched approximate greatest common divisor (AGCD) distribution will be used later.

Definition 6 (Batched AGCD distribution (Benarroch et al., 2017)). *Let τ, ρ, ψ, γ be integers, $p_1, \cdots, p_\tau$ be prime numbers of bit-size ψ, $\pi_\tau = \prod_{j=1}^{\tau} p_j$, $0 < \rho < \psi < \gamma$. The random variable $z = s + r\pi_\tau$ has the batched AGCD distribution $\mathcal{D}'_{\gamma,\rho}(q,\pi_\tau)$, where $s = \underset{p_1,\cdots,p_\tau}{CRT}(s_1, \cdots, s_\tau)$, each integer s_j and the integer r are independent random variables uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, \lfloor 2^\gamma/\pi_\tau \rfloor]$, $j = 1, 2, \cdots, \tau$.*

3 Vulnerability and Resilience of Homomorphic Encryption Schemes

In this chapter, the vulnerability of cloud-based control systems encrypted by homomorphic encryption (HE) schemes to sophisticated cyber attacks, such as the covert attacks, will be studied. To cope with this vulnerability, the resilient homomorphic encryption (RHE) scheme will be proposed. The RHE scheme is able to not only neutralize the effect of additive attacks injected into the ciphertexts but also satisfy the security requirement of IND-CPA.

HE schemes have received much attention in the control community recently, because they can not only ensure the confidentiality of data sent over the network, but they also enable arithmetic operations on ciphertexts (Kogiso and Fujita, 2015; Darup et al., 2021). Thus, a HE scheme can be employed to realize an encrypted controller in a cloud provided by a third party and meet the requirement for confidentiality. In the pioneering work of Kogiso and Fujita (2015), the Rivest-Shamir-Adleman (RSA) cryptosystem (Rivest et al., 1978) and the ElGamal cryptosystem (Elgamal, 1985) have been used to carry out the multiplications needed in a dynamic output feedback controller based on ciphertexts. Since then, various applications have been encrypted by partially homomorphic encryption (PHE) schemes, including state feedback controller, dynamic feedback controller, model predictive control (MPC), quadratic programming and average consensus (Shoukry et al., 2016; Farokhi et al., 2016; Kishida, 2018; Cheon et al., 2018; Darup et al., 2018; Alexandru et al., 2018; Ruan et al., 2019). However, PHE schemes only support encrypted addition or encrypted multiplication and thus complex computations can only be partially outsourced to a third party without compromising the security. The fully homomorphic encryption (FHE) schemes can be realized by making use of the bootstrapping technique firstly developed by Gentry (2009), so that an infinite number of additions and multiplications can be carried out based on ciphertexts. However, bootstrapping is computationally expensive. To cope with it, in Kim et al. (2016) three controllers are used in parallel to bridge the waiting time when the ciphertexts at the controller side are bootstrapped. Evaluating three controllers simultaneously heavily increases the computational load. Therefore, leveled HE schemes (Fan and Vercauteren, 2012; Gentry et al., 2013; Cheon et al., 2017) and somewhat HE schemes (Dyer et al., 2019) have attracted much attention most recently (see, for instance, Fritz et al. (2019), Alexandru et al. (2020), Teranishi et al. (2020), Suh and Tanaka (2021), Schlüter et al. (2021), Kosieradzki et al. (2022), Kim et al. (2023), and Teranishi et al. (2023)).

Different from PHE schemes, leveled HE schemes and somewhat HE schemes can support a limited number of both encrypted addition and encrypted multiplication, which bring much improvements in terms of outsourcing control laws completely to a cloud hosted by a third party and protecting confidential data. The so-called Cheon-Kim-Kim-Song (CKKS) cryptosystem given by Cheon et al. (2017) is used in Alexandru et al. (2020) to implement a data-driven linear quadratic regulator and in Suh and Tanaka (2021) to implement reinforcement learning algorithms. In Kim et al. (2023), the Gentry-Sahai-Waters (GSW) cryptosystem given by Gentry et al. (2013) is used to encrypt a dynamic output feedback controller. To avoid the decryption of the controller state at the plant side, the pole placement technique is used to transform all the entries of the state matrix of the controller into integers. Two other approaches that address the challenge of decrypting the controller state at the plant side have been developed by Schlüter et al. (2021) and Teranishi et al. (2023). In Schlüter et al. (2021), the dynamic output feedback controller is approximated by a finite impulse response (FIR) filter. In Teranishi et al. (2023), a dynamic output feedback controller is transformed into the form of an input-output history feedback controller (IOHFC). Based on that, the Brakerski/Fan-Vercauteren (BFV) cryptosystem given by Fan and Vercauteren (2012) is applied to carry out encrypted calculation. The somewhat HE scheme given by Dyer et al. (2019) is applied, respectively, in Fritz et al. (2019) to encrypt logic controllers widely existing in industrial practice and in Teranishi et al. (2020) to encrypt a nonlinear controller based on feedback linearization. In Kosieradzki et al. (2022), both the BFV cryptosystem given by Fan and Vercauteren (2012) and the somewhat HE scheme given by Dyer et al. (2019) have been used to encrypt a bilateral teleoperation control system with nonlinear friction compensation.

Although the vulnerability of cloud-based control systems regarding confidentiality of the signals can be tackled by making use of above mentioned HE schemes, the availability of the signals has not received much attention. Since a malicious adversary can still tamper the ciphertexts involved in a cloud-based control system, the signals needed by the controller and the actuators may become unavailable when needed. This issue can be addressed by achieving resilience in cloud-based control systems so that an acceptable level of service can be maintained even if an attack takes place in the control system. Therefore, it is beneficial to achieve resilience in encrypted control to ensure both the confidentiality and the availability of the sensor signals and the control input signals.

In this chapter, the vulnerability of encrypted cloud-based control system to sophisticated cyber attacks, such as covert attacks, will be studied by exploring the somewhat HE scheme given by Dyer et al. (2019). To cope with this vulnerability, the RHE scheme will be proposed. Compared with the existing HE schemes, the RHE scheme can cancel the influence of an additive attack out of the control system so that the controller can get the true sensor information and the actuators can get the true control input signals even in case of an attack. To satisfy the security requirement of IND-CPA with the RHE scheme, the divisor in the modulo operations and the noises in the encryption scheme are chosen from the approximate greatest common divisor (AGCD) distribution. It can be shown that retrieving the secret key from the ciphertexts generated by the RHE scheme is indeed an error-free approximate great-

est common divisor (EF-AGCD) problem. Due to the hardness of the EF-AGCD problem (Coron et al., 2011; Lepoint, 2014), it can be proven that the RHE scheme satisfies IND-CPA. After that, the cryptographic attacks against the RHE scheme are analyzed to find the constraints on the parameters in the RHE scheme. Based on it, a systematic procedure to select the parameters in the RHE scheme will be given to guarantee the desired security level.

The chapter is organized as follows. The somewhat HE scheme given by Dyer et al. (2019) is shown in Section 3.1. In Section 3.2, the vulnerability of the somewhat HE scheme given by Dyer et al. (2019) to additive attacks is analyzed. The RHE scheme is presented in Section 3.3. In Section 3.4, the resilience of the RHE scheme to additive attacks is analyzed. The security analysis and the parameter selection of the RHE scheme is given in Section 3.5. The quantization error that occurs in the encrypted cloud-based control system is analyzed in Section 3.6. Finally, an example of the well-established quadruple-tank system is given in Section 3.7 to show the vulnerability of the somewhat HE scheme given by Dyer et al. (2019) to additive attacks and the resilience of the proposed RHE scheme to additive attacks.

3.1 Somewhat homomorphic encryption

In this section, the somewhat HE scheme given by Dyer et al. (2019) is introduced to study the vulnerability of homomorphic encryption schemes against sophisticated cyber attacks like covert attacks.

The somewhat HE scheme given by Dyer et al. (2019) is a symmetric encryption scheme and uses the same secret key for both encryption and decryption. The somewhat HE scheme consists of four functions $\mathcal{E} = (KeyGen,\ Enc,\ Dec,\ Eval)$.

Let $\eta_1, \eta_2, \cdots, \eta_n$ be positive integer plaintexts that belong to the set $\{0, 1, \cdots, M\}$ and d is the degree of the polynomial that will be encrypted by the somewhat HE scheme (Dyer et al., 2019).

Key Generation ($KeyGen$): Choose the security parameter κ. According to Dyer et al. (2019), select a ψ-bit prime number p and a ψ'-bit prime number q in such a way that an adversary can not factorise pq to get the prime numbers p, q in polynomial time. In order to decrypt later correctly, it is required that $(n+1)^d M^d < \theta$ and $(n+1)^d(M+\theta^2)^d < p$, where θ is an integer. Finally, let $z_0 = qp$ be the devisor in the modulo operations and $sk = (\theta, p)$ is the secret key for encryption and decryption.

Encryption (Enc): A plaintext $\eta \in \{0, 1, \cdots, M\}$ is encrypted by

$$\begin{aligned} c = Enc(\eta, sk) &= (\eta + s\theta + rp) \bmod qp \\ &= (\eta + s\theta + rp) \bmod z_0 \end{aligned} \tag{3.1}$$

where the noise s is an integer uniformly selected from $\{0, 1, \cdots, \theta - 1\}$ and the noise r is an integer uniformly chosen from $\{1, 2, \cdots, q-1\}$.

Decryption (Dec): The decryption of an encrypted plaintext $c \in \mathbb{N}$ is given by

$$Dec(c, sk) = (c \bmod p) \bmod \theta \tag{3.2}$$

Evaluation ($Eval$): The addition of the ciphertext $c_1 = (\eta_1 + s_1\theta + r_1 p) \bmod z_0$ and the ciphertext $c_2 = (\eta_2 + s_2\theta + r_2 p) \bmod z_0$ is

$$c_{Add} = Add(c_1, c_2) = (c_1 + c_2) \bmod z_0 \tag{3.3}$$

whose decryption is equal to $\eta_1 + \eta_2$. The multiplication of the ciphertext c_1 and the ciphertext c_2 is

$$c_{Mult} = Mult(c_1, c_2) = (c_1 c_2) \bmod z_0 \tag{3.4}$$

whose decryption is equal to $\eta_1 \eta_2$.

As the dynamic output feedback controller (2.3) is in the form of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$, it will be shown how the encryption, decryption and evaluation function of the somewhat HE scheme given by Dyer et al. (2019) can be adapted to obtain the true result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ after the decryption.

Encryption (Enc): A matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha \times \beta}$ is encrypted by

$$\boldsymbol{F}_r = Enc(\boldsymbol{F}, sk) = (\boldsymbol{F} + \boldsymbol{S}_r\theta + \boldsymbol{R}_r p) \bmod z_0 \tag{3.5}$$

and a vector $\boldsymbol{w} \in \mathbb{N}^{\beta \times 1}$ is encrypted by

$$\boldsymbol{w}_r = Enc(\boldsymbol{w}, sk) = (\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \bmod z_0 \tag{3.6}$$

where all the entries f_{ij} and w_j in, respectively, $\boldsymbol{F}$ and $\boldsymbol{w}$ belong to the set $\{0, 1, \cdots, M\}$, the noises s_{ij}, s_j are uniformly selected from the set $\{0, 1, \cdots, \theta-1\}$, the integers r_{ij}, r_j are uniformly chosen from the set $\{1, 2, \cdots, q-1\}$, $i = 1, 2, \cdots, \alpha$ and $j = 1, 2, \cdots, \beta$.

Decryption (Dec): The decryption of an encrypted vector $\boldsymbol{c}_r \in \mathbb{N}^{\alpha \times 1}$ is given by

$$\boldsymbol{\nu}_r = Dec(\boldsymbol{c}_r, sk) = (\boldsymbol{c}_r \bmod p) \bmod \theta \tag{3.7}$$

Evaluation ($Eval$): The matrix-vector product of the encrypted matrix $\boldsymbol{F}_r$ and the encrypted vector $\boldsymbol{w}_r$ is

$$\boldsymbol{c}_r = (\boldsymbol{F}_r \boldsymbol{w}_r) \bmod z_0 \tag{3.8}$$

Now, a sufficient condition for the correct decryption is given to guarantee that the somewhat HE scheme delivers the correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ after the decryption (3.7).

As each entry v_i^* of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ is obtained by

$$v_i^* = \sum_{j=1}^{\beta} F_{ij} w_j \tag{3.9}$$

where F_{ij} denotes the entry in the i-th row and the j-th column of the matrix $\boldsymbol{F}$ and w_j denotes the j-th entry in the column vector $\boldsymbol{w}$. The degree d of the polynomial $F_{ij}w_j$ (3.9) is $d = 2$. Moreover, the number n of plaintexts that will be encrypted by (3.5)-(3.6) to obtain v_i^* (3.9) is $n = 2\beta$. Thus, the decryption of $\boldsymbol{c}_r$ by (3.7) is equal to $\boldsymbol{Fw}$, if

$$(2\beta + 1)^2 M^2 < \theta \tag{3.10a}$$

$$(2\beta + 1)^2 (M + \theta^2)^2 < p \tag{3.10b}$$

3.1.1 Mapping function

The somewhat HE scheme given by Dyer et al. (2019) allows only positive integer plaintexts from the set $\{0, 1, \cdots, M\}$. However, the signals in a cloud-based control system take often real values. Therefore, it is necessary to transform real values into positive integer values.

Let $\lambda_1, \lambda_2 \in \mathbb{N}$ represent the range and the resolution of the quantization. Then negative and positive numbers $\zeta \in [-2^{\lambda_1}, 2^{\lambda_1})$ can be mapped into the set $\mathcal{Q} = \{-2^{\lambda_1}, -2^{\lambda_1} + 2^{-\lambda_2}, \cdots, 2^{\lambda_1} - 2^{-\lambda_2}\}$ by the following quantization function

$$Q(\zeta) = \begin{cases} \max\{\overline{\zeta} \in \mathcal{Q} | \overline{\zeta} \leq \zeta\}, \text{ if } \zeta \geq 0 \\ \min\{\overline{\zeta} \in \mathcal{Q} | \overline{\zeta} \geq \zeta\}, \text{ if } \zeta < 0 \end{cases} \tag{3.11}$$

Let $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1} + 1$ and the bound M of the plaintexts is $M = 2^{\lambda_1+\lambda_2+1}$. The quantized value $\overline{\zeta}$ can be mapped to an integer by

$$\Gamma(\overline{\zeta}) = 2^{\lambda_2}\overline{\zeta} \bmod \mu \tag{3.12}$$

It will later turn out to be useful that we have two different inverse mapping functions. The first mapping function $\Gamma^{-1}(\eta)$ delivers the quantized value $\overline{\eta}$ that corresponds to an integer η obtained after the matrix-vector product. There is

$$\Gamma^{-1}(\eta) = \begin{cases} \frac{1}{2^{2\lambda_2}}(\eta \bmod \mu - \mu), & \text{if } \eta \bmod \mu > \mu/2 \\ \frac{1}{2^{2\lambda_2}}(\eta \bmod \mu), & \text{if } \eta \bmod \mu \leq \mu/2 \end{cases} \tag{3.13}$$

The second mapping function $\overline{\Gamma}^{-1}(\eta')$ produces the quantized value $\overline{\eta}'$, corresponding to an integer η' that was not used in a multiplication. There is

$$\overline{\Gamma}^{-1}(\eta') = \begin{cases} \frac{1}{2^{\lambda_2}}(\eta' \bmod \mu - \mu), & \text{if } \eta' \bmod \mu > \mu/2 \\ \frac{1}{2^{\lambda_2}}(\eta' \bmod \mu), & \text{if } \eta' \bmod \mu \leq \mu/2 \end{cases} \tag{3.14}$$

3.2 Vulnerability of somewhat homomorphic encryption

In this section, it will be shown that the somewhat HE scheme given in Section 3.1 is vulnerable to additive attacks, such as the covert attack introduced in Section 2.4.2.

For this purpose, assume that the attack $\boldsymbol{a}_1$ is injected into the ciphertext $\boldsymbol{w}_r$ obtained by (3.6) and the attack $\boldsymbol{a}_2$ is imposed on the ciphertext $\boldsymbol{c}_r^*$ got by (3.8). Now, the behaviour of the values obtained after the decryption (3.7) will be analyzed.

Theorem 1. *Let the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ and a vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ be encrypted by, respectively,* (3.5) *and* (3.6)*, which gives*

$$\begin{aligned} \boldsymbol{F}_r &= Enc(\boldsymbol{F}, sk) = (\boldsymbol{F} + \boldsymbol{S}_r\theta + \boldsymbol{R}_r p) \ mod\ z_0 \\ \boldsymbol{w}_r &= Enc(\boldsymbol{w}, sk) = (\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \ mod\ z_0 \end{aligned} \tag{3.15}$$

Let $\boldsymbol{a}_1 \in \mathbb{N}^{\beta\times 1}$ and $\boldsymbol{a}_2 \in \mathbb{N}^{\alpha\times 1}$ denote additive attacks on, respectively, the ciphertexts $\boldsymbol{w}_r$ and $\boldsymbol{c}_r^*$, i.e.

$$\begin{aligned} \boldsymbol{w}_r^* &= \boldsymbol{w}_r + \boldsymbol{a}_1 \\ \boldsymbol{c}_r &= \boldsymbol{c}_r^* + \boldsymbol{a}_2 \end{aligned} \tag{3.16}$$

where $\boldsymbol{c}_r^* = (\boldsymbol{F}_r\boldsymbol{w}_r^*)$ mod z_0 is obtained by (3.8)*. If an adversary imposes the additive attacks $\boldsymbol{a}_1, \boldsymbol{a}_2$ with*

$$\|\boldsymbol{w} + \boldsymbol{a}_1 + \boldsymbol{s}_r\theta\|_\infty < p \tag{3.17a}$$

$$\|\boldsymbol{w} + \boldsymbol{a}_1\|_\infty < \theta \tag{3.17b}$$

$$\|\theta(\boldsymbol{F}\boldsymbol{s}_r + \boldsymbol{S}_r\boldsymbol{w}^*) + \theta^2\boldsymbol{S}_r\boldsymbol{s}_r + \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2\|_\infty < p \tag{3.17c}$$

$$\|\boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2\|_\infty < \theta \tag{3.17d}$$

then the decryption of $\boldsymbol{w}_r^*$ and $\boldsymbol{c}_r$ with (3.7) *gives*

$$\begin{aligned} \boldsymbol{\nu}_r^* &= Dec(\boldsymbol{w}_r^*, sk) = \boldsymbol{w} + \boldsymbol{a}_1 \\ \boldsymbol{\nu}_r &= Dec(\boldsymbol{c}_r, sk) = \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2 \end{aligned} \tag{3.18}$$

Proof. According to (3.6), the encryption of $\boldsymbol{w}$ gives

$$\begin{aligned} \boldsymbol{w}_r &= Enc(\boldsymbol{w}, sk) \\ &= (\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \bmod z_0 \\ &= (\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \bmod qp \end{aligned} \tag{3.19}$$

where $z_0 = qp$, θ is an integer and q, p are prime numbers. Due to the additive attack $\boldsymbol{a}_1$,

$$\begin{aligned} \boldsymbol{w}_r^* &= \boldsymbol{w}_r + \boldsymbol{a}_1 \\ &= Enc(\boldsymbol{w}, sk) + \boldsymbol{a}_1 \\ &= (\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \bmod qp + \boldsymbol{a}_1 \end{aligned} \tag{3.20}$$

Substituting (3.20) into (3.7), it gives

$$\begin{aligned} \boldsymbol{\nu}_r^* = Dec(\boldsymbol{w}_r^*, sk) &= (\boldsymbol{w}_r^* \bmod p) \bmod \theta \\ &= \Big(\big((\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) \bmod qp + \boldsymbol{a}_1\big) \bmod p\Big) \bmod \theta \end{aligned}$$

$$= \Big(\big(\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p - \Big\lfloor \frac{\boldsymbol{w} + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p}{qp} \Big\rfloor qp + \boldsymbol{a}_1 \big) \bmod p \Big) \bmod \theta$$
$$= \big((\boldsymbol{w} + \boldsymbol{a}_1 + \boldsymbol{s}_r\theta) \bmod p \big) \bmod \theta \tag{3.21}$$

If (3.17a) holds, then

$$\begin{aligned} \boldsymbol{\nu}_r^* &= Dec(\boldsymbol{w}_r^*, sk) \\ &= (\boldsymbol{w} + \boldsymbol{a}_1 + \boldsymbol{s}_r\theta) \bmod \theta \end{aligned} \tag{3.22}$$

If (3.17b) holds, there is

$$\begin{aligned} \boldsymbol{\nu}_r^* &= Dec(\boldsymbol{w}_r^*, sk) \\ &= \boldsymbol{w} + \boldsymbol{a}_1 \end{aligned} \tag{3.23}$$

i.e. the vector $\boldsymbol{\nu}_r^*$ obtained after the decryption is influenced by the attack $\boldsymbol{a}_1$. Because of the attack $\boldsymbol{a}_2$, there is $\boldsymbol{c}_r = \boldsymbol{c}_r^* + \boldsymbol{a}_2$. Note that

$$\boldsymbol{c}_r \bmod p = (\boldsymbol{c}_r^* + \boldsymbol{a}_2) \bmod p \tag{3.24}$$
$$= \Big((\boldsymbol{F} + \boldsymbol{S}_r\theta + \boldsymbol{R}_f p)(\boldsymbol{w}^* + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p) - \Big\lfloor \frac{(\boldsymbol{F} + \boldsymbol{S}_r\theta + \boldsymbol{R}_f p)(\boldsymbol{w}^* + \boldsymbol{s}_r\theta + \boldsymbol{r}_r p)}{qp} \Big\rfloor qp + \boldsymbol{a}_2 \Big) \bmod p$$
$$= \big(\theta(\boldsymbol{F}\boldsymbol{s}_r + \boldsymbol{S}_r\boldsymbol{w}^*) + \theta^2 \boldsymbol{S}_r\boldsymbol{s}_r + \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2 \big) \bmod p \tag{3.25}$$

If (3.17c) holds, then

$$\boldsymbol{c}_r \bmod p = \theta(\boldsymbol{F}\boldsymbol{s}_r + \boldsymbol{S}_r\boldsymbol{w}^*) + \theta^2 \boldsymbol{S}_r\boldsymbol{s}_r + \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2 \tag{3.26}$$

Due to the decryption (3.7), it yields

$$\begin{aligned} \boldsymbol{\nu}_r &= Dec(\boldsymbol{c}_r, sk) \\ &= (\boldsymbol{c}_r \bmod p) \bmod \theta \\ &= (\theta(\boldsymbol{F}\boldsymbol{s}_r + \boldsymbol{S}_r\boldsymbol{w}^*) + \theta^2 \boldsymbol{S}_r\boldsymbol{s}_r + \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2) \bmod \theta \end{aligned} \tag{3.27}$$

If (3.17d) holds, there is

$$\begin{aligned} \boldsymbol{\nu}_r &= Dec(\boldsymbol{c}_r, sk) \\ &= \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2 \end{aligned} \tag{3.28}$$

i.e. the vector $\boldsymbol{\nu}_r$ obtained after the decryption is influenced by the attack $\boldsymbol{a}_2$. □

Theorem 1 shows that the attack $\boldsymbol{a}_1$ on the encrypted vector $\boldsymbol{w}_r$ (i.e. the vector after manipulation is $\boldsymbol{w}_r^* = \boldsymbol{w}_r + \boldsymbol{a}_1$) corrupts the corresponding vector received by the controller, i.e. $\boldsymbol{\nu}_r^* = Dec(\boldsymbol{w}_r^*, sk) = \boldsymbol{w} + \boldsymbol{a}_1$. Moreover, the attack $\boldsymbol{a}_2$ imposed on the encrypted vector $\boldsymbol{c}_r^*$ (i.e. the vector after manipulation is $\boldsymbol{c}_r = \boldsymbol{c}_r^* + \boldsymbol{a}_2$) affects the corresponding matrix-vector product obtained after the decryption, i.e. $\boldsymbol{\nu}_r = Dec(\boldsymbol{c}_r, sk) = \boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2$. If the adversary wants to change the vector $\boldsymbol{w}$ and the matrix-vector product $\boldsymbol{F}\boldsymbol{w}^*$ by, respectively, $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$, he just needs to change the encrypted vectors $\boldsymbol{w}_r, \boldsymbol{c}_r^*$ corresponding to the vectors $\boldsymbol{w}, \boldsymbol{F}\boldsymbol{w}^*$ by $\boldsymbol{a}_1, \boldsymbol{a}_2$, as long as he makes sure that (3.17) holds.

3.2.1 Influence of the resolution λ_2 on the effect of an additive attack

To handle real values in the context of encrypted transmission, the mapping function introduced in Section 3.1.1 is often applied. As a result, the mapping function will reduce the effect of the attacks $\boldsymbol{a}_1, \boldsymbol{a}_2$ on the vectors $\boldsymbol{w}, \boldsymbol{F}\boldsymbol{w}^*$ obtained by a monitoring system.

Let λ_2 be the resolution of the quantization used in the mapping function introduced in Section 3.1.1. Due to (3.23) and (3.28) and by considering the mapping function (3.12), it gives

$$\begin{aligned} \boldsymbol{\nu}_r^* = Dec(\boldsymbol{w}_r^*, sk) &= 2^{\lambda_2}\boldsymbol{w} + \boldsymbol{a}_1 \\ \boldsymbol{\nu}_r = Dec(\boldsymbol{c}_r, sk) &= 2^{\lambda_2}\boldsymbol{F}2^{\lambda_2}\boldsymbol{w}^* + \boldsymbol{a}_2 \\ &= 2^{2\lambda_2}\boldsymbol{F}\boldsymbol{w}^* + \boldsymbol{a}_2 \end{aligned} \tag{3.29}$$

After the decryption, the vector $\boldsymbol{\nu}_r^*$ is substituted into (3.14) and the vector $\boldsymbol{\nu}_r$ is substituted into (3.13). It yields

$$\begin{aligned} \overline{\Gamma}^{-1}(\boldsymbol{\nu}_r^*) &= \boldsymbol{w} + \frac{\boldsymbol{a}_1}{2^{\lambda_2}} \\ \Gamma^{-1}(\boldsymbol{\nu}_r) &= \boldsymbol{F}\boldsymbol{w}^* + \frac{\boldsymbol{a}_2}{2^{2\lambda_2}} \end{aligned} \tag{3.30}$$

As shown in (3.30), the attacks $\boldsymbol{a}_1, \boldsymbol{a}_2$ are reduced by different factors, i.e. the first attack $\boldsymbol{a}_1$ is about a factor 2^{λ_2} smaller and the second attack $\boldsymbol{a}_2$ is about a factor $2^{2\lambda_2}$ smaller. If the adversary has no knowledge about the value of the resolution λ_2, it could be a challenge for the adversary to carry out a covert attack on the encrypted cloud-based control system without being detected by a conventional monitoring system. However, if the adversary has comprehensive knowledge of the encrypted cloud-based control system, he can compensate the effect by using an attack factor λ_a.

3.2.2 Cloud-based control system encrypted by the somewhat HE scheme under covert attack

A cloud-based control system encrypted by the somewhat HE scheme under covert attack is illustrated in Fig. 3.1.

The controller parameters $\boldsymbol{A}_s$, $\boldsymbol{B}_s$, $\boldsymbol{C}_s$ and $\boldsymbol{D}_s$ are collected in the matrix $\boldsymbol{T}$ by (2.3) and quantized element-wise by (3.11) as $\overline{\boldsymbol{T}} = Q(\boldsymbol{T})$. Then, the quantized matrix $\overline{\boldsymbol{T}}$ is mapped element-wise by the mapping function $\Gamma(\overline{\boldsymbol{T}})$ in (3.12) and encrypted by (3.34), which gives $\boldsymbol{F}_r$.

Instead of sending the sensor outputs $\boldsymbol{y}(k)$ and the state vector $\boldsymbol{x}_s(k)$ directly over the communication network, $\boldsymbol{y}(k)$ and $\boldsymbol{x}_s(k)$ are stacked together by (2.3) and then mapped with, respectively, the quantization function (3.11) and the mapping function

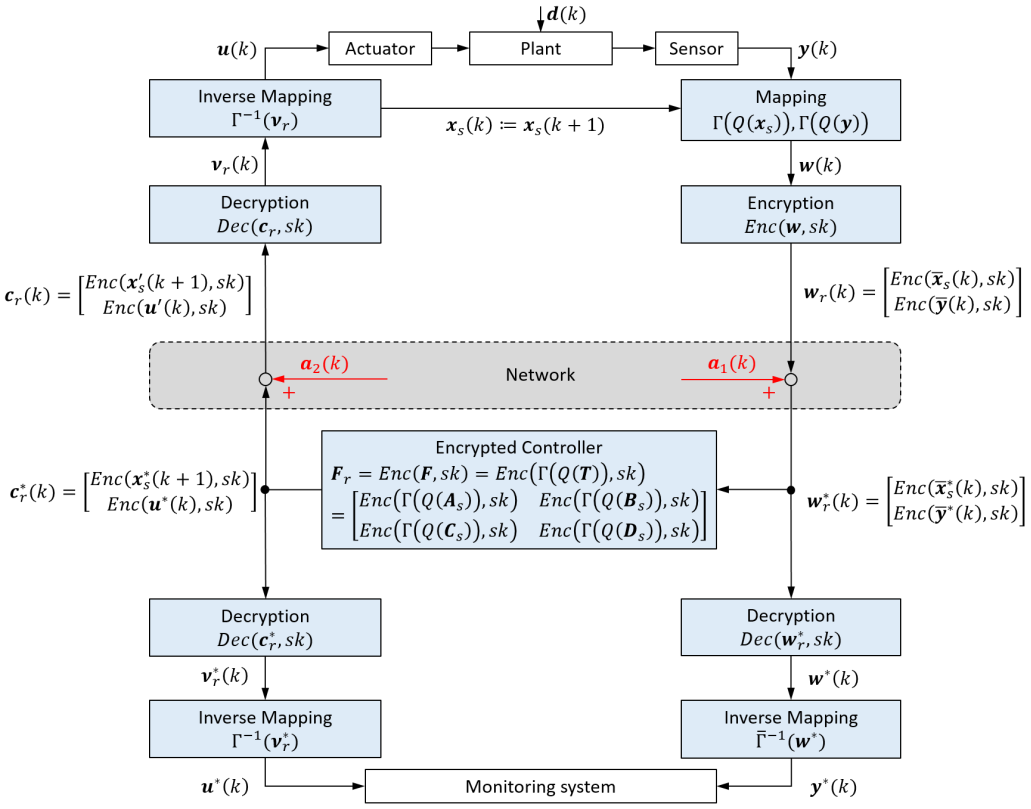

Figure 3.1: Encrypted cloud-based control system with the somewhat HE scheme given by Dyer et al. (2019) under covert attack

in (3.12) into the integer vector $\boldsymbol{w}(k) = [\Gamma^T(Q(\boldsymbol{x}_s))\ \Gamma^T(Q(\boldsymbol{y}))]^T$. Before $\boldsymbol{w}(k)$ is sent over the network to the controller, $\boldsymbol{w}(k)$ is encrypted to $\boldsymbol{w}_r(k)$ in (3.6). On the controller side, $\boldsymbol{w}_r^*(k)$ is processed by the evaluation procedure in (3.8), which gives $\boldsymbol{c}_r^*(k)$. To feed the control input signal $\boldsymbol{u}^*(k)$ and the sensor output signal $\boldsymbol{y}^*(k)$ into the monitoring system, the encrypted vectors $\boldsymbol{w}_r^*, \boldsymbol{c}_r^*(k)$ are decrypted to $\boldsymbol{w}^*(k), \boldsymbol{\nu}_r^*(k)$ by (3.7) and then the inverse mapping functions (3.13), (3.14) are used. The ciphertext $\boldsymbol{c}_r(k)$ arriving at the plant side will be decrypted by (3.7) and then the inverse mapping function in (3.13) is applied, which gives the control input signals $\boldsymbol{u}(k)$ and the state vector $\boldsymbol{x}_s(k+1)$. For the next controller cycle, the state vector $\boldsymbol{x}_s(k)$ is set to $\boldsymbol{x}_s(k+1)$, i.e. $\boldsymbol{x}_s(k) := \boldsymbol{x}_s(k+1)$.

The number of arithmetic operations of the somewhat HE scheme given by Dyer et al. (2019) is limited due to (3.10). Therefore, it is necessary to sent the encrypted state $Enc(\boldsymbol{x}_s^*(k+1), sk)$ generated by the controller to the plant side. If the encrypted state vector $Enc(\boldsymbol{x}_s^*(k+1), sk)$ is not transmitted to the plant side in every control cycle, then the entries $f_{ij} \in \{0, 1, \cdots, M\}$ of the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha \times \beta}$ and the entries $w_j(k) \in \{0, 1, \cdots, M\}$ of the vector $\boldsymbol{w}(k) \in \mathbb{N}^{\beta \times 1}$ involved in the evaluation process of the controller are summed up in every controller cycle. Then, in a finite number of controller cycles, the limit $(2\beta+1)^2 M^2 < \theta$ would be exceeded and the decryption would deliver incorrect values. Therefore, the encrypted state $Enc(\boldsymbol{x}_s^*(k+1), sk)$ calculated by the controller is sent to the plant side, decrypted and set to $\boldsymbol{x}_s(k)$. By

encrypting $\boldsymbol{x}_s(k)$ and sending it to the controller, $Enc(\overline{\boldsymbol{x}}_s(k), sk)$ is a fresh ciphertext in each controller cycle. In this way, the encrypted controller can operate with ciphertexts in an unlimited number of controller cycles.

Now, the behaviour of the encrypted cloud-based control system is analyzed, if a covert attack is considered. If there is no attack, then $\boldsymbol{w}_r^*(k) = \boldsymbol{w}_r(k)$ and $\boldsymbol{c}_r(k) = \boldsymbol{c}_r^*(k)$. Let $\boldsymbol{a}_1(k) = [\mathbf{0}^T \boldsymbol{a}_{11}^T]^T$ and $\boldsymbol{a}_2(k) = [\mathbf{0}^T \boldsymbol{a}_{21}^T]^T$ be the attacks of the adversary imposed, respectively, on $\boldsymbol{w}_r(k)$ and $\boldsymbol{c}_r^*(k)$, where $\boldsymbol{a}_{11}(k) \in \mathbb{N}^{b_y}$, $\boldsymbol{a}_{21}(k) \in \mathbb{N}^m$ and $\mathbf{0}$ is a zero vector of compatible dimensions. There is

$$\begin{aligned} \boldsymbol{w}_r^*(k) &= \begin{bmatrix} Enc\big(\overline{\boldsymbol{x}}_s(k)\big) \\ Enc\big(\overline{\boldsymbol{y}}(k)\big) \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \boldsymbol{a}_{11} \end{bmatrix} \\ \boldsymbol{c}_r(k) &= \begin{bmatrix} Enc\big(\boldsymbol{x}_s(k+1)\big) \\ Enc\big(\boldsymbol{u}(k)\big) \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \boldsymbol{a}_{21} \end{bmatrix} \end{aligned} \tag{3.31}$$

Assume that the adversary is able to cancel the influence of the attack $\boldsymbol{a}_2(k)$ on the sensor output signal $\boldsymbol{y}(k)$ completely. Hence, the monitoring system receives $\boldsymbol{y}^*(k) = \boldsymbol{y}(k)$ through the sensor output channel. After the decryption (3.7) and the inverse mapping (3.13)-(3.14), the signals received through the control input channel by the monitoring system and the actuators are given, respectively, by

$$\begin{aligned} \begin{bmatrix} \boldsymbol{x}_s^*(k) \\ \boldsymbol{y}^*(k) \end{bmatrix} &= \begin{bmatrix} \overline{\boldsymbol{x}}_s(k) \\ \overline{\boldsymbol{y}}(k) \end{bmatrix} + \frac{1}{2^{\lambda_2}} \begin{bmatrix} \mathbf{0} \\ \boldsymbol{a}_{11} \end{bmatrix} \\ \begin{bmatrix} \boldsymbol{x}_s(k+1) \\ \boldsymbol{u}(k) \end{bmatrix} &= \begin{bmatrix} \boldsymbol{x}_s^*(k+1) \\ \boldsymbol{u}^*(k) \end{bmatrix} + \frac{1}{2^{2\lambda_2}} \begin{bmatrix} \mathbf{0} \\ \boldsymbol{a}_{21} \end{bmatrix} \end{aligned} \tag{3.32}$$

The equations in (3.32) are telling us the following important facts.

- Even though an encryption scheme can guarantee the confidentiality of the signals (i.e. the adversary does not know the concrete values represented by $\boldsymbol{w}_r(k)$ and $\boldsymbol{c}_r^*(k)$), it can not prevent the adversary to impose an attack on the ciphertexts. The adversary may still select $\boldsymbol{a}_2(k)$ suitably to influence the plant behaviour and simultaneously impose the corresponding $\boldsymbol{a}_1(k)$ to compensate the influence of $\boldsymbol{a}_2(k)$ on the sensor output signals $\boldsymbol{y}^*(k)$ received by the monitoring system. *That means, the adversary can still implement a covert attack on cloud-based control systems with ciphertexts in a similar way as in unencrypted cloud-based control systems.*

- The resolution λ_2 can reduce the effect of the attacks $\boldsymbol{a}_1(k)$ and $\boldsymbol{a}_2(k)$ on the decrypted signals $\boldsymbol{u}(k)$ and $\boldsymbol{y}^*(k)$, respectively. The bigger the λ_2 is, the smaller the effect of the attack will be.

- The adversary usually does not know the parameters of the encryption scheme, including the resolution λ_2. But the adversary may circumvent it by multiplying the attacks $\boldsymbol{a}_1(k), \boldsymbol{a}_2(k)$ generated in (2.10) by an additional attack factor λ_a to adjust the attack effect, i.e.

$$\begin{aligned} \boldsymbol{w}_r^*(k) &= \boldsymbol{w}_r(k) + \hat{\boldsymbol{a}}_1(k) \\ \boldsymbol{c}_r(k) &= \boldsymbol{c}_r^*(k) + \hat{\boldsymbol{a}}_2(k) \end{aligned} \tag{3.33}$$

where

$$\hat{\boldsymbol{a}}_1(k) = 2^{\lambda_a}\boldsymbol{a}_1(k)$$
$$\hat{\boldsymbol{a}}_2(k) = 2^{2\lambda_a}\boldsymbol{a}_2(k)$$

3.3 Resilient homomorphic encryption

In this section, the RHE scheme is proposed that modifies the somewhat HE scheme given by Dyer et al. (2019) and neutralizes the effect of additive attacks imposed on the ciphertexts. As the RHE is homomorphic with respect to the matrix-vector product, not only the signals transmitted over the network can be encrypted but also the parameter matrix of dynamic output feedback controllers can be encrypted.

The four functions $\mathcal{E}' = (RHE.KeyGen,\ RHE.Enc,\ RHE.Dec,\ RHE.Eval)$ are defined for the RHE scheme.

Key Generation ($RHE.KeyGen$): At first, select the security parameter κ and choose the parameters ρ, θ, ψ, γ as discussed later in Section 3.5.2. Then, sample a ψ-bit prime number p and an integer q from $[0, \lfloor 2^{\gamma}/p \rfloor]$ so that $q > p$, q can not be factorized into integers smaller than 2^{ψ} and $qp \geq 2^{\gamma-1}$. Finally, let $z_0 = qp$ be the divisor in the modulo operations and $sk = (\theta, p)$ is the secret key for encryption and decryption.

Encryption ($RHE.Enc$): A matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ is encrypted by

$$\begin{aligned}\boldsymbol{F}_c &= RHE.Enc(\boldsymbol{F}, sk)\\ &= (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p) \bmod qp\\ &= (\boldsymbol{Z} + \boldsymbol{F}\theta) \bmod z_0\end{aligned} \tag{3.34}$$

and a vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ is encrypted by

$$\begin{aligned}\boldsymbol{w}_c &= RHE.Enc(\boldsymbol{w}, sk)\\ &= (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod qp\\ &= (\boldsymbol{z} + \boldsymbol{w}\theta) \bmod z_0\end{aligned} \tag{3.35}$$

where all the entries f_{ij} and w_j in, respectively, $\boldsymbol{F}$ and $\boldsymbol{w}$ belong to the set $\{0, 1, \cdots, M\}$, the entries s_{ij}, s_j in $\boldsymbol{S}_f, \boldsymbol{s}_w$ are integers uniformly selected from $\{-2^{\rho}+1, \cdots, 2^{\rho}-1\}$ and the entries r_{ij}, r_j in $\boldsymbol{R}_f, \boldsymbol{r}_w$ are integers uniformly selected from $\{0, 1, \cdots, q-1\}$, M is a known integer, $i = 1, 2, \cdots, \alpha$, $j = 1, 2, \cdots, \beta$.

Decryption ($RHE.Dec$): The decryption of an encrypted vector $\boldsymbol{c}_{\times} \in \mathbb{N}^{\alpha\times 1}$ is given by

$$\begin{aligned}\boldsymbol{\nu} &= RHE.Dec(\boldsymbol{c}_{\times}, sk)\\ &= \frac{\boldsymbol{c}_{\times} \bmod p - (\boldsymbol{c}_{\times} \bmod p) \bmod \theta^2}{\theta^2}\end{aligned} \tag{3.36}$$

Evaluation (*RHE.Eval*): The matrix-vector product of the encrypted matrix $\boldsymbol{F}_c$ and the encrypted vector $\boldsymbol{w}_c$ is

$$\boldsymbol{c}_\times = (\boldsymbol{F}_c \boldsymbol{w}_c) \bmod z_0 \tag{3.37}$$

whose decryption is equal to $\boldsymbol{F}\boldsymbol{w}$.

3.3.1 Conditions for the correct decryption in the RHE scheme

To ensure that the RHE scheme is homomorphic with respect to the matrix-vector product and delivers the correct result after the decryption (3.36), a sufficient condition for the correct decryption is given below.

Theorem 2. *Let $z_0 = qp$ denote the modulus, where q is an integer uniformly chosen from $[0, \lfloor 2^\gamma/p \rfloor]$ and p is a ψ-bit prime number. Let the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ and the vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ be encrypted by*

$$\begin{aligned} \boldsymbol{F}_c &= RHE.Enc(\boldsymbol{F}, sk) = (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p) \bmod z_0 \\ \boldsymbol{w}_c &= RHE.Enc(\boldsymbol{w}, sk) = (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod z_0 \end{aligned} \tag{3.38}$$

where all the entries f_{ij} and w_j in, respectively, $\boldsymbol{F}$ and $\boldsymbol{w}$ belong to the set $\{0, 1, \cdots, M\}$, the entries s_{ij}, s_j in $\boldsymbol{S}_f, \boldsymbol{s}_w$ are integers uniformly selected from $\{-2^\rho+1, \cdots, 2^\rho-1\}$ and the entries r_{ij}, r_j in $\boldsymbol{R}_f, \boldsymbol{r}_w$ are integers uniformly selected from $\{0, 1, \cdots, q-1\}$, M is a known integer, $i = 1, 2, \cdots, \alpha$, $j = 1, 2, \cdots, \beta$. Assume that the ciphertext $\boldsymbol{c}_\times$ is obtained by (3.37). If

$$\beta\big(2^{2\rho} + \theta M 2^{\rho+1}\big) + \beta\theta^2 M^2 < p \tag{3.39a}$$

$$\beta\big(2^{2\rho} + \theta M 2^{\rho+1}\big) < \theta^2 \tag{3.39b}$$

then $Dec(\boldsymbol{c}_\times, sk)$ in (3.36) delivers the true result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$, i.e.

$$RHE.Dec(\boldsymbol{c}_\times, sk) = \boldsymbol{F}\boldsymbol{w} \tag{3.40}$$

Proof. Due to (3.34) and (3.35), the vector $\boldsymbol{c}_\times$ in (3.37) is obtained by

$$\begin{aligned} \boldsymbol{c}_\times &= (\boldsymbol{F}_c \boldsymbol{w}_c) \bmod z_0 \\ &= \Big(\big((\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p) \bmod z_0\big)\big((\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod z_0\big)\Big) \bmod z_0 \\ &= \big((\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)\big) \bmod z_0 \\ &= (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) - \Big\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)}{z_0} \Big\rfloor z_0 \end{aligned} \tag{3.41}$$

Note that $z_0 = qp$ and

$$\boldsymbol{c}_\times \bmod p = \big((\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)$$

$$
\begin{aligned}
&\quad - \Big\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)}{qp} \Big\rfloor qp \big) \bmod p \\
&= \big((\boldsymbol{S}_f + \boldsymbol{F}\theta)(\boldsymbol{s}_w + \boldsymbol{w}\theta) \big) \bmod p \\
&= (\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w}) \bmod p
\end{aligned} \tag{3.42}
$$

Recall that all the entries f_{ij} of the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha \times \beta}$ and all the entries w_j of the vector $\boldsymbol{w} \in \mathbb{N}^{\beta \times 1}$ are from the set $\{0, 1, \cdots, M\}$. There is

$$
\begin{aligned}
&\|\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w}\|_\infty \\
&\quad \le \|\boldsymbol{S}_f \boldsymbol{s}_w\|_\infty + \theta(\|\boldsymbol{S}_f \boldsymbol{w}\|_\infty + \|\boldsymbol{F}\boldsymbol{s}_w\|_\infty) + \theta^2 \|\boldsymbol{F}\boldsymbol{w}\|_\infty \\
&\quad \le \beta \|\boldsymbol{S}_f\|_{max} \|\boldsymbol{s}_w\|_\infty + \beta\theta \|\boldsymbol{S}_f\|_{max} \|\boldsymbol{w}\|_\infty \\
&\qquad + \beta\theta \|\boldsymbol{F}\|_{max} \|\boldsymbol{s}_w\|_\infty + \beta\theta^2 \|\boldsymbol{F}\|_{max} \|\boldsymbol{w}\|_\infty \\
&\quad \le \beta\big(2^{2\rho} + \theta M 2^{\rho+1}\big) + \beta\theta^2 M^2
\end{aligned} \tag{3.43}
$$

If (3.39a) holds, then

$$
\boldsymbol{c}_\times \bmod p = \boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w} \tag{3.44}
$$

and

$$
\begin{aligned}
(\boldsymbol{c}_\times \bmod p) \bmod \theta^2 &= \big(\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w}\big) \bmod \theta^2 \\
&= \big(\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w)\big) \bmod \theta^2
\end{aligned} \tag{3.45}
$$

Note that

$$
\begin{aligned}
\|\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w)\|_\infty &\le \beta \|\boldsymbol{S}_f\|_{max} \|\boldsymbol{s}_w\|_\infty + \beta\theta \|\boldsymbol{S}_f\|_{max} \|\boldsymbol{w}\|_\infty \\
&\quad + \beta\theta \|\boldsymbol{F}\|_{max} \|\boldsymbol{s}_w\|_\infty \\
&\le \beta\big(2^{2\rho} + \theta M 2^{\rho+1}\big)
\end{aligned} \tag{3.46}
$$

If (3.39b) holds, there is

$$
(\boldsymbol{c}_\times \bmod p) \bmod \theta^2 = \boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) \tag{3.47}
$$

Substituting (3.44) and (3.47) into (3.36), we get

$$
\begin{aligned}
\boldsymbol{\nu} &= RHE.Dec(\boldsymbol{c}_\times, sk) \\
&= \frac{\boldsymbol{c}_\times \bmod p - (\boldsymbol{c}_\times \bmod p) \bmod \theta^2}{\theta^2} \\
&= \frac{\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w}}{\theta^2} - \frac{\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w)}{\theta^2} \\
&= \boldsymbol{F}\boldsymbol{w}
\end{aligned} \tag{3.48}
$$

i.e. the decryption (3.36) delivers the correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ and the RHE scheme is homomorphic with respect to the matrix-vector product. □

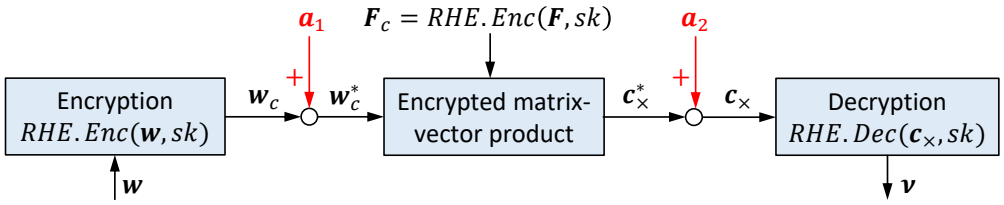

Figure 3.2: Attacks on the signals encrypted by the RHE scheme

3.4 Resilience of homomorphic encryption

In this section, the resilience of the RHE scheme to additive attacks will be shown. For this purpose, assume that two attacks are injected into the communication encrypted by the RHE scheme as shown in Fig. 3.2. The first additive attack $\boldsymbol{a}_1$ is injected into the signal $\boldsymbol{w}_c$ encrypted by (3.35). The second additive attack $\boldsymbol{a}_2$ is imposed on the ciphertext $\boldsymbol{c}_\times^*$ obtained after the encrypted matrix-vector product in (3.37). Now the behaviour of the value $\boldsymbol{\nu}$ obtained after the decryption will be analyzed.

Theorem 3. *Assume that the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ and the vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ are encrypted by, respectively,* (3.34) *and* (3.35)*, which gives*

$$\begin{aligned} \boldsymbol{F}_c &= RHE.Enc(\boldsymbol{F}, sk) = (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p) \ mod\ z_0 \\ \boldsymbol{w}_c &= RHE.Enc(\boldsymbol{w}, sk) = (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \ mod\ z_0 \end{aligned} \tag{3.49}$$

Let $\boldsymbol{a}_1 \in \mathbb{N}^{\beta\times 1}$ and $\boldsymbol{a}_2 \in \mathbb{N}^{\alpha\times 1}$ denote additive attacks on, respectively, the ciphertexts $\boldsymbol{w}_c$ and $\boldsymbol{c}_\times^*$, i.e.

$$\boldsymbol{w}_c^* = \boldsymbol{w}_c + \boldsymbol{a}_1, \quad \boldsymbol{c}_\times = \boldsymbol{c}_\times^* + \boldsymbol{a}_2, \tag{3.50}$$

where $\boldsymbol{c}_\times^* = (\boldsymbol{F}_c \boldsymbol{w}_c^*)$ mod z_0 is obtained by (3.37)*. If the decryption of $\boldsymbol{c}_\times$ is carried out by* (3.36)*, then*

$$\boldsymbol{\nu} = RHE.Dec(\boldsymbol{c}_\times, sk) = \boldsymbol{F}\boldsymbol{w}, \tag{3.51}$$

as long as

$$\boldsymbol{\delta} p - \boldsymbol{h} \leq \boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{a}_2 < \boldsymbol{\delta} p + \theta^2 \boldsymbol{1} - \boldsymbol{h}, \tag{3.52}$$

where $\boldsymbol{h} = \boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w)$, $\boldsymbol{G} = \boldsymbol{S}_f + \theta\boldsymbol{F}$, $\boldsymbol{1}_{\alpha\times 1}$ is a vector of ones and $\boldsymbol{\delta} \in \mathbb{N}^{\alpha\times 1}$ whose entries are $\delta_i \in \{0, 1, \cdots, q-1\}$.

Proof. According to (3.35), the encryption of $\boldsymbol{w}$ gives

$$\begin{aligned} \boldsymbol{w}_c &= RHE.Enc(\boldsymbol{w}, sk) \\ &= (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod z_0, \end{aligned} \tag{3.53}$$

where θ, z_0 are integers and p is a prime number. Due to the additive attack $\boldsymbol{a}_1$,

$$\begin{aligned} \boldsymbol{w}_c^* &= RHE.Enc(\boldsymbol{w}, sk) + \boldsymbol{a}_1 \\ &= (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod z_0 + \boldsymbol{a}_1 \end{aligned} \tag{3.54}$$

The matrix-vector product in (3.37) gives

$$\begin{aligned}\boldsymbol{c}_{\times}^{*} &= (\boldsymbol{F}_c \boldsymbol{w}_c^{*}) \bmod z_0 \\ &= (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p + \boldsymbol{a}_1) \\ &\quad - \Big\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p + \boldsymbol{a}_1)}{z_0} \Big\rfloor z_0\end{aligned}$$

Because of the attack $\boldsymbol{a}_2$, there is $\boldsymbol{c}_{\times} = \boldsymbol{c}_{\times}^{*} + \boldsymbol{a}_2$. Note that $z_0 = qp$ and

$$\begin{aligned}\boldsymbol{c}_{\times} \bmod p &= \Big((\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p + \boldsymbol{a}_1) \\ &\quad - \Big\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p + \boldsymbol{a}_1)}{qp} \Big\rfloor qp + \boldsymbol{a}_2 \Big) \bmod p \\ &= \big(\underbrace{(\boldsymbol{S}_f + \theta \boldsymbol{F})}_{=\boldsymbol{G}} \boldsymbol{a}_1 + \underbrace{\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w)}_{=\boldsymbol{h}} + \theta^2 \boldsymbol{F}\boldsymbol{w} + \boldsymbol{a}_2 \big) \bmod p \qquad (3.55)\end{aligned}$$

If the attacks $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ satisfy (3.52), then $\boldsymbol{\delta} p \leq \boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{h} + \boldsymbol{a}_2 < \boldsymbol{\delta} p + \theta^2 \mathbf{1}$. Let

$$\boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{h} + \boldsymbol{a}_2 = \boldsymbol{\delta} p + \boldsymbol{\Delta}, \qquad (3.56)$$

where $\boldsymbol{\Delta} \in \mathbb{N}^{\alpha \times 1}$ whose entries are $\Delta_i \in \{0, 1, \cdots, \theta^2 - 1\}$. Thus,

$$\begin{aligned}\boldsymbol{c}_{\times} \bmod p &= (\boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{h} + \boldsymbol{a}_2 + \theta^2 \boldsymbol{F}\boldsymbol{w}) \bmod p \qquad (3.57) \\ &= (\boldsymbol{\delta} p + \boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}) \bmod p \\ &= \boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w} \qquad (3.58)\end{aligned}$$

Due to the decryption (3.36), it yields

$$\begin{aligned}\boldsymbol{\nu} &= RHE.Dec(\boldsymbol{c}_{\times}, sk) \\ &= \frac{\boldsymbol{c}_{\times} \bmod p - (\boldsymbol{c}_{\times} \bmod p) \bmod \theta^2}{\theta^2} \\ &= \frac{\boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w} - (\boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}) \bmod \theta^2}{\theta^2} \\ &= \boldsymbol{F}\boldsymbol{w},\end{aligned} \qquad (3.59)$$

i.e. the vector $\boldsymbol{\nu}$ is still the correct result of $\boldsymbol{F}\boldsymbol{w}$. □

3.5 Security proof and parameter selection

In this section, it will be shown that the ciphertexts generated by the RHE scheme given in Section 3.3 obeys the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q, p)$ described in Definition 2 and the RHE scheme satisfies IND-CPA. Moreover, the well-known attacks against the EF-AGCD problem will be considered to derive the requirements of the parameters in the RHE scheme.

3.5.1 Security analysis

At first, the concept of truncated distributions will be introduced. A truncated distribution is a distribution that has been restricted to a specific range by imposing bounds on the random variable, as shown in Definition 7.

Definition 7 (Truncated distribution (Limnios and Nikulin, 2000))**.** *Let H be a random variable following the distribution $\mathcal{H}$ with the probability mass function (PMF) $f_H(h)$, where $h \in \mathbb{Z}$. Assume that h_0 is a fixed integer value and $F(h_0) = P(H \leq h_0)$ is the cumulative distribution function (CDF). The right-truncated distribution $\mathcal{H}^{(<h_0)}$ is obtained by normalizing the PMF $f_H(h)$ over the truncated interval $(-\infty, h_0)$, i.e.*

$$f_H(h \mid H < h_0) = \begin{cases} f_H(h)/F(h_0), & \text{if } h < h_0 \\ 0, & \text{if } h \geq h_0 \end{cases}$$

The left-truncated distribution $\mathcal{H}^{(\geq h_0)}$ is obtained by normalizing the PMF $f_H(h)$ over the truncated interval $[h_0, \infty)$, i.e.

$$f_H(h \mid H \geq h_0) = \begin{cases} 0, & \text{if } h < h_0 \\ f_H(h)/(1 - F(h_0)), & \text{if } h \geq h_0 \end{cases}$$

Next, a distribution can be constructed that is efficiently computable and computationally indistinguishable from the uniform distribution, which shows that the distribution of the ciphertexts generated by the RHE scheme is computationally indistinguishable from the uniform distribution.

Lemma 1. *Suppose that $\mathcal{U}_\gamma$ is an uniform distribution over the interval $[0, 2^\gamma - 1]$. Let u_0 be an integer chosen uniformly from the interval $[2^{\gamma-1}, 2^\gamma - 1]$, $\mathcal{U}_\gamma^{(<u_0)}$ is the right-truncated uniform distribution with support over $[0, u_0 - 1]$. Denote by $z_0 = qp$ an integer, where p is an ψ-bit prime number, q is an integer uniformly selected from $[0, \lfloor 2^\gamma/p \rfloor]$ and $z_0 \in [2^{\gamma-1}, 2^\gamma - 1]$. Let $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q, p)$ be the right-truncated AGCD distribution with support over $\{z \mid z = s + rp, z < z_0\}$, where s and r are independent random integers uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, q - 1]$, $\mathcal{D}_{\gamma,\rho}(q, p)$ is the AGCD distribution given in Definition 2. Then, it holds that the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ and the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q, p)$ are computationally indistinguishable.*

Proof. Let U be the random variable following the uniform distribution $\mathcal{U}_\gamma$ with the PMF $f_U(u)$, where u is a given integer from the interval $[0, 2^\gamma - 1]$. Denote by $\mathcal{U}_\gamma^{(<u_0)}$ the right-truncated uniform distribution with the PMF $f_U(u \mid U < u_0)$, where u_0 is an integer uniformly chosen from the interval $[2^{\gamma-1}, 2^\gamma - 1]$ and $P[U < u_0] \geq 1/2$. An independent sample $\overline{U}$ drawn from the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ can be obtained by exploiting the uniform distribution $\mathcal{U}_\gamma$ as follows.

Step 1. Draw an independent sample U according to $f_U(u)$.

Step 2. If $U < u_0$, set $\overline{U} = U$. If $U \geq u_0$, then repeat Step 1.

Since $P[U < u_0] \geq 1/2$, the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ can be effectively generated with the uniform distribution $\mathcal{U}_\gamma$. Moreover, the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ is an uniform distribution with support over $[0, u_0 - 1]$.

Recall that p is a ψ-bit prime number, q is an integer uniformly chosen from the interval $[0, \lfloor 2^\gamma/p \rfloor]$ and $z_0 = qp$ is an integer that satisfies $z_0 \geq 2^{\gamma-1}$. Denote by Z a random variable following the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ defined in Definition 2 with PMF $f_Z(z)$. Assume that z is a given integer from the set $\{z \mid z = s + rp\}$, where s and r are independent random integers uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, q-1]$. Let $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ be the right-truncated AGCD distribution with PMF $f_Z(z \mid Z < z_0)$ and $P[Z < z_0] \geq 1/2$. An independent sample $\overline{Z}$ drawn from the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ can be obtained by using the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ as follows.

Step 1. Draw an independent sample Z according to $f_Z(z)$.

Step 2. If $Z < z_0$, set $\overline{Z} = Z$. If $Z \geq z_0$, then repeat Step 1.

Since $P[Z < z_0] \geq 1/2$, the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ can be efficiently generated from the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$. Moreover, the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ is also an AGCD distribution with support over $\{z \mid z = s + rp, z < z_0\}$. According to Lepoint (2014), Cheon and Stehlé (2015), Benarroch et al. (2017), and Pereira (2021), currently no algorithm exists that can distinguish between the uniform distribution $\mathcal{U}_\gamma$ and the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ in polynomial time. Since the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ follows an uniform distribution and the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ follows an AGCD distribution, the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ and the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ are computationally indistinguishable. □

Lemma 1 shows that the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ and the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ are computationally indistinguishable.

IND-CPA ensures that an encryption scheme remains secure even if an adversary has access to ciphertexts corresponding to chosen plaintexts. Thus, an adversary can learn nothing about the plaintext based on the corresponding ciphertext. In the following, the well-established *hybrid argument technique* will be exploited to show that the RHE scheme satisfies IND-CPA. The hybrid argument technique enables to show the indistinguishability between different distributions (Mittelbach and Fischlin, 2021). For this purpose, we define two hybrid arguments $\mathcal{H}_0$ and $\mathcal{H}_1$ so that the advantage for any adversary to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$ is negligible. Due to these hybrid arguments, it can be concluded that any adversary can not distinguish between the ciphertexts generated by the RHE scheme and integers uniformly distributed and thus the RHE scheme satisfies IND-CPA. According to Katz and Lindell (2020), an encryption scheme that satisfies IND-CPA for the encryption of a single plaintext automatically satisfies IND-CPA for multiple encryptions. That means, we can focus on one encrypted plaintext instead of the encrypted matrix $\boldsymbol{F}_c$ in (3.34) and the encrypted vector $\boldsymbol{w}_c$ in (3.35), as shown below.

Theorem 4. *The RHE scheme given in Section 3.3 satisfies IND-CPA because of the computational indistinguishability of the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ and the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ proven in Lemma 1.*

Proof. Let $\mathcal{A}$ be the adversary that tries to win the CPA experiment introduced in Section 2.5. The adversary $\mathcal{A}$ chooses two plaintexts $w_i \in \{0, 1, \cdots, M\}$, where $i = 1, 2$. Then the integer v is selected randomly from the set $\{1, 2\}$ so that the adversary does not know whether w_1 or w_2 is now encrypted.

Hybrid $\mathcal{H}_0$: Let $\mathcal{E}_0' = (RHE.KeyGen_0, RHE.Enc_0, RHE.Dec_0, RHE.Eval_0)$ be the RHE scheme whose key generation function is denoted by $RHE.KeyGen_0(1^\kappa)$, the secret key is $sk = (\theta, p)$ and the parameters are γ, ψ, ρ, z_0, where $z_0 \geq 2^{\gamma-1}$. Then, the plaintext w_v is encrypted by

$$\begin{aligned} c_0 &= RHE.Enc_0(w_v, sk) \\ &= (s + w_v\theta + rp) \bmod qp \\ &= (z + w_v\theta) \bmod z_0 \end{aligned} \tag{3.60}$$

where z follows the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ with supported over the set $\{z \mid z = s + rp, z < z_0\}$, s and r are independent random integers uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, q-1]$, $\mathcal{D}_{\gamma,\rho}(q,p)$ is the AGCD distribution given in Definition 2.

Hybrid $\mathcal{H}_1$: Suppose that $\mathcal{U}_\gamma$ is an uniform distribution over the interval $[0, 2^\gamma - 1]$. Let $\overline{u}$ be a random integer following the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ with support over $[0, u_0 - 1]$, where u_0 is an integer uniformly chosen from $[2^{\gamma-1}, 2^\gamma - 1]$. Then, let $\mathcal{E}_1' = (RHE.KeyGen_1, RHE.Enc_1, RHE.Dec_1, RHE.Eval_1)$ denotes the encryption scheme whose key generation function $RHE.KeyGen_1(1^\kappa)$ outputs the secret key $sk = (\theta, p)$ and the parameters γ, ψ, ρ, u_0. The ciphertexts c_1 following the distribution $\mathcal{H}_1$ generated by the encryption function $RHE.Enc_1(w_v, sk)$ is given as

$$\begin{aligned} c_1 &= RHE.Enc_1(w_v, sk) \\ &= (\overline{u} + w_v\theta) \bmod u_0 \\ &= (\overline{u} + \overline{w}_v) \bmod u_0 \\ &= \overline{u}_w \end{aligned} \tag{3.61}$$

Recall that $\overline{w}_v = w_v\theta$ is a constant integer during the CPA experiment and $\overline{u}$ is a random integer following the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ with support over $[0, u_0 - 1]$. Thus, $\overline{u} + \overline{w}_v$ is a random integer and has an uniform distribution supported over $[\overline{w}_v, \overline{w}_v + u_0 - 1]$. Due to the modulo operator u_0 applied on $\overline{u} + \overline{w}_v$, the integer $\overline{u}_w = (\overline{u} + \overline{w}_v) \bmod u_0$ follows the right-truncated uniform distributions $\mathcal{U}_\gamma^{(<u_0)}$. That means, the ciphertext c_1 obtained in (3.61) also follows the right-truncated uniform distributions $\mathcal{U}_\gamma^{(<u_0)}$. The difference between the hybrid argument $\mathcal{H}_0$ and the hybrid argument $\mathcal{H}_1$ lies in the integers z, z_0 in (3.60) and the integers $\overline{u}, u_0$ in (3.61) defined by, respectively, the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ and the right-truncated uniform distributions $\mathcal{U}_\gamma^{(<u_0)}$. Since the

right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$ and the right-truncated uniform distribution $\mathcal{U}_{\gamma}^{(<u_0)}$ are computationally indistinguishable according to Lemma 1, the adversary $\mathcal{A}$ can not distinguish between the hybrid argument $\mathcal{H}_0$ and the hybrid argument $\mathcal{H}_1$. Hence, the difference between the probability of success for the adversary $\mathcal{A}$ to win the CPA experiment in the hybrid argument $\mathcal{H}_0$ and the probability of success for the adversary $\mathcal{A}$ to win the CPA experiment in the hybrid argument $\mathcal{H}_1$ is negligible, which is denoted by

$$\left|\Pr_{\mathcal{H}_0}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_0'}(\kappa)=1]-\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1]\right|\leq negl(\kappa) \tag{3.62}$$

where $negl(\cdot)$ is the negligible function. According to Benarroch et al. (2017), the success for the adversary $\mathcal{A}$ to win the CPA experiment in a hybrid argument following an uniform distribution is 1/2. Thus, the probability for the adversary $\mathcal{A}$ to correctly guess whether w_1 or w_2 has been encrypted in the hybrid argument $\mathcal{H}_1$ which follows the right-truncated uniform distribution $\mathcal{U}_{\gamma}^{(<u_0)}$ is 1/2, i.e.

$$\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1]=\frac{1}{2} \tag{3.63}$$

Due to (3.62) and (3.63), the success for the adversary $\mathcal{A}$ to win the CPA experiment in the hybrid argument $\mathcal{H}_0$ is given by

$$\begin{aligned}\left|\Pr_{\mathcal{H}_0}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_0'}(\kappa)=1]\right| &= \Big|\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1] \\ &\quad+\Pr_{\mathcal{H}_0}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_0'}(\kappa)=1]-\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1]\Big| \\ &\leq \left|\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1]\right| \\ &\quad+\left|\Pr_{\mathcal{H}_0}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_0'}(\kappa)=1]-\Pr_{\mathcal{H}_1}[\text{IND-CPA}_{\mathcal{A},\mathcal{E}_1'}(\kappa)=1]\right| \\ &\leq \frac{1}{2}+negl(\kappa)\end{aligned} \tag{3.64}$$

That means, the probability for the adversary $\mathcal{A}$ to successfully guess whether w_1 or w_2 has been encrypted by the RHE scheme is negligibly better than 1/2. Thus, the RHE scheme satisfies IND-CPA. □

Since the RHE scheme satisfies IND-CPA, ciphertexts generated by the RHE scheme reveals no information about the plaintext.

3.5.2 Selection of parameters

The question now is how to choose the parameters ρ, θ, p, ψ and γ of the RHE scheme, so that the encryption scheme is homomorphic with respect to the matrix-vector product and simultaneously secure against the main families of known attacks, namely, brute force attacks (Chen and Nguyen, 2012; Coron et al., 2012), factorisation of the modulus $z_0 = qp$ (Lenstra, 1987; Lenstra et al., 1993) and lattice attacks (Cheon and Stehlé, 2015; Galbraith et al., 2016).

According to Theorem 2, the integer θ and the prime number p in the secret key $sk = (\theta, p)$ need to satisfy (3.39), so that the decryption (3.36) applied on $\boldsymbol{c}_\times = (\boldsymbol{F}_c \boldsymbol{w}_c) \bmod z_0$ (3.37) delivers the true result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$. Moreover, in order to ensure that the main families of known attacks are not able to gain access to the secret key $sk = (\theta, p)$, the bit-size ρ of the noises in (3.34) and (3.35), the bit-size ψ of the prime number p and the bit-size γ of the ciphertext space should satisfy further conditions. Note that in the field of cryptography, an encryption scheme is said to be secure with security level κ, if the main families of known attacks require at least 2^κ operations to gain access to the secret key (Lepoint, 2014; Benarroch et al., 2017; Pereira, 2020).

Brute force attacks: The brute force attack tries to break an encryption scheme by trying all potential secret keys until the true value of the secret key $sk = (\theta, p)$ used in the encryption scheme has been found.

According to Chen and Nguyen (2012), the brute force attack can not find the secret key $sk = (\theta, p)$ in polynomial time, if

$$\rho \geq 2\kappa \tag{3.65}$$

Factorisation attacks: Until now, the most efficient methods to factorise $z_0 = qp$ to get the integer q and the prime number p are the elliptic-curve method (ECM) (Lenstra, 1987) and the number field sieve (NFS) (Lenstra et al., 1993).

ECM: Recall that $z_0 = qp$ denotes the divisor in the modulo operations, where p is a ψ-bit prime number, q is an integer and $q > p$. Then the factorisation of the divisor z_0 in the modulo operations requires at least $2^{\kappa_{ECM}}$ operations, where κ_{ECM} is given by

$$\kappa_{ECM} = \frac{1}{\ln 2}\Big(2\psi \ln(\psi \ln 2)\Big)^{\frac{1}{2}} + 5. \tag{3.66}$$

NFS: Recall that γ is the bit-size of the ciphertext space and z_0 is the divisor in the modulo operations used in the encryption (3.34), (3.35). Then at least $2^{\kappa_{NFS}}$ operations are required to factorise z_0, where

$$\kappa_{NFS} = \Big(\frac{64}{9}\Big)^{\frac{1}{3}} \big(\gamma \ln 2\big)^{\frac{1}{3}} \Big(\ln\big(\gamma \ln 2\big)\Big)^{\frac{2}{3}} - 14 \tag{3.67}$$

Thus, as long as the parameters of the RHE scheme are chosen in such a way that

$$\kappa_{ECM} \geq \kappa \tag{3.68a}$$

$$\kappa_{NFS} \geq \kappa \tag{3.68b}$$

hold, the divisor z_0 in the modulo operations can not be factorised in polynomial time.

Lattice attacks: According to Galbraith et al. (2016), the most efficient method to solve the EF-AGCD problem by lattice attacks is the so-called orthogonal lattice (OL) attack. At first, the OL attack tries to find vectors that are orthogonal to the

unknown vector $\boldsymbol{r} \in \mathbb{N}^{1\times l}$ whose entries are the noise $r_i \in [0, q-1]$ contained in the integer $z_i = s_i + r_i p$, $i = 1, 2, \cdots, l$, drawn from the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q, p)$ given in Definition 2. Then, the prime number p can be figured out and the encryption scheme based on the EF-AGCD problem is broken.

The OL attacks can only be carried out in polynomial time, if $\gamma \leq l(\psi - \rho) + \rho$ holds. Until now, if $l \geq 800$, then the OL attacks are regarded as infeasible (Benarroch et al., 2017; Cominetti and Simplicio, 2020). Thus, it is required that

$$\gamma > 800(\psi - \rho) + \rho \tag{3.69}$$

The parameters ρ, θ, p, ψ and γ of the RHE scheme in Section 3.3 can be systematically determined as follows.

Step 1: Choose the security level κ according to National Institute of Standards and Technology (2020).

Step 2: Set $\rho = 2\kappa$ to satisfy (3.65) and select the integer θ so that (3.39b) holds.

Step 3: Select the bit-size ψ and the prime number p so that condition (3.39a) and condition (3.68a) are fulfilled simultaneously.

Step 4: Choose the bit-size γ of the ciphertext to satisfy condition (3.68b) and condition (3.69) simultaneously.

3.6 Analysis of mapping function and quantization error

In this section, it will be proven that the transformation between quantized values and integer values causes no error in the calculation of the matrix-vector product. Since the transformation between real values and quantized values causes the so-called quantization error and may affect the plant behaviour, a condition for the stability of the closed-loop system will be derived.

3.6.1 Mapping function applied on the matrix-vector product

In this subsection, it will be shown that if the mapping function Γ in (3.12) and the inverse mapping function Γ^{-1} in (3.13) are used pairwise, then there is no approximation error caused by the transformation between quantized values and integer values of the system matrix $\overline{\boldsymbol{T}}$ and the signals $\overline{\boldsymbol{g}}(k)$. Thus, the inverse mapping function Γ^{-1} in (3.13) always delivers the correct result of the matrix-vector product $\overline{\boldsymbol{T}}\overline{\boldsymbol{g}}(k)$.

Theorem 5. *Let the quantized matrix $\overline{\boldsymbol{T}} \in \mathcal{Q}^{\alpha\times\beta}$ and the quantized vector $\overline{\boldsymbol{g}}(k) \in \mathcal{Q}^{\beta\times 1}$ be mapped element-wise by* (3.12)*, which gives $\Gamma(\overline{\boldsymbol{T}})$ and $\Gamma(\overline{\boldsymbol{g}}(k))$. The inverse mapping function is given by* (3.13)*. Then*

$$\Gamma^{-1}\Big(\Gamma(\overline{\boldsymbol{T}})\Gamma\big(\overline{\boldsymbol{g}}(k)\big)\Big) = \overline{\boldsymbol{T}}\overline{\boldsymbol{g}}(k) \tag{3.70}$$

Proof. Assume that the matrix $\boldsymbol{T}$ and the vector $\boldsymbol{g}(k)$ are element-wise quantized by (3.11), which yields

$$\overline{\boldsymbol{T}} = Q(\boldsymbol{T}) = \begin{bmatrix} Q(T_{11}) & \cdots & Q(T_{1\beta}) \\ \vdots & \ddots & \vdots \\ Q(T_{\alpha 1}) & \cdots & Q(T_{\alpha\beta}) \end{bmatrix} = \begin{bmatrix} \overline{T}_{11} & \cdots & \overline{T}_{1\beta} \\ \vdots & \ddots & \vdots \\ \overline{T}_{\alpha 1} & \cdots & \overline{T}_{\alpha\beta} \end{bmatrix} \tag{3.71}$$

and

$$\overline{\boldsymbol{g}}(k) = Q(\boldsymbol{g}(k)) = \begin{bmatrix} Q(g_1(k)) \\ \vdots \\ Q(g_\beta(k)) \end{bmatrix} = \begin{bmatrix} \overline{g}_1(k) \\ \vdots \\ \overline{g}_\beta(k) \end{bmatrix} \tag{3.72}$$

Let the vector $\overline{\boldsymbol{\nu}}(k)$ be defined as

$$\overline{\boldsymbol{\nu}}(k) = \Gamma(\overline{\boldsymbol{T}})\Gamma\big(\overline{\boldsymbol{g}}(k)\big) \tag{3.73}$$

The i-th entry $\overline{\nu}_i(k)$ of the vector $\overline{\boldsymbol{\nu}}(k)$ is obtained by the matrix-vector product $\Gamma(\overline{\boldsymbol{T}})\Gamma(\overline{\boldsymbol{g}}(k))$ as

$$\overline{\nu}_i(k) = \sum_{j=1}^{\beta} \Gamma(\overline{T}_{ij})\Gamma(\overline{g}_j(k)), \tag{3.74}$$

where $i = 1, 2, \cdots, \alpha$, $\overline{T}_{ij}$ denotes the entry in the i-th row and the j-th column of the matrix $\overline{\boldsymbol{T}}$ and $\overline{g}_j(k)$ denotes the j-th entry in the column vector $\overline{\boldsymbol{g}}(k)$. Define a Heaviside function

$$\sigma(z) = \begin{cases} 1, & \text{if } z \geq 0 \\ 0, & \text{if } z < 0 \end{cases} \tag{3.75}$$

According to (3.12), there is

$$\begin{aligned} \overline{\nu}_i(k) &= \sum_{j=1}^{\beta} \Gamma(\overline{T}_{ij})\Gamma(\overline{g}_j(k)) \\ &= \sum_{j=1}^{\beta} (2^{\lambda_2}\overline{T}_{ij} \bmod \mu)(2^{\lambda_2}\overline{g}_j(k) \bmod \mu) \end{aligned} \tag{3.76}$$

As $\overline{T}_{ij} \in \mathcal{Q}$ and $\overline{g}_j(k) \in \mathcal{Q}$, both $2^{\lambda_2}\overline{T}_{ij}$ and $2^{\lambda_2}\overline{g}_j(k)$ are integers in the interval $[-2^{\lambda_1+\lambda_2}, 2^{\lambda_1+\lambda_2})$. Since $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1} + 1$ and $\beta \geq 1$ is an integer, $\lambda_1 \in \mathbb{N}$, $\lambda_2 \in \mathbb{N}$, there is

$$-\mu < 2^{\lambda_2}\overline{T}_{ij} < \mu, \quad -\mu < 2^{\lambda_2}\overline{g}_j(k) < \mu \tag{3.77}$$

It gives

$$\begin{aligned} 2^{\lambda_2}\overline{T}_{ij} \bmod \mu &= \begin{cases} 2^{\lambda_2}\overline{T}_{ij}, & \text{if } \overline{T}_{ij} \geq 0 \\ \mu + 2^{\lambda_2}\overline{T}_{ij}, & \text{if } \overline{T}_{ij} < 0 \end{cases} \\ 2^{\lambda_2}\overline{g}_j(k) \bmod \mu &= \begin{cases} 2^{\lambda_2}\overline{g}_j(k), & \text{if } \overline{g}_j(k) \geq 0 \\ \mu + 2^{\lambda_2}\overline{g}_j(k), & \text{if } \overline{g}_j(k) < 0 \end{cases} \end{aligned} \tag{3.78}$$

With the help of the Heaviside function σ defined in (3.75), we have

$$\begin{aligned} 2^{\lambda_2}\overline{T}_{ij} \bmod \mu &= \big(1 - \sigma(\overline{T}_{ij})\big)\mu + 2^{\lambda_2}\overline{T}_{ij} \\ 2^{\lambda_2}\overline{g}_j(k) \bmod \mu &= \Big(1 - \sigma\big(\overline{g}_j(k)\big)\Big)\mu + 2^{\lambda_2}\overline{g}_j(k) \end{aligned} \tag{3.79}$$

Substituting (3.79) into (3.76), we get

$$\begin{aligned}\overline{\nu}_i(k) &= \sum_{j=1}^{\beta}\big[\big(1-\sigma(\overline{T}_{ij})\big)\mu + 2^{\lambda_2}\overline{T}_{ij}\big]\big[\big(1-\sigma\big(\overline{g}_j(k)\big)\big)\mu + 2^{\lambda_2}\overline{g}_j(k)\big] \\ &= \sum_{j=1}^{\beta}\big(1-\sigma(\overline{T}_{ij})\big)\big(1-\sigma\big(\overline{g}_j(k)\big)\big)\mu^2 + \sum_{j=1}^{\beta}\big(1-\sigma(\overline{T}_{ij})\big)\mu 2^{\lambda_2}\overline{g}_j(k) \\ &\quad + \sum_{j=1}^{\beta}\big(1-\sigma(\overline{g}_j(k))\big)\mu 2^{\lambda_2}\overline{T}_{ij} + \sum_{j=1}^{\beta}2^{2\lambda_2}\overline{T}_{ij}\overline{g}_j(k)\end{aligned} \tag{3.80}$$

Then

$$\overline{\nu}_i(k) \bmod \mu = \big(\sum_{j=1}^{\beta}2^{2\lambda_2}\overline{T}_{ij}\overline{g}_j(k)\big) \bmod \mu \tag{3.81}$$

As mentioned before,

$$\begin{aligned}2^{\lambda_2}\overline{T}_{ij} &\in [-2^{\lambda_1+\lambda_2},\, 2^{\lambda_1+\lambda_2}) \\ 2^{\lambda_2}\overline{g}_j(k) &\in [-2^{\lambda_1+\lambda_2},\, 2^{\lambda_1+\lambda_2})\end{aligned} \tag{3.82}$$

it holds

$$2^{2\lambda_2}\overline{T}_{ij}\overline{g}_j(k) = 2^{\lambda_2}\overline{T}_{ij}2^{\lambda_2}\overline{g}_j(k) \in (-2^{2(\lambda_1+\lambda_2)},\, 2^{2(\lambda_1+\lambda_2)}] \tag{3.83}$$

and thus

$$\overline{\nu}_i(k) = \sum_{j=1}^{\beta}2^{2\lambda_2}\overline{T}_{ij}\overline{g}_j(k) \in (-\beta 2^{2(\lambda_1+\lambda_2)},\, \beta 2^{2(\lambda_1+\lambda_2)}] \tag{3.84}$$

Recall that $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1}+1$ and $\beta \geq 1$ is an integer, $\lambda_1 \in \mathbb{N}$, $\lambda_2 \in \mathbb{N}$. Then $\frac{1}{2}\mu = \beta 2^{2(\lambda_1+\lambda_2)} + \frac{1}{2}$, from which we can see that

$$0 < \beta 2^{2(\lambda_1+\lambda_2)} < \frac{1}{2}\mu \tag{3.85}$$

From (3.81) and (3.85), we obtain

$$\overline{\nu}_i(k) \bmod \mu = \begin{cases}\mu + \overline{\nu}_i(k) \in (\frac{1}{2}\mu,\, \mu), & \text{if } \overline{\nu}_i(k) \in (-\beta 2^{2(\lambda_1+\lambda_2)},\, 0) \\ \overline{\nu}_i(k) \in [0\,, \frac{1}{2}\mu), & \text{if } \overline{\nu}_i(k) \in [0,\, \beta 2^{2(\lambda_1+\lambda_2)}]\end{cases} \tag{3.86}$$

Considering the inverse mapping function (3.13), it yields

$$\begin{aligned}\Gamma^{-1}(\overline{\nu}_i(k)) &= \begin{cases}\frac{1}{2^{2\lambda_2}}(\overline{\nu}_i(k) \bmod \mu - \mu), & \text{if } \overline{\nu}_i(k) \bmod \mu > \frac{\mu}{2} \\ \frac{1}{2^{2\lambda_2}}(\overline{\nu}_i(k) \bmod \mu), & \text{if } \overline{\nu}_i(k) \bmod \mu \leq \frac{\mu}{2}\end{cases} \\ &= \begin{cases}\frac{1}{2^{2\lambda_2}}\big(\mu + \overline{\nu}_i(k) - \mu\big), & \text{if } \overline{\nu}_i(k) \bmod \mu > \frac{\mu}{2} \\ \frac{1}{2^{2\lambda_2}}\overline{\nu}_i(k), & \text{if } \overline{\nu}_i(k) \bmod \mu \leq \frac{\mu}{2}\end{cases} \\ &= \frac{1}{2^{2\lambda_2}}\overline{\nu}_i(k) = \frac{1}{2^{2\lambda_2}}\sum_{j=1}^{\beta}2^{2\lambda_2}\overline{T}_{ij}\overline{g}_j(k) = \sum_{j=1}^{\beta}\overline{T}_{ij}\overline{g}_j(k)\end{aligned} \tag{3.87}$$

As (3.87) holds for any $i = 1, 2, \cdots, \alpha$, there is

$$\Gamma^{-1}(\overline{\boldsymbol{\nu}}(k)) = \overline{\boldsymbol{T}}\overline{\boldsymbol{g}}(k) \tag{3.88}$$

By substituting (3.73) into (3.88), it is clear that (3.70) holds. □

Theorem 5 shows that, if the mapping function (3.12) and the inverse mapping (3.13) are used pairwise, then there is no approximation error caused by the mapping between quantized values and integer values of the system matrices $\overline{\boldsymbol{T}}$ and the signals $\overline{\boldsymbol{g}}(k)$.

3.6.2 Stability of the closed-loop system

The quantization function $Q(\zeta)$ given in (3.11) transforms real values ζ into quantized values $\overline{\zeta}$ so that the controller parameters and the signals transmitted over the network can be encrypted. However, the quantization function $Q(\zeta)$ causes some quantization error, which affects the behaviour of the encrypted cloud-based control system. In this subsection, the influence of the quantization error on the stability of the closed-loop system will be analyzed for the case when a dynamic output feedback controller is encrypted.

In order to illustrate the basic idea and for the sake of clarity, in the following derivation it is assumed that the plant in (2.1) is simplified by $\boldsymbol{d}(k) = \boldsymbol{0}$ and $\boldsymbol{D} = \boldsymbol{O}$.

The dynamics of the system can be equivalently rewritten as

$$\begin{aligned}\begin{bmatrix}\boldsymbol{x}_s(k+1)\\ \boldsymbol{x}(k+1)\end{bmatrix} &= \begin{bmatrix}\boldsymbol{O} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{A}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}_s(k)\\ \boldsymbol{x}(k)\end{bmatrix} + \begin{bmatrix}\boldsymbol{I} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{B}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}_s(k+1)\\ \boldsymbol{u}(k)\end{bmatrix}\\ \begin{bmatrix}\boldsymbol{x}_s(k)\\ \boldsymbol{y}(k)\end{bmatrix} &= \begin{bmatrix}\boldsymbol{I} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{C}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}_s(k)\\ \boldsymbol{x}(k)\end{bmatrix}\end{aligned} \tag{3.89}$$

where the matrix $\boldsymbol{I}$ and the matrix $\boldsymbol{O}$ denote, respectively, an identity matrix and a zero matrix of compatible dimensions. Since the controller parameters $\boldsymbol{A}_s, \boldsymbol{B}_s, \boldsymbol{C}_s, \boldsymbol{D}_s$, the state vector of the controller $\boldsymbol{x}_s(k)$ and the sensor output vector $\boldsymbol{y}(k)$ need to be quantized by (3.11) element-wise before they are mapped and encrypted, it yields

$$\begin{bmatrix}\boldsymbol{x}_s(k+1)\\ \boldsymbol{u}(k)\end{bmatrix} = \begin{bmatrix}\overline{\boldsymbol{A}}_s & \overline{\boldsymbol{B}}_s\\ \overline{\boldsymbol{C}}_s & \overline{\boldsymbol{D}}_s\end{bmatrix}\begin{bmatrix}\overline{\boldsymbol{x}}_s(k)\\ \overline{\boldsymbol{y}}(k)\end{bmatrix} \tag{3.90}$$

Taking into account (3.89), the dynamics of the closed-loop system is given by

$$\begin{aligned}\boldsymbol{x}_\Sigma(k+1) &= \boldsymbol{A}_\Sigma\boldsymbol{x}_\Sigma(k) + \boldsymbol{B}_\Sigma\overline{\boldsymbol{g}}(k)\\ \boldsymbol{g}(k) &= \boldsymbol{C}_\Sigma\boldsymbol{x}_\Sigma(k)\end{aligned} \tag{3.91}$$

where

$$\begin{aligned}&\boldsymbol{x}_\Sigma(k) = \begin{bmatrix}\boldsymbol{x}_s(k)\\ \boldsymbol{x}(k)\end{bmatrix},\ \boldsymbol{g}(k) = \begin{bmatrix}\boldsymbol{x}_s(k)\\ \boldsymbol{y}(k)\end{bmatrix},\ \overline{\boldsymbol{g}}(k) = \begin{bmatrix}\overline{\boldsymbol{x}}_s(k)\\ \overline{\boldsymbol{y}}(k)\end{bmatrix}\\ &\boldsymbol{A}_\Sigma = \begin{bmatrix}\boldsymbol{O}\ \boldsymbol{O}\\ \boldsymbol{O}\ \boldsymbol{A}\end{bmatrix},\ \boldsymbol{B}_\Sigma = \begin{bmatrix}\boldsymbol{I}\ \boldsymbol{O}\\ \boldsymbol{O}\ \boldsymbol{B}\end{bmatrix}\begin{bmatrix}\overline{\boldsymbol{A}}_s\ \overline{\boldsymbol{B}}_s\\ \overline{\boldsymbol{C}}_s\ \overline{\boldsymbol{D}}_s\end{bmatrix},\ \boldsymbol{C}_\Sigma = \begin{bmatrix}\boldsymbol{I}\ \boldsymbol{O}\\ \boldsymbol{O}\ \boldsymbol{C}\end{bmatrix}\end{aligned} \tag{3.92}$$

Let the vector $\boldsymbol{\Delta}_{\boldsymbol{g}}(k)$ be the quantization error defined as

$$\boldsymbol{\Delta}_g(k) = \overline{\boldsymbol{g}}(k) - \boldsymbol{g}(k) = \overline{\boldsymbol{g}}(k) - \boldsymbol{C}_\Sigma\boldsymbol{x}_\Sigma(k) \tag{3.93}$$

Then the closed-loop system (3.91) can be equivalently rewritten as

$$\begin{aligned} \boldsymbol{x}_\Sigma(k+1) &= \boldsymbol{A}_\Sigma \boldsymbol{x}_\Sigma(k) + \boldsymbol{B}_\Sigma\big(\boldsymbol{\Delta}_g(k) + \boldsymbol{C}_\Sigma \boldsymbol{x}_\Sigma(k)\big) \\ &= (\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\boldsymbol{x}_\Sigma(k) + \boldsymbol{B}_\Sigma \boldsymbol{\Delta}_g(k) \end{aligned} \tag{3.94}$$

Next, the set invariance theory, which provides stability conditions for control systems with bounded disturbances (see, for instance, Gayek (1991), Rakovic et al. (2005), and Wang and Ong (2011)), will be exploited to analyze the stability of the closed-loop system.

Recall that after the quantization the signals take values in a finite set $\mathcal{Q} = \{-2^{\lambda_1}, -2^{\lambda_1} + 2^{-\lambda_2}, \cdots, 2^{\lambda_1} - 2^{-\lambda_2}\}$, where λ_1 and λ_2 represents, respectively, the range and the resolution of the quantization. Let the set of the quantization error $\boldsymbol{\Delta}_g(k)$ be denoted by

$$\mathcal{G} = \{\boldsymbol{\Delta}_g(k) \in \mathbb{R}^{\beta \times 1} |\, \|\boldsymbol{\Delta}_g(k)\|_\infty \leq 2^{-\lambda_2}\} \tag{3.95}$$

and the reachable set of the state $\boldsymbol{x}_\Sigma(k)$ be denoted by

$$\boldsymbol{x}_\Sigma(k) \in \mathcal{X}_\Sigma = \{\boldsymbol{x}_\Sigma(k) \in \mathbb{R}^{(n_s+n_x)\times 1} |\, \|\boldsymbol{x}_\Sigma(k)\|_\infty \leq \chi\} \tag{3.96}$$

with $0 < \chi < 2^{\lambda_1}$. Recall that a robust positively invariant (RPI) set is a subset of the state space where all trajectories starting from within the subset will remain in this subset. According to Darup et al. (2019), if there exists a non-empty RPI set $\mathcal{F}$ that satisfies

$$\emptyset \subset \mathcal{F} \subseteq \mathcal{X}_\Sigma \text{ and } (\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\mathcal{F} + \boldsymbol{B}_\Sigma \mathcal{G} \subseteq \mathcal{F} \tag{3.97}$$

and the matrix

$$\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma = \begin{bmatrix} \overline{\boldsymbol{A}}_s & \overline{\boldsymbol{B}}_s \boldsymbol{C} \\ \boldsymbol{B}\overline{\boldsymbol{C}}_s & \boldsymbol{A} + \boldsymbol{B}\overline{\boldsymbol{D}}_s \boldsymbol{C} \end{bmatrix} \tag{3.98}$$

is Schur stable, then the closed-loop system in (3.94) is stable. According to Rakovic et al. (2005), each trajectory that starts in the largest set $\mathcal{F}$ satisfying (3.97) converges to the RPI set $\mathcal{S} \subseteq \mathcal{X}_\Sigma$. It yields

$$\mathcal{S} = \bigoplus_{k=0}^{K} (\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)^k \boldsymbol{B}_\Sigma \mathcal{G} \tag{3.99}$$

where K is a sufficiently large integer so that $\mathcal{S}$ is a convex, closed and bounded RPI set. If K tends to infinity, then $\mathcal{S}$ converges to the minimal RPI set denoted by $\mathcal{S}_\infty$. Since in general it is difficult to obtain an explicit characterization of the minimal RPI set $\mathcal{S}_\infty$ (Gayek, 1991), the results given by Wang and Ong (2011) are exploited to find the stability conditions for the closed-loop system (3.94).

Recall that a support function of a non-empty convex closed set is giving the distance of the supporting hyperplane from the origin and the upper bound of the set. According to Wang and Ong (2011), the support function $h_S(\mathbf{1})$ of the RPI set $\mathcal{S}$ (3.99) can be calculated by

$$h_\mathcal{S}(\mathbf{1}) = \sum_{k=0}^{K} h_\mathcal{G}\Big(\big((\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)^k \boldsymbol{B}_\Sigma\big)^T \mathbf{1}\Big) \tag{3.100}$$

where $\mathbf{1}$ denotes a column vector of compatible dimensions and $h_{\mathcal{G}}$ denotes the support function of the set $\mathcal{G}$. Similar as given by Wang and Ong (2011), it can be derived that the support function $h_{\mathcal{G}}$ in (3.100) is upper bounded by

$$\begin{aligned} & h_{\mathcal{G}}\Big(\big((\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)^k \boldsymbol{B}_\Sigma\big)^T \mathbf{1}\Big) \\ & \quad \leq \|\mathbf{1}\|_2 \max_{\boldsymbol{\Delta}_g(k)\in\mathcal{G}} \|\boldsymbol{\Delta}_g(k)\|_2 \big(\|(\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\boldsymbol{B}_\Sigma\|_2\big)^k \\ & \quad \leq \sqrt{(n_s+n_x)\beta}\, 2^{-\lambda_2} \big(\|(\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\boldsymbol{B}_\Sigma\|_2\big)^k \end{aligned} \tag{3.101}$$

Substituting (3.101) into (3.100), we get

$$h_{\mathcal{S}}(\mathbf{1}) \leq \sqrt{(n_s+n_x)\beta}\, 2^{-\lambda_2} \sum_{k=0}^{K} \big(\|(\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\boldsymbol{B}_\Sigma\|_2\big)^k \tag{3.102}$$

Recall that $\boldsymbol{x}_\Sigma(k)$ is upper bounded by χ and $0 < \chi < 2^{\lambda_1}$. Thus, $\mathcal{S} \subseteq \mathcal{X}_\Sigma$, if

$$\sqrt{(n_s+n_x)\beta}\, 2^{-\lambda_2} \sum_{k=0}^{K} \big(\|(\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma)\boldsymbol{B}_\Sigma\|_2\big)^k \leq \chi < 2^{\lambda_1} \tag{3.103}$$

In summary, despite the existence of the quantization error $\boldsymbol{\Delta}_g(k)$, the closed-loop system is stable, if λ_1 and λ_2 are chosen large enough so that $\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma$ is Schur stable and the condition (3.103) holds. Note that the closed-loop stability is only influenced by the range λ_1 and the resolution λ_2 of the mapping function, while the parameters of the RHE scheme ρ, θ, p, ψ and γ have no influence on the closed-loop stability.

3.7 Simulation example

In this section, an example will be given to show the vulnerability of cloud-based control systems encrypted by the somewhat HE scheme given in Section 3.1 to covert attacks. Then, the ability of resilience of the RHE scheme proposed in Section 3.3 to covert attacks will be shown. In the simulation, the quadruple-tank system, the monitoring system and the dynamic output feedback controller introduced in Section 2.3 will be used.

3.7.1 Somewhat HE scheme

In this subsection, the behaviour of the cloud-based control system will be investigated, if the somewhat HE scheme in Section 3.1 will be used. The somewhat HE scheme given by Dyer et al. (2019) applied to the dynamic output feedback controller will be implemented as shown in Fig. 3.1.

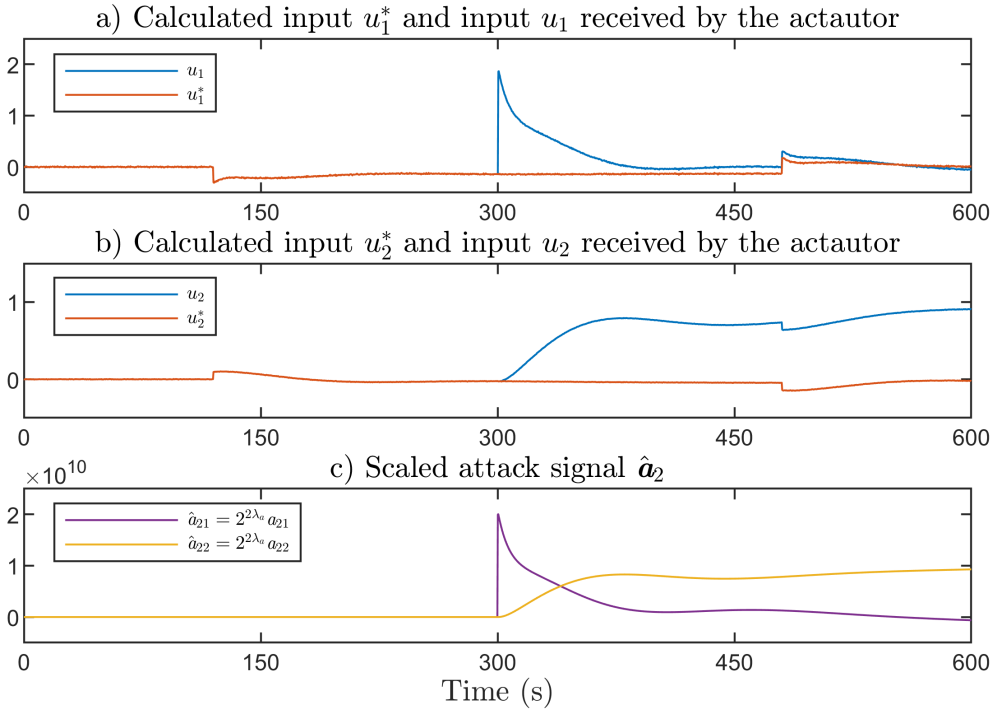

Figure 3.3: Input channels under covert attack with the somewhat HE scheme given by Dyer et al. (2019)

The parameters of the somewhat HE scheme are selected as follow. To figure out the minimum requirements to satisfy condition (3.103) so that the closed-loop system stability can be ensured, the plaintext space $M = 2^{\lambda_1+\lambda_2+1}$ is required. Due to the physical limitations of the plant, the maximal signal value in the system is smaller than 15. Thus, select $\lambda_1 = 4$. It can be checked that (3.103) is satisfied, if $\lambda_2 = 16$ and $M = 2^{21}$. As a result, $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1} + 1 = 4 \times 2^{41} + 1$. Based on (2.6), (2.7) and (3.92), it can be checked that $\boldsymbol{A}_\Sigma + \boldsymbol{B}_\Sigma \boldsymbol{C}_\Sigma$ is Schur stable. Recall that the parameter matrix $\boldsymbol{T} \in \mathbb{R}^{\alpha \times \beta}$ of the dynamic output feedback controller is of dimensions $\alpha \times \beta$, where $\alpha = 4$ and $\beta = 4$.

At first, the security level κ is required. According to National Institute of Standards and Technology (2020), the commonly used security levels κ are chosen from the set $\{80, 112, 128, 192, 256\}$. In the simulation, the security level κ is chosen as $\kappa = 80$. Then, the integer θ is selected from the interval $(2^{95}, 2^{96})$ to satisfy condition (3.10a). In order to decrypt later correctly and prevent factorisation attacks, the bit-size ψ of the prime number p is $\psi = 384$ to satisfy simultaneously condition (3.10b) and condition (3.68a). As the ciphertext space γ is given by $\lceil \log_2(z_0) \rceil = \lceil \log_2(qp) \rceil$, where q is a ψ'-bit prime number, the ciphertexts space is $\gamma = \psi + \psi'$. Finally, we can make sure that condition (3.68b) holds by selecting $\gamma = 2934$ and $\psi' = \gamma - \psi = 2550$.

The parameter matrix $\boldsymbol{T}$ of the controller is mapped by (3.11), (3.12) and then encrypted by (3.5). Due to the bit-size $\gamma = 2934$ of the ciphertexts, the controller parameters encrypted by the somewhat HE scheme are large integers and thus omitted here.

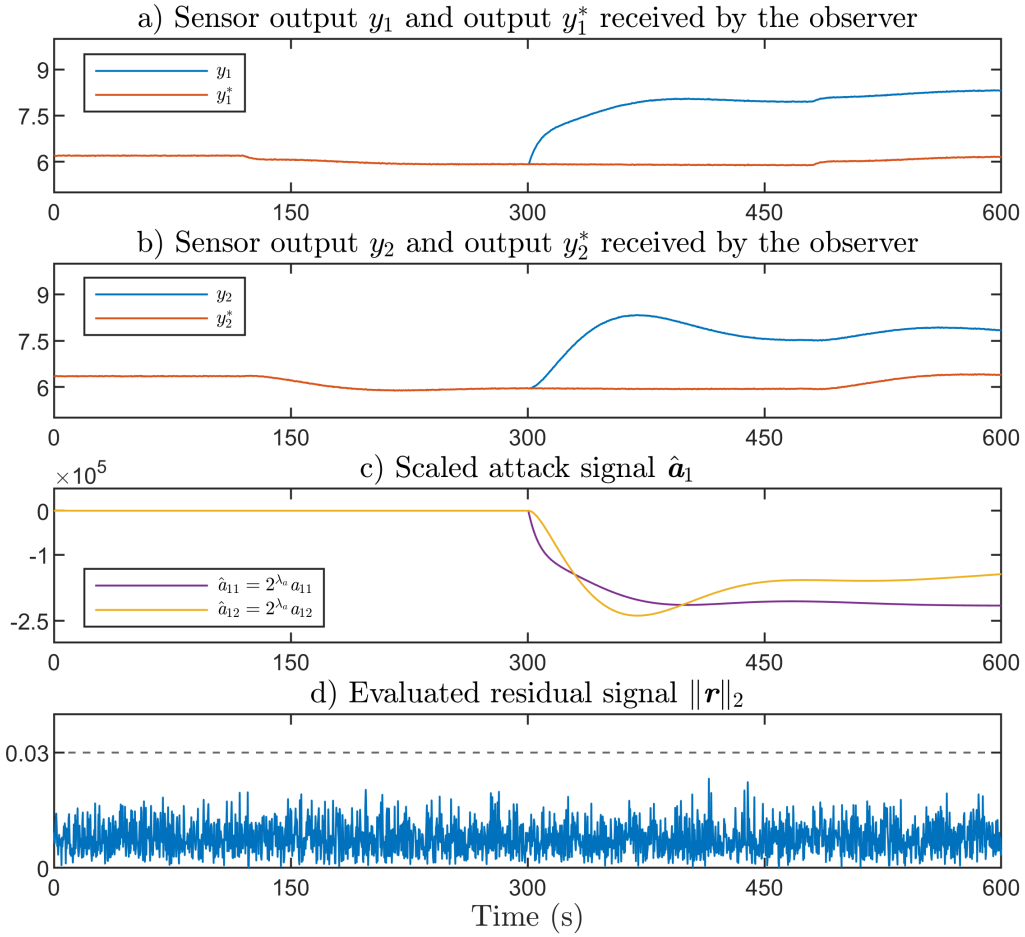

Figure 3.4: Output channels under covert attack with the somewhat HE scheme given by Dyer et al. (2019)

Assume that a covert attack in the form of (3.33) is carried out on the cloud-based control system encrypted by the somewhat HE scheme given by Dyer et al. (2019). The aim of the adversary is to raise the liquid level in the first tank, i.e. $\boldsymbol{w}_a = [2\ 0]^T cm$. To reach this goal, a dynamic output feedback controller in the form of (2.2) with the parameters (2.7) is utilized. As mentioned in Section 3.2.2, the adversary may use an attack factor λ_a to adjust its influence on the plant (2.6). Assume that the attacker uses the attack factor $\lambda_a = 16$.

During the simulation, the scaled attack signals $\hat{\boldsymbol{a}}_1(k)$ and $\hat{\boldsymbol{a}}_2(k)$ are imposed on, respectively, the encrypted sensor output signals and the encrypted control input signals (i.e. $\hat{\boldsymbol{a}}_1(k) = 2^{\lambda_a}\boldsymbol{a}_1(k) = 2^{\lambda_a}[0\,0\,a_{11}(k)\,a_{12}(k)]^T$ and $\hat{\boldsymbol{a}}_2(k) = 2^{2\lambda_a}\boldsymbol{a}_2(k) = 2^{2\lambda_a}[0\,0\,a_{21}(k)\,a_{22}(k)]^T$) at $k = 300s$, while there is no attack on the encrypted state vectors. From Fig. 3.3a and Fig. 3.3b it can be seen that the scaled attack signal $\hat{\boldsymbol{a}}_2(k) = 2^{2\lambda_a}\boldsymbol{a}_2(k)$ (see Fig. 3.3c) imposed on the ciphertext $\boldsymbol{c}_r^*(k)$ leads to an obvious change in the control input signals $\boldsymbol{u}(k)$ received by the actuators. Due to large ciphertexts, the ciphertext $\boldsymbol{w}_r(k)$ and the ciphertext $\boldsymbol{c}_r^*(k)$ obtained after the evaluation process of the controller can not be displayed here. The influence of the attack $\hat{\boldsymbol{a}}_2(k) = 2^{2\lambda_a}\boldsymbol{a}_2(k)$ is compensated by the simultaneous injection of

$\hat{\boldsymbol{a}}_1(k) = 2^{\lambda_a}\boldsymbol{a}_1(k)$ (see Fig. 3.4c) into the ciphertext $\boldsymbol{w}_r(k)$, where $\boldsymbol{a}_1(k)$ satisfies $\boldsymbol{A}_1(z) = -\boldsymbol{G}(z)\boldsymbol{A}_2(z) = -(\boldsymbol{D} + \boldsymbol{C}(z\boldsymbol{I} - \boldsymbol{A})^{-1}\boldsymbol{B})\boldsymbol{A}_2(z)$. As can be seen from Fig. 3.4d, no change can be observed in the evaluated residual signal $\|\boldsymbol{r}\|_2$ before and after the attack and the threshold δ_r is never exceeded. The covert attack $\hat{\boldsymbol{a}}_1(k)$ and $\hat{\boldsymbol{a}}_2(k)$ on the encrypted cloud-based control system is invisible to the monitoring system, even if the parameter matrix of the controller and the signals transmitted over the network are encrypted.

3.7.2 RHE scheme

Now, the simulation results of the cloud-based control system encrypted by the RHE scheme given in Section 3.3 are presented.

The range λ_1 and the resolution λ_2 of the mapping function are the same as in the somewhat HE scheme, i.e. $\lambda_1 = 4$ and $\lambda_2 = 16$. Thus, the bound M of the plaintexts is given by $M = 2^{21}$ and $\mu = 4 \times 2^{41} + 1$. The security level κ is chosen to be the same as in the somewhat HE scheme, i.e. $\kappa = 80$. The bit-size ρ of the noises s_{ij} in the

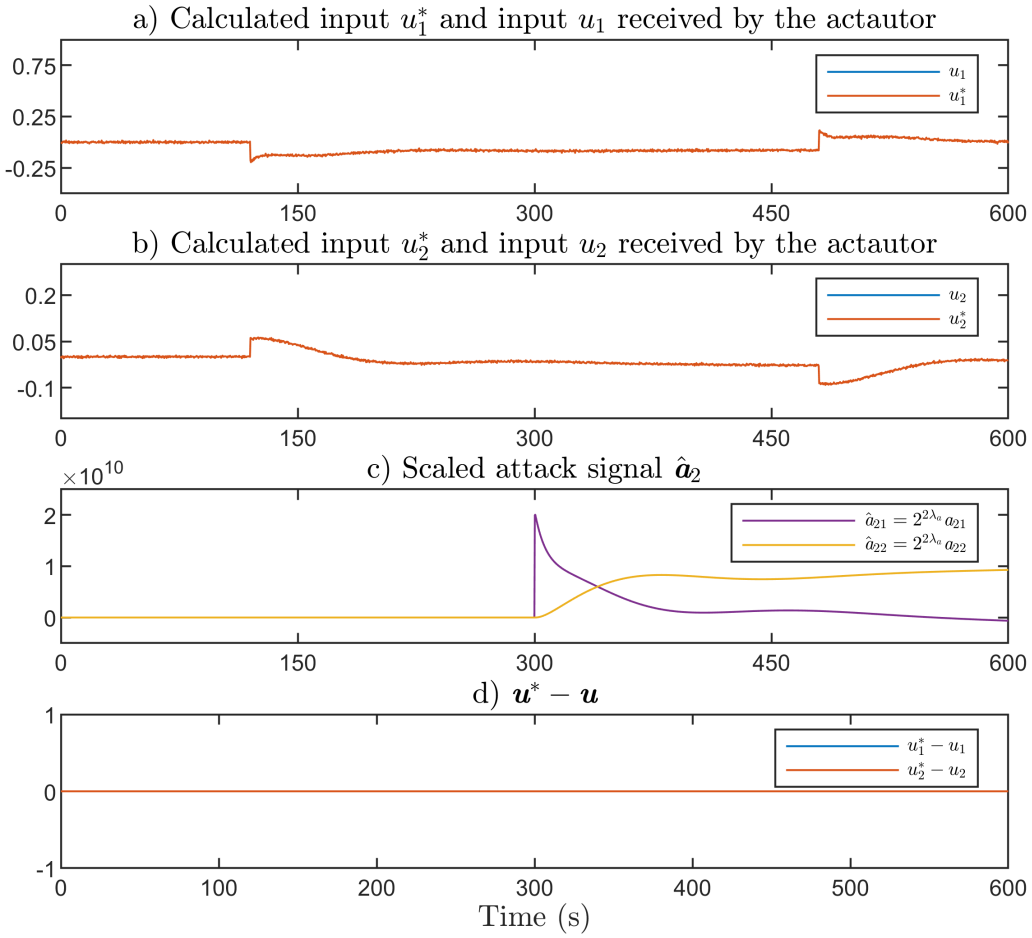

Figure 3.5: Input channels under covert attack with the RHE scheme

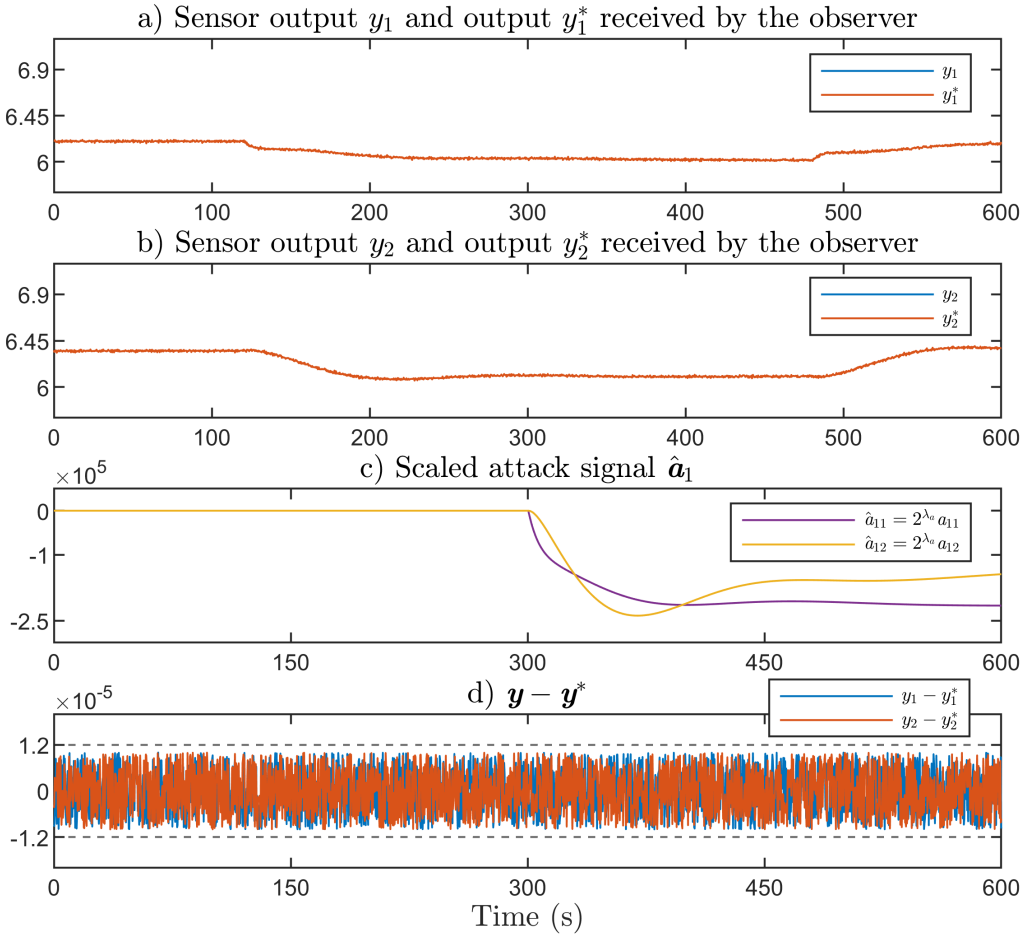

Figure 3.6: Output channels under covert attack with the RHE scheme

encrypted matrix (3.34) and s_j in the encrypted vector (3.35) are set as $\rho = 2\kappa = 160$ in order to satisfy (3.65). Then, the integer θ is selected from the interval $(2^{207}, 2^{208})$ to satisfy condition (3.39b). The bit-size ψ of the prime number p is $\psi = 505$ to satisfy simultaneously condition (3.39a) and condition (3.68a). After that, the bit-size γ of the ciphertext space is selected as $\gamma = 276160$ to satisfy simultaneously condition (3.68b) and condition (3.69). The integer q is a sample drawn from a uniform distribution over the interval $[0, \lfloor 2^\gamma / p \rfloor]$ so that $q > p$, q can not be factorized into integers smaller than 2^ψ and $qp \geq 2^{\gamma-1}$. Finally, the divisor z_0 in the modulo operations is set as $z_0 = qp$.

During the simulation, the attack signals $\hat{\boldsymbol{a}}_1(k)$ and $\hat{\boldsymbol{a}}_2(k)$ are exactly the same as in the last subsection (see Fig. 3.5c and Fig. 3.6c). The simulation results show that the influence of the attack signals $\hat{\boldsymbol{a}}_1(k)$ and $\hat{\boldsymbol{a}}_2(k)$ on, respectively, $\boldsymbol{y}(k)$ and $\boldsymbol{u}^*(k)$ has disappeared (see Fig. 3.5a,b and Fig. 3.6a,b), which shows the resilience of the RHE scheme to the covert attack. As the attack $\hat{\boldsymbol{a}}_2(k)$ has no influence on the control input signals $\boldsymbol{u}(k)$ received by the actuators, the control input signals $\boldsymbol{u}(k)$ received by the actuators and the control input signals $\boldsymbol{u}^*(k)$ received by the monitoring system are exactly the same, i.e. $\forall k,\ u_i^*(k) - u_i(k) = 0$, where $i = 1, 2$ (see Fig. 3.5d). The slight difference between the sensor output signals $\boldsymbol{y}(k)$ and the

sensor output signals $\boldsymbol{y}^*(k)$ received by the monitoring system (see Fig. 3.6d) is only due to the transformation (3.11) between real values and quantized values. In Fig. 3.6d, it can be checked that $\forall k$, $|y_i(k) - y_i^*(k)| < 1.2 \times 10^{-5}$, where $i = 1, 2$. The quantization error can be further reduced by increasing the resolution λ_2.

In summary, the influence of the covert attack on the cloud-based control system encrypted by the RHE scheme is neutralized and the encrypted cloud-based control system is resilient to the covert attack.

3.8 Discussion

In this chapter, the vulnerability of cloud-based control systems encrypted by the somewhat HE scheme given by Dyer et al. (2019) to covert attacks is investigated. Even though the somewhat HE scheme can guarantee the confidentiality of the signals transmitted over the network and the confidentiality of the parameter matrix of the controller, it can not prevent an adversary from manipulating the ciphertexts. To cope with this problem, the somewhat HE scheme is modified. The proposed RHE scheme is not only able to neutralize the effect of an attack injected into the ciphertexts but also satisfies the security requirement of IND-CPA. Thus, a control system can still operate even if an attack takes place. To achieve it, there are four key steps. At first, the plaintext and the random values in the somewhat HE scheme (Dyer et al., 2019) are interchanged. Secondly, the decryption step of the somewhat HE scheme is modified to achieve the homomorphicity with respect to the matrix-vector product. Thirdly, the controller should be brought into the form of a matrix-vector product. Finally, the random values in the RHE scheme are selected so that the ciphertexts obtained by the RHE scheme follow the AGCD distribution. Thus, the RHE scheme relies on the hardness assumption of the EF-AGCD problem, which can not be solved in polynomial time by any known attack. After that conditions for the correct decryption in the RHE scheme and the resilience of the RHE scheme to additive attacks are shown. Then, it is proven that the distribution of the ciphertexts generated by the RHE scheme is computationally indistinguishable from the uniform distribution. That means, the adversary is not able to deduce the plaintexts from the ciphertexts. Therefore, the RHE scheme satisfies IND-CPA. Finally, a procedure for the selection of the parameters in the RHE scheme according to the desired security level is given.

Furthermore, it is shown that the transformation between quantized values and integer values causes no error in the calculation of the matrix-vector product. A condition is derived for the stability of the closed-loop system with a dynamic output feedback controller by considering the quantization error caused by the transformation between real values and quantized values.

The vulnerability of the somewhat HE scheme to covert attacks and the resilience of the RHE scheme to covert attacks is validated with the well-established quadruple-tank process. The simulation results show that an adversary can impose an attack

on the ciphertexts obtained by the standard somewhat HE scheme in such a way that the plant behaviour of the cloud-based control system is influenced while the attack can not be detected by a conventional monitoring system. By encrypting the cloud-based control system with the RHE scheme, the attack imposed on the ciphertexts obtained by the RHE scheme has no effect of the control input signals received by the actuators. That means, the RHE scheme can not only guarantee the confidentiality of the cloud-based control system but also make the cloud-based control system resilient to attacks such as the covert attack. Therefore, the RHE scheme is an useful method to enhance the cyber security of cloud-based control systems.

4 Post-Quantum Security

In this chapter, the post-quantum secure resilient homomorphic encryption (PQS-RHE) scheme will be proposed. The PQS-RHE scheme is not only able to carry out dynamic output feedback controllers with ciphertexts but also is post-quantum secure. Moreover, the PQS-RHE scheme preserves the ability of resilience and can neutralize attacks imposed on the ciphertexts. Thus, a control system can still operate even in case of an attack.

The upcoming post-quantum era will reshape the landscape of HE schemes, because powerful quantum computers may retrieve the secret key from the ciphertexts generated by various HE schemes. For instance, Shor's algorithm carried out on a quantum computer can efficiently solve discrete logarithms and the factorisation problem of large integers (Shor, 1999). Thus, the partially homomorphic encryption (PHE) schemes widely utilized in encrypted control (see, for instance, Kogiso and Fujita (2015), Shoukry et al. (2016), Kishida (2018), Ruan et al. (2019), Farokhi et al. (2016), Cheon et al. (2018), Darup et al. (2018), and Alexandru et al. (2018)), namely the Rivest-Shamir-Adleman (RSA) cryptosystem (Rivest et al., 1978), the ElGamal cryptosystem (Elgamal, 1985) and the Paillier cryptosystem (Paillier, 1999), can be broken by a quantum computer. That means, the control systems encrypted by those PHE schemes become unsecure in the post-quantum era. In principle, HE schemes whose security relies on the learning with errors (LWE) problem (Fan and Vercauteren, 2012; Gentry et al., 2013; Cheon et al., 2017) and the decisional approximate greatest common divisor (AGCD) problem (Lepoint, 2014; Cheon and Stehlé, 2015; Benarroch et al., 2017; Pereira, 2021) can solve this issue as they are regarded as post-quantum secure. However, it remains a challenge to find suitable parameters of an HE scheme to ensure the security against modern cryptographic attacks and simultaneously meet the real-time requirements of cloud-based control systems.

Control systems encrypted by HE schemes that are regarded as post-quantum secure are given by, for instance, Alexandru et al. (2020), Suh and Tanaka (2021), Schlüter et al. (2021), Kim et al. (2023), and Teranishi et al. (2023). To implement a data-driven linear quadratic regulator as described in Alexandru et al. (2020) and reinforcement learning algorithms as outlined in Suh and Tanaka (2021) within an encrypted environment, the Cheon-Kim-Kim-Song (CKKS) cryptosystem given by Cheon et al. (2017) is utilized. The Gentry-Sahai-Waters (GSW) cryptosystem given by Gentry et al. (2013) is employed in Kim et al. (2023) to carry out multiplication and addition of a dynamic output feedback controller with ciphertexts. To avoid decrypting the controller state on the plant side, the pole placement method is used to ensure all entries of the state matrix are integers. Two additional methods for avoiding the decryption of the controller state on the plant side are given

by Schlüter et al. (2021) and Teranishi et al. (2023). In Schlüter et al. (2021), the dynamic output feedback controller is approximated with a finite impulse response (FIR) filter. In Teranishi et al. (2023), the controller is reformulated as an input-output history feedback controller (IOHFC), allowing encrypted computations using the Brakerski/Fan-Vercauteren (BFV) cryptosystem given by Fan and Vercauteren (2012).

In this chapter, it will be investigated how to make the RHE scheme become post-quantum secure without influencing the homomorphism and the resilience. As a result, the PQS-RHE scheme will be developed. The key is to select the divisor in the modulo operations and the noises used in the encryption suitably so that the divisor in the modulo operations and the ciphertexts obtained by the PQS-RHE scheme are samples drawn from an AGCD distribution. As the divisor in the modulo operations selected in this way increases the noise accumulated during encrypted additions and encrypted multiplications, the homomorphic property may be lost. To cope with it, the decomposition technique given by Benarroch et al. (2017) is integrated into the evaluation process of the encrypted controller. In order to prove that the PQS-RHE scheme is post-quantum secure, the decisional AGCD problem will be employed, which is known to be hard to solve even when an adversary has access to a quantum computer (Cheon and Stehlé, 2015; Benarroch et al., 2017; Pereira, 2020; Cominetti and Simplicio, 2020). As it can be shown that the ciphertexts obtained by the PQS-RHE scheme follow an AGCD distribution, to distinguish between the distribution of the ciphertexts got by the PQS-RHE scheme and the uniform distribution is indeed the decisional AGCD problem. Thus, the PQS-RHE scheme can be regarded as post-quantum secure. An approach will be given for selecting the parameters in the PQS-RHE scheme to achieve the desired security levels that are approved for the protection of sensitive information, both for different operating environments and for different time spans according to National Institute of Standards and Technology (2020).

The chapter is organized as follows. The PQS-RHE scheme is presented in Section 4.1. In Section 4.2, the resilience of the PQS-RHE scheme to additive attacks is analyzed. The security analysis and the parameter selection of the PQS-RHE scheme is shown in Section 4.3. Finally, an example of the well-established quadruple-tank system is given in Section 4.4 to show the resilience of the proposed PQS-RHE scheme to additive attacks.

4.1 Post-quantum secure resilient homomorphic encryption

In this subsection, the PQS-RHE scheme will be introduced. Since Shor's algorithm can factorise large integers in polynomial time when a quantum computer becomes practical (Shor, 1999), the divisor $z_0 = qp$ in the modulo operation used in the encryption (3.34)-(3.35) and the evaluation function (3.37) is the crucial vulnerability

of the RHE scheme given in Section 3.3 in the post-quantum era.

The key idea of the new encryption scheme proposed here is to replace the divisor z_0 in the modulo operations with a sample $\overline{z}_0 = s_0 + qp$ drawn from an AGCD distribution and make sure that $\overline{z}_0 \geq 2^{\gamma-1}$ holds. Additionally, the parameters of the new encryption scheme are selected to ensure that the ciphertexts follow an AGCD distribution and simultaneously are within the range of $[0, 2^{\gamma-1})$. In this way, factorisation attacks against the ciphertexts and the divisor $\overline{z}_0$ of the modulo operation can be prevented, even when a quantum computer is utilized.

However, changing the divisor in the modulo operation from $z_0 = qp$ to $\overline{z}_0 = s_0 + qp$ may lead to the loss of the homomorphic property, as shown below. Without loss of generality, assume that $\overline{z}_0$ is big enough so that the matrix $\boldsymbol{F}$ and the vector $\boldsymbol{w}$ are encrypted, respectively, by

$$\begin{aligned} \boldsymbol{F}_c &= RHE.Enc(\boldsymbol{F}, sk) \\ &= (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p) \bmod \overline{z}_0 \\ &= \boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p \end{aligned} \tag{4.1}$$

and

$$\begin{aligned} \boldsymbol{w}_c &= RHE.Enc(\boldsymbol{w}, sk) \\ &= (\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \bmod \overline{z}_0 \\ &= \boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p \end{aligned} \tag{4.2}$$

Substituting $\overline{z}_0 = s_0 + qp$ into (4.1)-(4.2) and (3.37), it yields

$$\begin{aligned} \boldsymbol{c}_\times &= (\boldsymbol{F}_c \boldsymbol{w}_c) \bmod \overline{z}_0 \\ &= \big((\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)\big) \bmod (s_0 + qp) \\ &= (\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p) \\ &\quad - \left\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)}{s_0 + qp} \right\rfloor (s_0 + qp) \end{aligned} \tag{4.3}$$

Note that

$$\boldsymbol{c}_\times \bmod p = \big(\boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) + \theta^2 \boldsymbol{F}\boldsymbol{w} - \mathcal{N} s_0\big) \bmod p \tag{4.4}$$

where

$$\mathcal{N} = \left\lfloor \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)}{s_0 + qp} \right\rfloor \in \mathbb{N}^{\alpha \times 1} \tag{4.5}$$

In order to ensure that the decryption (3.36) still leads to the correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$, the following inequality

$$\left\| \boldsymbol{S}_f \boldsymbol{s}_w + \theta(\boldsymbol{S}_f \boldsymbol{w} + \boldsymbol{F}\boldsymbol{s}_w) - \mathcal{N} s_0 \right\|_\infty < \theta^2 \tag{4.6}$$

needs to hold, so that

$$\boldsymbol{\nu} = RHE.Dec(\boldsymbol{c}_\times, sk)$$

$$= \frac{\boldsymbol{c}_\times \bmod p - (\boldsymbol{c}_\times \bmod p) \bmod \theta^2}{\theta^2}$$
$$= \boldsymbol{F}\boldsymbol{w} \tag{4.7}$$

In order to ensure the security of the new encryption scheme, the divisor $\overline{z}_0$ in the modulo operations must be a sample drawn from an AGCD distribution and $\overline{z}_0 \geq 2^{\gamma-1}$. Moreover, the parameters of the new encryption scheme are chosen so that the ciphertexts obey an AGCD distribution and simultaneously lie in the range of $[0, 2^{\gamma-1})$. Therefore, it can be proven later that the divisor $\overline{z}_0$ of the modulo operations and the ciphertexts obtained by the new encryption scheme are computationally indistinguishable from an uniform distribution. Recall that distinguishing between an AGCD distribution and an uniform distribution is indeed the decisional AGCD problem, as defined in Definition 5. Hence, the new encryption scheme can be regarded as post-quantum secure. However, as all the entries of $\boldsymbol{F}_c$ and $\boldsymbol{w}_c$ are ciphertexts, $\|\boldsymbol{F}_c\|_{max} < 2^{\gamma-1}$, $\|\boldsymbol{w}_c\|_\infty < 2^{\gamma-1}$ and $\overline{z}_0 \geq 2^{\gamma-1}$. There is

$$\left\| \frac{(\boldsymbol{S}_f + \boldsymbol{F}\theta + \boldsymbol{R}_f p)(\boldsymbol{s}_w + \boldsymbol{w}\theta + \boldsymbol{r}_w p)}{s_0 + qp} \right\|_\infty < \frac{\beta 2^{\gamma-1} 2^{\gamma-1}}{2^{\gamma-1}} = \beta 2^{\gamma-1} \tag{4.8}$$

From (4.5) and (4.8) it can be seen that the maximal absolute value of the vector $\mathcal{N}$ could be bigger than the divisor $\overline{z}_0$ in the modulo operations. As θ^2 is in the ciphertext space defined by $\overline{z}_0$, it may happen that $\|\mathcal{N}\|_\infty > \theta^2$, which does not satisfy the condition in (4.6). In this case, the decryption (3.36) would lead to an incorrect result of the matrix-vector product and the encryption (4.1)-(4.2) would lose the homomorphic property.

To cope with this problem and avoid the loss of the homomorphic property, the decomposition technique given by Benarroch et al. (2017) will be employed and can be carried out in two steps.

At first, in order to reduce the maximal value of the entries in the noise $\mathcal{N}$ described by (4.5), the base-b decomposition g_f^{-1} is applied to the encrypted vector $\boldsymbol{w}_c$. The base-b decomposition of the vector $\boldsymbol{w}_c$ is $g_f^{-1}(\boldsymbol{w}_c) = [g_1 \cdots g_{\beta\phi}]^T$, where $\|g_f^{-1}(\boldsymbol{w}_c)\|_\infty < b$ and $\phi = \lceil \log_b(\overline{z}_0) \rceil$. For instance, let $\beta = 2, b = 2$ and $\phi = 3$. Assume that the vector $\boldsymbol{w}_c = [w_{c1}\, w_{c2}]^T = [5\ 7]^T$, then $g_f^{-1}(w_{c1}) = [1\,0\,1]^T$, $g_f^{-1}(w_{c2}) = [1\,1\,1]^T$. As a result, $g_f^{-1}(\boldsymbol{w}_c) = [g_f^{-1}(w_{c1})^T\, g_f^{-1}(w_{c2})^T] = [1\,0\,1\,1\,1\,1]^T$. That means, the vector $\boldsymbol{w}_c$ is transformed to a vector of higher dimension whose entries are all small integers. In order to execute a matrix-vector product with the decomposition technique, the encrypted matrix $\boldsymbol{F}_c$ needs to be reshaped into an equivalent matrix with more columns $\overline{\boldsymbol{F}}_c \in \mathbb{N}^{\alpha \times \beta\phi}$, so that it can be multiplied by $g_f^{-1}(\boldsymbol{w}_c) \in \mathbb{N}^{\beta\phi \times 1}$, i.e. the matrix-vector product is carried out as

$$\boldsymbol{c}_\times = (\overline{\boldsymbol{F}}_c g_f^{-1}(\boldsymbol{w}_c)) \bmod \overline{z}_0 \tag{4.9}$$

then

$$\boldsymbol{c}_\times \bmod p = \left(\overline{\boldsymbol{F}}_c g_f^{-1}(\boldsymbol{w}_c) - \overline{\mathcal{N}} s_0\right) \bmod p \tag{4.10}$$

where

$$\overline{\mathcal{N}} = \left\lfloor \frac{\overline{\boldsymbol{F}}_c g_f^{-1}(\boldsymbol{w}_c)}{s_0 + qp} \right\rceil \in \mathbb{N}^{\alpha \times 1} \tag{4.11}$$

Recall that $\|g^{-1}(\boldsymbol{w}_c)\|_\infty < b$. It yields

$$\left\| \frac{\overline{\boldsymbol{F}}_c g_f^{-1}(\boldsymbol{w}_c)}{s_0 + qp} \right\|_\infty < \frac{2^\gamma b\beta\phi}{2^{\gamma-1}} = 2\beta\phi b \tag{4.12}$$

Recall that the integer β is defined by the dimension of the parameter matrix $\boldsymbol{T} \in \mathbb{R}^{\alpha\times\beta}$ given in (2.3) and usually a small integer and $\phi = \lceil \log_b(\overline{z}_0) \rceil$. Thus, the noise $\overline{\mathcal{N}}$ given in (4.11) can be controlled by the integer b and can be made much smaller than θ^2 so that the correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ could be obtained after the decryption.

Secondly, before the correct matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ can be obtained, the vector $\boldsymbol{w}$ contained in the vector $\boldsymbol{w}_c$ (4.2) needs to be acquired from its base-2 decomposition $g_f^{-1}(\boldsymbol{w}_c)$ before decryption. This can be achieved by integrating the so-called gadget matrix $\boldsymbol{G}_f = \boldsymbol{I}_\beta \otimes \boldsymbol{g}_f^T \in \mathbb{N}^{\beta\times\phi\beta}$ into the encryption (3.34), where $\boldsymbol{g}_f^T = [b^{\phi-1}\, b^{\phi-2} \cdots b\ 1] \in \mathbb{N}^{1\times\phi}$. For instance, in the last example $\beta = 2, b = 2$ and $\phi = 3$, then $\boldsymbol{g}_f^T = [b^2\ b\ 1]^T = [4\ 2\ 1]^T$ and the gadget matrix $\boldsymbol{G}_f$ is

$$\boldsymbol{G}_f = \boldsymbol{I}_2 \otimes \boldsymbol{g}_f^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 4 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 2 & 1 \end{bmatrix} \tag{4.13}$$

The vector $\boldsymbol{w}_c$ can be obtained from its base-2 decomposition $g_f^{-1}(\boldsymbol{w}_c) = [1\,0\,1\,1\,1\,1]^T$ through $\boldsymbol{w}_c = \boldsymbol{G}_f g_f^{-1}(\boldsymbol{w}_c)$. Notice that $\theta^2\boldsymbol{F}\boldsymbol{w} = \theta\boldsymbol{F}\boldsymbol{G}_f g_f^{-1}(\theta\boldsymbol{w})$, where θ is an integer scalar. The correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ can be obtained after decryption (3.36), if the gadget matrix $\boldsymbol{G}_f$ is considered in the encryption of the matrix $\boldsymbol{F}$.

Finally, four functions $\overline{\mathcal{E}} = (PQS.KeyGen,\ PQS.Enc,\ PQS.Dec,\ PQS.Eval)$ can be defined for the proposed PQS-RHE scheme.

Key Generation ($PQS.KeyGen$): At first, select the security parameter κ according to National Institute of Standards and Technology (2020) and choose the parameters $b, \rho, \theta, \psi, \gamma$ as discussed later in Subsection 4.3.2. Then, select a ψ-bit prime number p and sample the integers s_0 and q uniformly from, respectively, $[-2^\rho + 1, 2^\rho - 1]$ and $[0, \lfloor 2^\gamma/p \rfloor]$ so that $s_0 + qp \geq 2^{\gamma-1}$. Finally, let $sk = (\theta, p)$ be the secret key for encryption and decryption and set $\overline{z}_0 = s_0 + qp$.

Encryption ($PQS.Enc$): A matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ is encrypted by

$$\begin{aligned} \overline{\boldsymbol{F}}_c &= PQS.Enc(\boldsymbol{F}, sk) \\ &= (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p) \bmod (s_0 + qp) \\ &= (\overline{\boldsymbol{Z}} + \boldsymbol{F}\boldsymbol{G}_f\theta) \bmod \overline{z}_0 \end{aligned} \tag{4.14}$$

and a vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ is encrypted by

$$\begin{aligned} \overline{\boldsymbol{w}}_c &= PQS.Enc(\boldsymbol{w}, sk) \\ &= (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod (s_0 + qp) \\ &= (\overline{\boldsymbol{z}} + \boldsymbol{w}\theta) \bmod \overline{z}_0 \end{aligned} \tag{4.15}$$

where $\boldsymbol{G}_f = \boldsymbol{I}_\beta \otimes \boldsymbol{g}_f^T \in \mathbb{N}^{\beta \times \beta\phi}$ is the gadget matrix, $\boldsymbol{g}_f^T = [b^{\phi-1}\, b^{\phi-2} \cdots b\, 1] \in \mathbb{N}^{1\times\phi}$, $\phi = \lceil \log_b(2^\gamma) \rceil$ and b is a known integer constrained by $b \geq 2$. All the entries $\overline{s}_{id}$, $\overline{s}_j$ in $\overline{\boldsymbol{S}}_f \in \mathbb{N}^{\alpha\times\beta\phi}, \overline{\boldsymbol{s}}_w \in \mathbb{N}^{\beta\times 1}$ are integers uniformly selected from $\{-2^\rho + 1, \cdots, 2^\rho - 1\}$ and all the entries $\overline{r}_{id}$, $\overline{r}_j$ in $\overline{\boldsymbol{R}}_f \in \mathbb{N}^{\alpha\times\beta\phi}, \overline{\boldsymbol{r}}_w \in \mathbb{N}^{\beta\times 1}$ are integers uniformly selected from $\{0, 1, \cdots, q-1\}$, $i = 1, 2, \cdots, \alpha$, $j = 1, 2, \cdots, \beta$, $d = 1, 2, \cdots, \beta\phi$.

Decryption ($PQS.Dec$): The decryption of an encrypted vector $\overline{\boldsymbol{c}}_\times \in \mathbb{N}^{\alpha\times 1}$ is given by

$$\begin{aligned} \overline{\boldsymbol{\nu}} &= PQS.Dec(\overline{\boldsymbol{c}}_\times, sk) \\ &= \frac{\overline{\boldsymbol{c}}_\times \bmod p - (\overline{\boldsymbol{c}}_\times \bmod p) \bmod \theta^2}{\theta^2} \end{aligned} \tag{4.16}$$

Evaluation ($PQS.Eval$): Let $g_f^{-1}(\overline{\boldsymbol{w}}_c) \in \mathbb{N}^{\beta\phi\times 1}$ denote the base-b decomposition of the ciphertexts $\overline{\boldsymbol{w}}_c$ so that $\overline{\boldsymbol{w}}_c = \boldsymbol{G}_f g_f^{-1}(\overline{\boldsymbol{w}}_c)$ holds. Then the matrix-vector product of the encrypted matrix $\overline{\boldsymbol{F}}_c$ and the encrypted vector $\overline{\boldsymbol{w}}_c$ is

$$\overline{\boldsymbol{c}}_\times = (\overline{\boldsymbol{F}}_c g_f^{-1}(\overline{\boldsymbol{w}}_c)) \bmod \overline{z}_0 \tag{4.17}$$

whose decryption is equal to $\boldsymbol{F}\boldsymbol{w}$.

4.1.1 Conditions for the correct decryption in the PQS-RHE scheme

In this subsection, a sufficient condition for the correct decryption will be given to guarantee that the PQS-RHE scheme delivers the correct result of a matrix-vector product after the decryption (4.16).

Theorem 6. *Let $\overline{z}_0 = s_0 + qp$ denote the divisor in the modulo operation, where s_0 is an integer uniformly chosen from $[-2^\rho + 1, 2^\rho - 1]$, q is an integer uniformly chosen from $[0, \lfloor 2^\gamma/p \rfloor]$ and p is a ψ-bit prime number. Denote by $sk = (\theta, p)$ the secret key, where θ is an integer value. Let the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ and the vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ be encrypted by*

$$\begin{aligned} \overline{\boldsymbol{F}}_c &= PQS.Enc(\boldsymbol{F}, sk) = (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p) \bmod \overline{z}_0 \\ \overline{\boldsymbol{w}}_c &= PQS.Enc(\boldsymbol{w}, sk) = (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod \overline{z}_0 \end{aligned} \tag{4.18}$$

where $\boldsymbol{G}_f = \boldsymbol{I}_\beta \otimes \boldsymbol{g}_f^T \in \mathbb{N}^{\beta\times\beta\phi}$ denotes the gadget matrix, $\boldsymbol{g}_f^T = [b^{\phi-1}\, b^{\phi-2} \cdots b\, 1] \in \mathbb{N}^{1\times\phi}$, $\phi = \lceil log_b(2^\gamma) \rceil$, b is a known integer constrained by $b \geq 2$. The entries f_{ij} and w_j in, respectively, $\boldsymbol{F}$ and $\boldsymbol{w}$ belong to the set $\{0, 1, \cdots, M\}$, the entries s_{id}, s_j in $\overline{\boldsymbol{S}}_f \in \mathbb{N}^{\alpha\times\beta\phi}, \overline{\boldsymbol{s}}_w \in \mathbb{N}^{\beta\times 1}$ are uniformly selected integers from $[-2^\rho + 1, 2^\rho - 1]$ and the entries r_{id}, r_j in $\overline{\boldsymbol{R}}_f \in \mathbb{N}^{\alpha\times\beta\phi}, \overline{\boldsymbol{r}}_w \in \mathbb{N}^{\beta\times 1}$ are uniformly selected integers from $[0, q-1]$, $i = 1, 2, \cdots, \alpha$, $j = 1, 2, \cdots, \beta$, $d = 1, 2, \cdots, \beta\phi$, M is a known integer. Assume that $\overline{\boldsymbol{c}}_\times$ is obtained by (4.17). If

$$2^\rho \beta M\theta + 2^\rho \beta\phi b(\beta M\theta + 5) + \beta\theta^2 M^2 < p \tag{4.19a}$$

$$2^\rho \beta M\theta + 2^\rho \beta\phi b(\beta M\theta + 5) < \theta^2 \tag{4.19b}$$

then $\overline{Dec}(\overline{\boldsymbol{c}}_{\times}, sk)$ *in* (4.16) *delivers the true result of the matrix-vector product* $\boldsymbol{Fw}$*, i.e.*

$$\overline{\boldsymbol{\nu}} = PQS.Dec(\overline{\boldsymbol{c}}_{\times}, sk) = \boldsymbol{Fw} \tag{4.20}$$

Proof. Let $\overline{z}_0 = s_0 + qp$, where s_0 is an integer uniformly selected from $[-2^{\rho}+1, 2^{\rho}-1]$, q is an integer and p is a prime number. Substituting (4.14) into (4.17), there is

$$\begin{aligned}
\overline{\boldsymbol{c}}_{\times} &= (\overline{\boldsymbol{F}}_c g_f^{-1}(\overline{\boldsymbol{w}}_c)) \bmod \overline{z}_0 \\
&= \Big(((\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p) \bmod \overline{z}_0) g_f^{-1}(\overline{\boldsymbol{w}}_c) \Big) \bmod \overline{z}_0 \\
&= \Big(\big(\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p - \Big\lfloor \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{\overline{z}_0} \Big\rfloor \overline{z}_0 \big) g_f^{-1}(\overline{\boldsymbol{w}}_c) \Big) \bmod \overline{z}_0 \\
&= (\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p) g_f^{-1}(\overline{\boldsymbol{w}}_c) - \Big\lfloor \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \Big\rfloor (s_0 + qp)\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
&\quad - \Big\lfloor \frac{\big(\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p\big) g_f^{-1}(\overline{\boldsymbol{w}}_c)}{s_0 + qp} - \Big\lfloor \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \Big\rfloor g_f^{-1}(\overline{\boldsymbol{w}}_c) \Big\rfloor (s_0 + qp)
\end{aligned} \tag{4.21}$$

where $g_f^{-1}(\overline{\boldsymbol{w}}_c) \in \mathbb{N}^{\beta\phi \times 1}$ is the base-b decomposition of the ciphertexts $\overline{\boldsymbol{w}}_c \in \mathbb{N}^{\beta \times 1}$. Let

$$\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) = \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \tag{4.22}$$

Note that $\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p < \overline{z}_0$, $\overline{\boldsymbol{w}}_c = \boldsymbol{G}_f g_f^{-1}(\overline{\boldsymbol{w}}_c)$ with $\overline{\boldsymbol{w}}_c$ got in (4.15) and thus

$$\begin{aligned}
&\overline{\boldsymbol{c}}_{\times} \bmod p \\
&= \Big(\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{FG}_f\theta g_f^{-1}(\overline{\boldsymbol{w}}_c) - \Big\lfloor \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \Big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
&\quad - \Big\lfloor \frac{\big(\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p\big) g_f^{-1}(\overline{\boldsymbol{w}}_c)}{s_0 + qp} - \Big\lfloor \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \Big\rfloor g_f^{-1}(\overline{\boldsymbol{w}}_c) \Big\rfloor s_0 \Big) \bmod p \\
&= \big(\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\theta(\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
&\quad - \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0 \big) \bmod p
\end{aligned} \tag{4.23}$$

Recall that all entries f_{ij} of the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha \times \beta}$ and all entries w_j of the vector $\boldsymbol{w} \in \mathbb{N}^{\beta \times 1}$ are from the set $\{0, 1, \cdots, M\}$, $s_0 + qp \geq 2^{\gamma-1}$, all entries s_{id} of the matrix $\overline{\boldsymbol{S}}_f \in \mathbb{N}^{\alpha \times \beta\phi}$ are integers uniformly chosen from $[-2^{\rho}+1, 2^{\rho}-1]$, all entries r_{id} of the matrix $\overline{\boldsymbol{R}}_f \in \mathbb{N}^{\alpha \times \beta\phi}$ are integers uniformly chosen from $[0, q-1]$, $\phi = \log_b(2^{\gamma})$, $b \geq 2$ and $\boldsymbol{G}_f = \boldsymbol{I}_{\beta} \otimes \boldsymbol{g}_f^T \in \mathbb{N}^{\beta \times \beta\phi}$ with $\boldsymbol{g}_f^T = [b^{\phi-1}\, b^{\phi-2} \cdots b\, 1] \in \mathbb{N}^{1 \times \phi}$. There is

$$\begin{aligned}
\|\mathcal{N}(\overline{c}_{\times})\|_{max} &= \Big\| \frac{\overline{\boldsymbol{S}}_f + \boldsymbol{FG}_f\theta + \overline{\boldsymbol{R}}_f p}{s_0 + qp} \Big\|_{max} \\
&< \frac{2^{\rho} + \beta M b^{\phi-1}\theta + 2^{\gamma}}{2^{\gamma-1}}
\end{aligned}$$

$$
\begin{aligned}
&< \frac{2^{\rho} + \beta M b^{\log_b(2^{\gamma})-1}\theta + 2^{\gamma}}{2^{\gamma-1}} \\
&< \frac{2^{\rho} + \beta M 2^{\gamma}\theta/b + 2^{\gamma}}{2^{\gamma-1}} < \beta M\theta + 3
\end{aligned} \tag{4.24}
$$

and

$$
\|g_f^{-1}(\overline{\boldsymbol{w}}_c)\|_{\infty} < b \tag{4.25}
$$

so that

$$
\begin{aligned}
&\Big\| \overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\theta(\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
&\quad - \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0 \|_{\infty} \\
&< \beta\phi \|\overline{\boldsymbol{S}}_f\|_{max} \|g_f^{-1}(\overline{\boldsymbol{w}}_c)\|_{\infty} + \beta\theta \|\boldsymbol{F}\|_{max} \big(\|\overline{\boldsymbol{s}}_w\|_{\infty} + \theta \|\boldsymbol{w}\|_{\infty} \big) \\
&\quad + 2^{\rho}\beta\phi \|\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \rfloor\|_{max} \|g_f^{-1}(\overline{\boldsymbol{w}}_c)\|_{\infty} \\
&\quad + 2^{\rho}\beta\phi \|\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \rfloor\|_{max} \|g_f^{-1}(\overline{\boldsymbol{w}}_c)\|_{\infty} \\
&< 2^{\rho}\beta\phi b + \beta\theta M(2^{\rho} + \theta M) + 2^{\rho}\beta\phi(\beta M\theta + 3)b + 2^{\rho}\beta\phi b \\
&< 2^{\rho}\beta M\theta + 2^{\rho}\beta\phi b(\beta M\theta + 5) + \beta\theta^2 M^2
\end{aligned} \tag{4.26}
$$

If (4.19a) holds, then

$$
\begin{aligned}
\overline{\boldsymbol{c}}_{\times} \bmod p = \overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
- \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0 + \boldsymbol{F}\boldsymbol{w}\theta^2
\end{aligned} \tag{4.27}
$$

and

$$
\begin{aligned}
(\overline{\boldsymbol{c}}_{\times} \bmod p) \bmod \theta^2 = \big(\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
- \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0 \big) \bmod \theta^2
\end{aligned} \tag{4.28}
$$

Note that

$$
\begin{aligned}
&\|\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
&\quad - \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0 \|_{\infty} \\
&< 2^{\rho}\beta M\theta + 2^{\rho}\beta\phi b(\beta M\theta + 5)
\end{aligned} \tag{4.29}
$$

If (4.19b) holds, there is

$$
\begin{aligned}
(\overline{\boldsymbol{c}}_{\times} \bmod p) \bmod \theta^2 = \overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c) \\
- \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_{\times}) - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \big\rfloor s_0
\end{aligned} \tag{4.30}
$$

Substituting (4.27) and (4.30) into (4.16), we get

$$
\begin{aligned}
\overline{\boldsymbol{\nu}} = PQS.Dec(\overline{\boldsymbol{c}}_{\times}, sk) &= \frac{\overline{\boldsymbol{c}}_{\times} \bmod p - (\overline{\boldsymbol{c}}_{\times} \bmod p) \bmod \theta^2}{\theta^2} \\
&= \frac{\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \big\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_{\times}) \big\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c)}{\theta^2}
\end{aligned}
$$

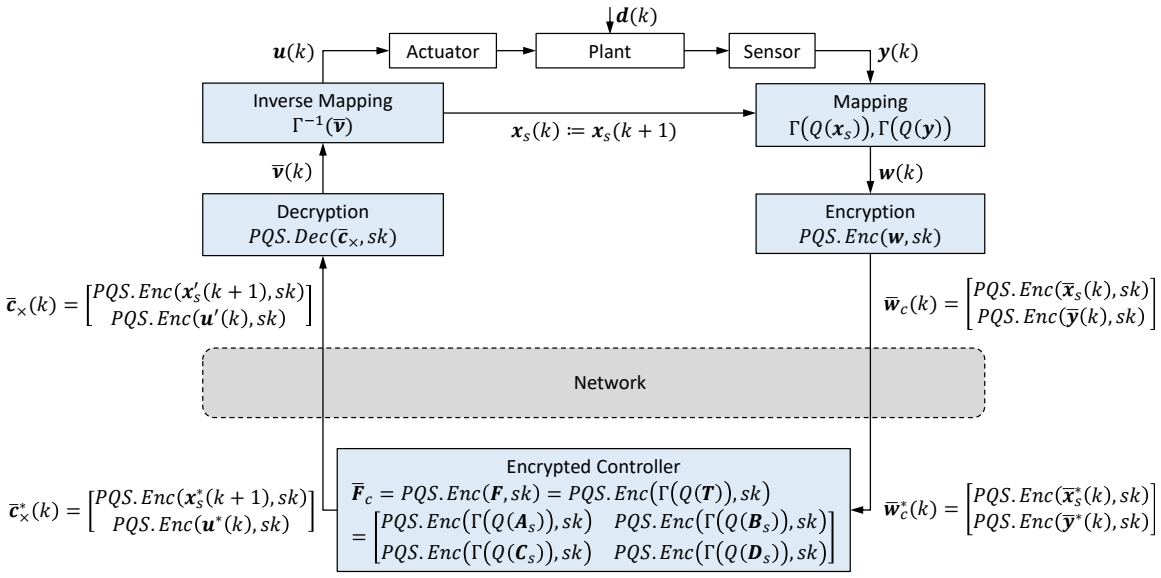

Figure 4.1: Encrypted cloud-based control system with the PQS-RHE scheme

$$
\begin{aligned}
&- \frac{\left\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times) \rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \right\rfloor s_0}{\theta^2} + \frac{\boldsymbol{F}\boldsymbol{w}\theta^2}{\theta^2} \\
&- \frac{\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c) + \boldsymbol{F}\overline{\boldsymbol{s}}_w\theta - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times) \rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c)}{\theta^2} \\
&+ \frac{\left\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times) \rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c) \right\rfloor s_0}{\theta^2} \\
&= \boldsymbol{F}\boldsymbol{w}
\end{aligned}
\tag{4.31}
$$

i.e. the decryption (4.16) gives the correct result of the matrix-vector product $\boldsymbol{F}\boldsymbol{w}$ and the PQS-RHE scheme is homomorphic with respect to the matrix-vector product. □

4.1.2 Encrypted cloud-based control system

The structure of the encrypted cloud-based control system with the PQS-RHE is shown in Fig. 4.1.

The matrix $\boldsymbol{T}$ (2.3) with the controller parameters $\boldsymbol{A}_s$, $\boldsymbol{B}_s$, $\boldsymbol{C}_s$ and $\boldsymbol{D}_s$ is quantized element-wise by (3.11), which gives $\overline{\boldsymbol{T}} = Q(\boldsymbol{T})$. The encrypted parameter matrix $\overline{\boldsymbol{F}}_c$ is obtained by firstly mapping each entry in the quantized matrix $\overline{\boldsymbol{T}}$ with the mapping function $\Gamma(\overline{\boldsymbol{T}})$ (3.12) and then applying the encryption (4.14).

In each controller cycle, the sensor outputs $\boldsymbol{y}(k)$ and the state vector $\boldsymbol{x}_s(k)$ are stacked together by (2.3) and then mapped with, respectively, the quantization function (3.11) and the mapping function in (3.12), which gives the integer vector $\boldsymbol{w}(k) = [\Gamma^T(Q(\boldsymbol{x}_s))\ \Gamma^T(Q(\boldsymbol{y}))]^T$. The encrypted vector $\overline{\boldsymbol{w}}_c(k)$, which will be transmitted over the network to the controller, is obtained by substituting $\boldsymbol{w}(k)$ into (4.15). The encrypted vector $\overline{\boldsymbol{w}}_c^*(k)$ arriving at the controller side is processed by the evaluation procedure in (4.17), which gives $\overline{\boldsymbol{c}}_\times^*(k)$. To feed the actuators with the control

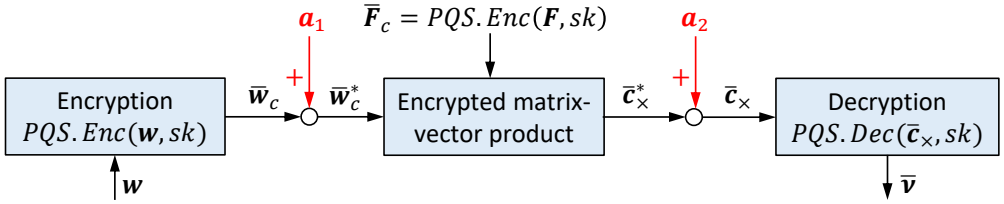

Figure 4.2: Attacks on the signals encrypted by the PQS-RHE scheme

input signal $\boldsymbol{u}(k)$ and obtain the state vector $\boldsymbol{x}_s(k+1)$, the encrypted vector $\overline{\boldsymbol{c}}_\times(k)$ arriving at the plant side will be decrypted by (4.16) and then the inverse mapping function in (3.13) is applied. For the next controller cycle, the state vector $\boldsymbol{x}_s(k)$ is set to $\boldsymbol{x}_s(k+1)$, i.e. $\boldsymbol{x}_s(k) := \boldsymbol{x}_s(k+1)$.

4.2 Resilience of post-quantum secure encryption

In this subsection, it will be shown that, even though the decomposition technique is integrated into the encryption process, the PQS-RHE scheme is still resilient to additive attacks. For this purpose, assume that two attacks are injected into the communication channels encrypted by the PQS-RHE scheme as shown in Fig. 4.2. The first additive attack $\boldsymbol{a}_1 \in \mathbb{N}^{\beta\times 1}$ is injected into the signal $\overline{\boldsymbol{w}}_c$ encrypted by (4.15). The second additive attack $\boldsymbol{a}_2 \in \mathbb{N}^{\alpha\times 1}$ is imposed on the ciphertext $\overline{\boldsymbol{c}}_\times^*$ obtained after the encrypted matrix-vector product in (4.17). Now we are going to analyze the behaviour of the value $\overline{\boldsymbol{\nu}}$ obtained after the decryption.

Theorem 7. *Assume that the matrix $\boldsymbol{F} \in \mathbb{N}^{\alpha\times\beta}$ and a vector $\boldsymbol{w} \in \mathbb{N}^{\beta\times 1}$ are encrypted by, respectively,* (4.14) *and* (4.15)*, which gives*

$$\overline{\boldsymbol{F}}_c = PQS.Enc(\boldsymbol{F}, sk) = (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p) \bmod \overline{z}_0 \tag{4.32}$$

$$\overline{\boldsymbol{w}}_c = PQS.Enc(\boldsymbol{w}, sk) = (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod \overline{z}_0 \tag{4.33}$$

Let $\boldsymbol{a}_1 \in \mathbb{N}^{\beta\times 1}$ and $\boldsymbol{a}_2 \in \mathbb{N}^{\alpha\times 1}$ denote additive attacks on, respectively, the ciphertexts $\overline{\boldsymbol{w}}_c$ and $\overline{\boldsymbol{c}}_\times^*$, i.e.

$$\begin{aligned} \overline{\boldsymbol{w}}_c^* &= \overline{\boldsymbol{w}}_c + \boldsymbol{a}_1 \\ \overline{\boldsymbol{c}}_\times &= \overline{\boldsymbol{c}}_\times^* + \boldsymbol{a}_2 \end{aligned} \tag{4.34}$$

where $\overline{\boldsymbol{c}}_\times^* = (\overline{\boldsymbol{F}}_c g_f^{-1}(\overline{\boldsymbol{w}}_c^*)) \bmod \overline{z}_0$ is obtained by (4.17)*. If the decryption of $\overline{\boldsymbol{c}}_\times$ is carried out by* (4.16)*, then*

$$\overline{\boldsymbol{\nu}} = PQS.Dec(\overline{\boldsymbol{c}}_\times, sk) = \boldsymbol{F}\boldsymbol{w} \tag{4.35}$$

as long as

$$\boldsymbol{\delta} p - \overline{\boldsymbol{h}} \leq \boldsymbol{F}\theta\boldsymbol{a}_1 + \boldsymbol{a}_2 < \boldsymbol{\delta} p + \theta^2\boldsymbol{1} - \overline{\boldsymbol{h}}, \tag{4.36}$$

where

$$\begin{aligned}\overline{\boldsymbol{h}} = \overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) + \boldsymbol{F}\theta\overline{\boldsymbol{s}}_w - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) \\ - \left\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)\right\rfloor s_0\end{aligned}$$

and $\mathcal{N}(\overline{\boldsymbol{c}}_\times) = (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p)/\overline{z}_0$, $g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)$ *is the base-b decomposition of* $\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1$, $\mathbf{1}_{\alpha\times 1}$ *is a vector of ones,* $\boldsymbol{\delta} \in \mathbb{N}^{\alpha\times 1}$ *is a vector whose entries are* $\delta_i \in \{0, 1, \cdots, q-1\}$.

Proof. According to (4.15), the encryption of $\boldsymbol{w}$ gives

$$\begin{aligned}\overline{\boldsymbol{w}}_c &= PQS.Enc(\boldsymbol{w}, sk) \\ &= (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod \overline{z}_0\end{aligned} \tag{4.37}$$

where θ and $\overline{z}_0$ are integers and p is a prime number. Due to the additive attack $\boldsymbol{a}_1$,

$$\begin{aligned}\overline{\boldsymbol{w}}_c^* &= Enc(\boldsymbol{w}, sk) + \boldsymbol{a}_1 \\ &= \overline{\boldsymbol{w}}_c + \boldsymbol{a}_1 \\ &= (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod \overline{z}_0 + \boldsymbol{a}_1\end{aligned} \tag{4.38}$$

Substituting (4.14) and (4.38) into (4.17) and considering (4.21), (4.22), there is

$$\begin{aligned}\overline{\boldsymbol{c}}_\times^* &= (\overline{\boldsymbol{F}}_c g_f^{-1}(\overline{\boldsymbol{w}}_c^*)) \bmod \overline{z}_0 \\ &= (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) \\ &\quad - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor \overline{z}_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) - \left\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)\right\rfloor \overline{z}_0\end{aligned} \tag{4.39}$$

Because of the attack $\boldsymbol{a}_2$, there is $\overline{\boldsymbol{c}}_\times = \overline{\boldsymbol{c}}_\times^* + \boldsymbol{a}_2$. Note that $\overline{z}_0 = s_0 + qp$, where s_0 and q are integers, and $\boldsymbol{G}_f g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) = \overline{\boldsymbol{w}}_c + \boldsymbol{a}_1$. It yields

$$\begin{aligned}\overline{\boldsymbol{c}}_\times \bmod p &= (\overline{\boldsymbol{c}}_\times^* + \boldsymbol{a}_2) \bmod p \\ &= \big((\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) \\ &\quad - \left\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)\right\rfloor s_0 + \boldsymbol{a}_2\big) \bmod p \\ &= \big(\underbrace{\overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) + \boldsymbol{F}\theta\overline{\boldsymbol{s}}_w}_{\overline{\boldsymbol{h}}_1} + \boldsymbol{F}\theta\boldsymbol{a}_1 + \boldsymbol{F}\boldsymbol{w}\theta^2 - \underbrace{\lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)}_{\overline{\boldsymbol{h}}_2} \\ &\quad - \underbrace{\left\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)\right\rfloor s_0}_{\overline{\boldsymbol{h}}_3} + \boldsymbol{a}_2\big) \bmod p\end{aligned} \tag{4.40}$$

If the attacks $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ satisfy (4.36), then $\boldsymbol{\delta}p \le \boldsymbol{F}\theta\boldsymbol{a}_1 + \overline{\boldsymbol{h}} + \boldsymbol{a}_2 < \boldsymbol{\delta}p + \theta^2\mathbf{1}$, where $\overline{\boldsymbol{h}} = \overline{\boldsymbol{h}}_1 - \overline{\boldsymbol{h}}_2 - \overline{\boldsymbol{h}}_3$ and $\boldsymbol{\delta} \in \mathbb{N}^{\alpha\times 1}$ whose entries are $\delta_i \in \{0, 1, \cdots, q-1\}$. Let

$$\boldsymbol{F}\theta\boldsymbol{a}_1 + \overline{\boldsymbol{h}} + \boldsymbol{a}_2 = \boldsymbol{\delta}p + \boldsymbol{\Delta}, \tag{4.41}$$

where $\boldsymbol{\Delta} \in \mathbb{N}^{\alpha\times 1}$ whose entries are $\Delta_i \in \{0, 1, \cdots, \theta^2 - 1\}$. Thus,

$$\overline{\boldsymbol{c}}_\times \bmod p = (\boldsymbol{F}\theta\boldsymbol{a}_1 + \overline{\boldsymbol{h}} + \boldsymbol{a}_2 + \boldsymbol{F}\boldsymbol{w}\theta^2) \bmod p$$

$$
\begin{aligned}
&= (\boldsymbol{\delta} p + \boldsymbol{\Delta} + \boldsymbol{F}\boldsymbol{w}\theta^2) \bmod p \\
&= \boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}
\end{aligned} \tag{4.42}
$$

Due to the decryption (4.16), it yields

$$
\begin{aligned}
\overline{\boldsymbol{\nu}} &= PQS.Dec(\overline{\boldsymbol{c}}_{\times}, sk) \\
&= \frac{\overline{\boldsymbol{c}}_{\times} \bmod p - (\overline{\boldsymbol{c}}_{\times} \bmod p) \bmod \theta^2}{\theta^2} \\
&= \frac{\boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w} - (\boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}) \bmod \theta^2}{\theta^2} \\
&= \boldsymbol{F}\boldsymbol{w}
\end{aligned} \tag{4.43}
$$

i.e. the vector $\overline{\boldsymbol{\nu}}$ is still the correct result of $\boldsymbol{F}\boldsymbol{w}$. □

4.3 Security proof and parameter selection

In this section, it will be shown that the PQS-RHE scheme given in Section 4.1 is post-quantum secure. Moreover, an approach will be given to select the parameters of the PQS-RHE scheme systematically to achieve the desired security level.

4.3.1 Security analysis

Lemma 1 builds the basis for showing that the ciphertexts obtained by the PQS-RHE scheme and integers drawn from an uniform distribution are computationally indistinguishable. As the PQS-RHE scheme should be secure against any PPT algorithms carried out on a quantum computer, it must be ensured that the ciphertexts obtained by the PQS-RHE scheme and simultaneously the divisor $\overline{z}_0$ in the modulo operations are computationally indistinguishable from integers drawn from an uniform distribution. By employing the concept of truncated distributions, it can be shown that an integer drawn from the uniform distribution and the integer $\overline{z}_0$ drawn from an AGCD distribution are computationally indistinguishable, as given below.

Lemma 2. *Suppose that $\mathcal{U}_{\gamma}^{(\geq 2^{\gamma-1})}$ is the left-truncated uniform distribution with support over $[2^{\gamma-1}, 2^{\gamma} - 1]$. Let $\overline{z}_0$ be an integer drawn from the left-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q, p)$ with support over $\{\overline{z}_0 \mid \overline{z}_0 = s_0 + qp, \overline{z}_0 \geq 2^{\gamma-1}\}$, where s_0 is a sample drawn from an uniform distribution over the interval $[-2^{\rho} + 1, 2^{\rho} - 1]$ and q is a sample drawn from an uniform distribution over the interval $[0, \lfloor 2^{\gamma}/p \rfloor]$. Then the left-truncated uniform distribution $\mathcal{U}_{\gamma}^{(\geq 2^{\gamma-1})}$ and the left-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q, p)$ are computationally indistinguishable.*

Proof. The proof here can be carried out in a manner similar to the proof of Lemma 1 and is therefore omitted. □

In order to prove the post-quantum security of the PQS-RHE scheme, the well-established *hybrid argument technique* will be employed. The hybrid argument technique allows to show the indistinguishability between distinct distributions (Mittelbach and Fischlin, 2021). For this purpose, we define two hybrid arguments $\mathcal{H}_0$ and $\mathcal{H}_1$ so that the advantage for any adversary to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$ is negligible. Due to these hybrid arguments, it can be concluded that an adversary can not distinguish between ciphertexts generated by the PQS-RHE scheme that obey an AGCD distribution and integers uniformly distributed. Moreover, as the divisor $\overline{z}_0$ in the modulo operations follow an AGCD distribution, $\overline{z}_0$ is computationally indistinguishable from an integer drawn from an uniform distribution. As the decisional AGCD problem is the problem of distinguishing between the AGCD distribution and the uniform distribution, which can not be solved by any adversary in polynomial time even with access to a quantum computer, the PQS-RHE scheme is post-quantum secure.

The proof for the post-quantum security of the PQS-RHE scheme can be shown for both the encrypted vector $\overline{\boldsymbol{w}}_c$ in (4.15) and the encrypted matrix $\overline{\boldsymbol{F}}_c$ in (4.14) in a similar manner. Thus, the focus of the following proof takes into account the encrypted vector $\overline{\boldsymbol{w}}_c$ in (4.15) and omits the encrypted matrix $\overline{\boldsymbol{F}}_c$ in (4.14).

Theorem 8. *For an adversary $\mathcal{A}$ that has access to any PPT algorithm and a quantum computer, the probability for the adversary $\mathcal{A}$ to distinguish between the distribution of the ciphertexts obtained by the PQS-RHE scheme that obey an AGCD distribution and an uniform distribution in polynomial time is negligible. Moreover, as the distribution of the divisor $\overline{z}_0$ in the modulo operations follows an AGCD distribution, $\overline{z}_0$ is computationally indistinguishable from an integer drawn from an uniform distribution. Thus, the PQS-RHE scheme is post-quantum secure.*

Proof. Let $\mathcal{A}$ be the adversary that tries to distinguish between the distribution $\mathcal{H}_0$ and the distribution $\mathcal{H}_1$ given as follows.

Hybrid $\mathcal{H}_0$: Let $\overline{\mathcal{E}}_0 = (PQS.KeyGen_0, PQS.Enc_0, PQS.Dec_0, PQS.Eval_0)$ be the PQS-RHE scheme whose key generation function is denoted by $PQS.KeyGen_0(1^\kappa)$, the secret key is $sk = (\theta, p)$ and $\gamma, \psi, \rho, \overline{z}_0$ are parameters for encryption, where $\overline{z}_0$ is an integer drawn from the left-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q,p)$ with support over the set $\{\overline{z}_0 \mid \overline{z}_0 = s_0 + qp, \overline{z}_0 \geq 2^{\gamma-1}\}$, p is a prime number, s_0 and q are random integers uniformly distributed, respectively, in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $[0, \lfloor 2^\gamma/p \rfloor]$. Then, the vector $\boldsymbol{w}$ is encrypted by

$$\begin{aligned}\overline{\boldsymbol{w}}_c &= PQS.Enc(\boldsymbol{w}, sk) \\ &= (\overline{\boldsymbol{s}}_w + \boldsymbol{w}\theta + \overline{\boldsymbol{r}}_w p) \bmod (s_0 + qp) \\ &= (\overline{\boldsymbol{z}} + \boldsymbol{w}\theta) \bmod \overline{z}_0 \end{aligned} \tag{4.44}$$

where the entry $\overline{z}_j = \overline{s}_j + \overline{r}_j p$ in $\overline{\boldsymbol{z}}$ follows the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<\overline{z}_0)}(q,p)$ with support over the set $\{\overline{z}_j \mid \overline{z}_j = \overline{s}_j + \overline{r}_j p, \overline{z}_j < \overline{z}_0\}$, $\overline{s}_j$ in $\overline{\boldsymbol{s}}_w$ are random integers uniformly distributed in the interval $[-2^\rho + 1, 2^\rho - 1]$ and $\overline{r}_j$ in $\overline{\boldsymbol{r}}_w$ are random integers uniformly distributed in the interval $[0, q-1]$, $j = 1, 2, \cdots, \beta$.

Hybrid $\mathcal{H}_1$: Suppose that $\mathcal{U}_\gamma$ is an uniform distribution over the interval $[0, 2^\gamma - 1]$. Let $\overline{\boldsymbol{u}}$ be a vector whose entries $\overline{u}_j$ are random integers following the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ with support over $[0, u_0 - 1]$, where u_0 is an integer drawn from the left-truncated uniform distribution $\mathcal{U}_\gamma^{(\geq 2^{\gamma-1})}$ with support over $[2^{\gamma-1}, 2^\gamma - 1]$. Then, let $\overline{\mathcal{E}}_1 = (PQS.KeyGen_1, PQS.Enc_1, PQS.Dec_1, PQS.Eval_1)$ denotes the encryption scheme whose key generation function $PQS.KeyGen_1(1^\kappa)$ outputs the secret key $sk = (\theta, p)$ and the parameters γ, ψ, ρ, u_0. The ciphertexts $\overline{\boldsymbol{u}}_w$ following the distribution $\mathcal{H}_1$ generated by the encryption function $PQS.Enc_1(\boldsymbol{w}, sk)$ is given as

$$\begin{aligned} \overline{\boldsymbol{u}}_w &= PQS.Enc_1(\boldsymbol{w}, sk) \\ &= (\overline{\boldsymbol{u}} + \boldsymbol{w}\theta) \bmod u_0 \\ &= \boldsymbol{u}^* \end{aligned} \tag{4.45}$$

Recall that all entries $w_j\theta$ in $\boldsymbol{w}\theta$ are constant integers during the hybrid arguments $\mathcal{H}_0, \mathcal{H}_1$ and all entries $\overline{u}_j$ in $\overline{\boldsymbol{u}}$ are random integers following the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ with support over $[0, u_0 - 1]$. Thus, all entries $\overline{u}_j + w_j\theta$ in $\overline{\boldsymbol{u}} + \overline{\boldsymbol{w}}$ are random integers and have an uniform distribution supported over $[w_j\theta, w_j\theta + u_0 - 1]$. Due to the modulus u_0 applied on $\overline{\boldsymbol{u}} + \boldsymbol{w}\theta$, all integers u_j^* in $\boldsymbol{u}^* = (\overline{\boldsymbol{u}} + \boldsymbol{w}\theta) \bmod u_0$ follow the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$. That means, all the entries in the vector $\overline{\boldsymbol{u}}_w$ obtained in (4.45) also follow the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$. The difference between the hybrid argument $\mathcal{H}_0$ and the hybrid argument $\mathcal{H}_1$ lies in $\overline{\boldsymbol{z}}, \overline{z}_0$ in (4.44) and $\overline{\boldsymbol{u}}, u_0$ in (4.45) defined by, respectively, the truncated AGCD distributions $\mathcal{D}_{\gamma,\rho}^{(<\overline{z}_0)}(q, p), \mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q, p)$ and the truncated uniform distributions $\mathcal{U}_\gamma^{(<u_0)}, \mathcal{U}_\gamma^{(\geq 2^{\gamma-1})}$. Recall that the right-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(<\overline{z}_0)}(q, p)$ and the right-truncated uniform distribution $\mathcal{U}_\gamma^{(<u_0)}$ are computationally indistinguishable according to Lemma 1. As proven in Lemma 2, the left-truncated AGCD distribution $\mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q, p)$ and the left-truncated uniform distribution $\mathcal{U}_\gamma^{(\geq 2^{\gamma-1})}$ are computationally indistinguishable. Thus, the probability for the adversary $\mathcal{A}$ to distinguish between the distribution $\mathcal{H}_0$ and the distribution $\mathcal{H}_1$ is negligible. As a result, to distinguish between the ciphertexts obtained by the PQS-RHE scheme and an integer that obey the uniform distribution is indeed the decisional AGCD problem given in Definition 5. Moreover, to distinguish between the divisor $\overline{z}_0$ in the modulo operations and an integer drawn from an uniform distribution is also the decisional AGCD problem. Thus, the PQS-RHE scheme is post-quantum secure. □

According to Cheon and Stehlé (2015), an HE scheme whose security is based on the decisional AGCD problem automatically satisfies the security requirement of IND-CPA. Thus, ciphertexts generated by the PQS-RHE scheme do not reveal any information about the plaintexts.

4.3.2 Selection of parameters

In this subsection, an approach to select the parameters ρ, θ, p, ψ and γ of the PQS-RHE scheme will be given in order to ensure the homomorphic property of the PQS-RHE scheme and simultaneously achieve the desired security level against the main families of known attacks, namely, brute force attacks (Chen and Nguyen, 2012; Coron et al., 2012) and lattice attacks (Cheon and Stehlé, 2015; Galbraith et al., 2016).

The factorisation attacks, such as the elliptic-curve method (Lenstra, 1987) and the number field sieve (Lenstra et al., 1993) are often considered in security analysis when it is assumed that an adversary has access to an integer $z_0 = qp$, where p is a prime number and q is a large integer. However, the ciphertexts generated by the PQS-RHE scheme and the divisor $\overline{z}_0 = s_0 + qp$ in the modulo operations obey the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ given in Definition 2. Until now, there does not exist a known PPT algorithm that makes use of factorization attacks to gain access to the prime number p from samples that follow the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$ in less time than, for instance, lattice attacks. Therefore, factorisation attacks do not need to be considered here.

In order to obtain the correct result of the matrix-vector product $\boldsymbol{Fw}$ after the decryption (4.16), the integer θ and the prime number p in the secret key $sk = (\theta, p)$ need to satisfy (4.19). Moreover, we have to make sure that the main families of known attacks are not able to gain access to the secret key $sk = (\theta, p)$. That means, the PQS-RHE scheme needs to satisfy condition (3.65) to prevent brute force attacks and condition (3.69) to prevent lattice attacks.

Before the selection of the parameters b, ρ, θ, p, ψ and γ of the PQS-RHE scheme will be shown, the influence of the parameter b on the computational workload in the cloud platform and the communication load will be addressed. The conditions for the selection of the prime number p in (4.19a) and the integer θ in (4.19b) are influenced by $b\phi = b\lceil \log_b 2^\gamma \rceil$. If b increases, the prime number p and the integer θ rises and thus the bit-size γ of ciphertexts grows and more communication capacities are required for the transmission of ciphertexts. However, by increasing the parameter b, the dimension of the encrypted matrix $\overline{\boldsymbol{F}}_c \in \mathbb{N}^{\alpha \times \beta\phi}$ decreases, where $\phi = \lceil \log_b(2^\gamma) \rceil$, so that much fewer encrypted additions and encrypted multiplications needs to be carried out for evaluating the controller with ciphertexts. As a result, increasing the parameter b reduces the computational workload in the cloud. In summary, the choice of the parameter b depends on the resources available for evaluating the controller in the cloud and the communication channels.

Now, the parameters b, ρ, θ, p, ψ and γ of the PQS-RHE scheme in Section 4.1 can be systematically determined as follows.

Step 1: Choose the security level κ according to National Institute of Standards and Technology (2020).

Step 2: Set $\rho = 2\kappa$ to satisfy (3.65) and select the bit-size ψ of the prime number p and the bit-size γ of the ciphertext so that (3.69) holds.

Step 3: Select the integer θ and the integer b, then calculate the integer $\phi = \lceil \log_b(2^\gamma) \rceil$.

Step 4: Repeat Step 2 and Step 3 until condition (4.19) is fulfilled.

4.4 Simulation example

In this section, an example of the encrypted cloud-based control system with the PQS-RHE scheme will be given to illustrate the main results. In the simulation, the quadruple-tank system and the dynamic output feedback controller introduced in Section 2.3 will be used.

The parameters of the PQS-RHE scheme can be selected systemically as follows. At first, the range λ_1 and the resolution λ_2 in the mapping function can be chosen as $\lambda_1 = 4$ and $\lambda_2 = 16$ so that the closed-loop system is stable. Thus, the bound of the plaintext is $M = 2^{\lambda_1+\lambda_2+1} = 2^{21}$ and $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1} + 1 = 4 \times 2^{41} + 1$. According to National Institute of Standards and Technology (2020), the commonly used security levels κ are chosen from the set $\{80, 112, 128, 192, 256\}$. As an example, the security level κ is chosen as $\kappa = 128$. The bit-size ρ of the noises s_{id} in the encrypted matrix (4.14) and s_j in the encrypted vector (4.15) is set as $\rho = 2\kappa = 256$ to satisfy (3.65). In order to make sure that condition (3.39) and condition (3.69) hold simultaneously, the integer θ is chosen from the interval $[2^{445}, 2^{446})$, $b = 2^{128}$, $\phi = 4550$, $\psi = 978$ and $\gamma = 577856$. Finally, the divisor $\overline{z}_0$ in the modulo operations is a constant integer and $\overline{z}_0 = s_0 + qp \geq 2^{\gamma-1}$, where s_0 is a sample drawn from a uniform distribution over the interval $[-2^\rho + 1, 2^\rho - 1]$ and q is a sample drawn from a uniform distribution over the interval $[0, \lfloor 2^\gamma / p \rfloor]$, p is a ψ-bit-sized prime number.

The controller parameters (2.7) are mapped by (3.11), (3.12) and then encrypted by (4.14). Due to the bit-size $\gamma = 577856$ of the ciphertext space, the encrypted controller parameters are large integers and thus omitted here.

In the encrypted cloud-based control system, the sensor output signal $\boldsymbol{y}(k)$ (see Fig. 4.3a) and the state vector $\boldsymbol{x}_s(k)$ of the dynamic output feedback controller are stacked together, mapped into the integer vector $\boldsymbol{w}(k)$ and then encrypted by the PQS-RHE scheme which leads to the ciphertext $\overline{\boldsymbol{w}}_c(k)$. Due to large ciphertexts, the ciphertext $\overline{\boldsymbol{w}}_c(k)$ and the ciphertext $\overline{\boldsymbol{c}}^*_\times(k)$ obtained after the evaluation process of the dynamic output feedback controller can not be displayed here. Recall that the encrypted vector $\overline{\boldsymbol{c}}^*_\times(k)$ transmitted over the network from the controller to the actuators is composed of the state vector $\boldsymbol{x}^*_s(k+1)$ of the controller and the control input signals $\boldsymbol{u}^*(k)$.

During the simulation, an attack is imposed on the encrypted control input signals (i.e. $\boldsymbol{a}_2(k) = [0\ 0\ a_{21}(k)\ a_{22}(k)]^T$) from $k = 125s$ to $k = 475s$ (see Fig. 4.3b), while there is no attack on the sensor output channels (i.e. $\boldsymbol{a}_1(k) = \boldsymbol{0}$). Fig. 4.3c shows the control input signals $\boldsymbol{u}(k)$ received by the actuators obtained after the decryption. As a comparison, Fig. 4.3d shows the control input signals $\boldsymbol{u}'(k)$ generated by the unencrypted dynamic output feedback controller in the form of (2.2) and (2.7) based

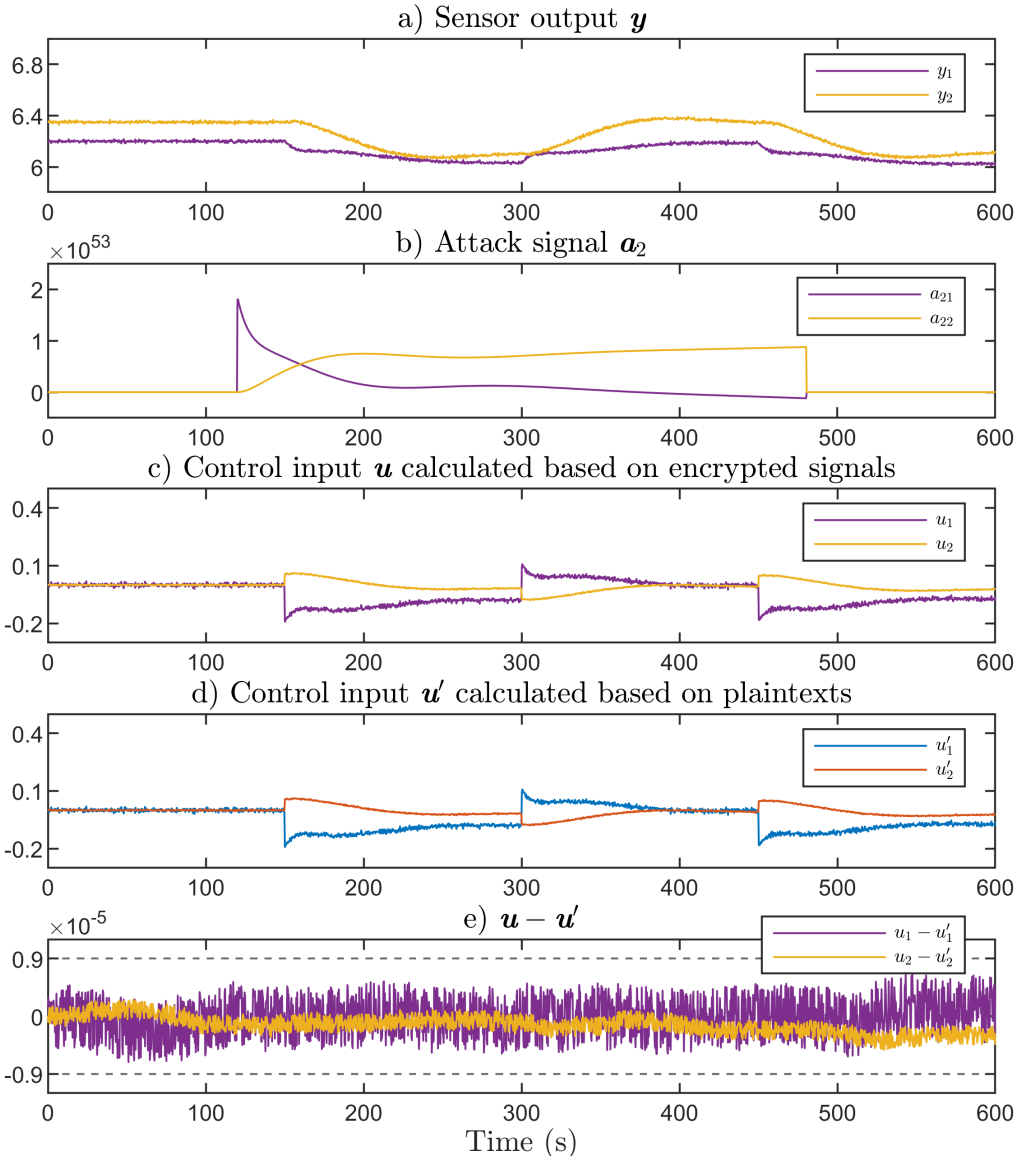

Figure 4.3: Encrypted cloud-based control system with the PQS-RHE scheme

on the controller parameters in plaintexts and the signals sent over the network in plaintexts.

During the time interval from $k = 125s$ to $k = 475s$, the attack signal $\boldsymbol{a}_2(k)$ is always inside of the resilience range, because $\mathbf{0} \leq \boldsymbol{a}_2 < \theta^2\mathbf{1} - \overline{\boldsymbol{h}}$, where $\overline{\boldsymbol{h}} = \overline{\boldsymbol{S}}_f g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) + \boldsymbol{F}\theta\overline{\boldsymbol{s}}_w - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor s_0\, g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1) - \big\lfloor (\mathcal{N}(\overline{\boldsymbol{c}}_\times) - \lfloor \mathcal{N}(\overline{\boldsymbol{c}}_\times)\rfloor) g_f^{-1}(\overline{\boldsymbol{w}}_c + \boldsymbol{a}_1)\big\rfloor s_0$ and $\mathcal{N}(\overline{\boldsymbol{c}}_\times) = (\overline{\boldsymbol{S}}_f + \boldsymbol{F}\boldsymbol{G}_f\theta + \overline{\boldsymbol{R}}_f p)/\overline{z}_0$. By taking a look at Fig. 4.3c, no effect of the attack signal $\boldsymbol{a}_2(k)$ on the control input signals $\boldsymbol{u}(k)$ obtained after the decryption can be observed, which is the result of the neutralization effect of the PQS-RHE scheme. That means, the true values of the control input signals $\boldsymbol{u}(k)$ reaches the actuators despite the existence of the attack $\boldsymbol{a}_2(k)$. As the transformation between real values and quantized values realized by (3.11) causes the so-called quantization error, a slight difference between $\boldsymbol{u}(k)$ obtained after the decryption and $\boldsymbol{u}'(k)$ calculated

directly based on plaintexts can be observed (see Fig. 4.3e). The quantization error is bounded by $|u_1(k) - u_1'(k)| \leq 0.9 \times 10^{-5}$, $\forall k$ and can be further reduced by increasing the resolution λ_2 (see Fig. 4.3e). Similar phenomenon can be observed in the second control input signal $u_2(k)$.

In summary, the PQS-RHE scheme enables to carry out the evaluation process of the dynamic output feedback controller in an encrypted environment so that the confidentiality of both the controller parameters and the signals transmitted over the network can be ensured. Moreover, the PQS-RHE scheme has the ability of resilience and additive attacks can be neutralized so that the plant can still operate even when an attack takes place in the encrypted control system. The influence of the quantization error caused by the transformation between real values and integer values of the signals during the encryption is negligible. The control performance in the encrypted cloud-based control system is almost the same as that achieved by the dynamic output feedback controller whose calculation is carried out in plaintexts.

4.5 Discussion

In this chapter, the PQS-RHE scheme is proposed that not only encrypts the control law of dynamic output feedback controllers but also is post-quantum secure. Moreover, the PQS-RHE scheme has the ability of resilience so that the influence of an additive attack can be cancelled out of the cloud-based control system.

To achieve post-quantum security, at first it is shown how to select the divisor in the modulo operations in the PQS-RHE scheme so that the divisor in the modulo operations follows an AGCD distribution. Due to the change in the divisor in the modulo operations, the noise accumulated during encrypted additions and encrypted multiplications is increased, which may lead to a loss of the homomorphism. To cope with it, a decomposition technique is integrated into the evaluation process of the encrypted controller. Then it is proven that the ciphertexts obtained by the PQS-RHE scheme that obey an AGCD distribution are computationally indistinguishable from a uniform distribution. As the problem of distinguishing between the AGCD distribution and the uniform distribution is the decisional AGCD problem, there does not exist any known attack carried out on a quantum computer that can gain any useful information from the ciphertexts obtained by the PQS-RHE scheme in polynomial time. That means, the PQS-RHE scheme is post-quantum secure. In order to achieve the desired security level in the PQS-RHE scheme, an approach to select the parameters in the PQS-RHE scheme is provided.

The well-established quadruple-tank system is used to validate the PQS-RHE scheme. As shown in the simulation results, the PQS-RHE scheme has the property of resilience and an attack imposed on the ciphertexts has no effect on the true values obtained after the decryption. As the encrypted cloud-based control system can operate with the true values of sensor signals and control input signals despite the existence of an attack, the availability of the encrypted cloud-based control system

is increased. Therefore, the PQS-RHE scheme is a useful approach to enhance the cyber security of cloud-based control systems.

5 Reduction of Network Load

In this chapter, the RHE scheme will be further developed to reduce the network communication load significantly while preserving the resilience property. As a result, the so-called multi-slot homomorphic encryption (MS-RHE) scheme is obtained.

As the bit-length of a ciphertext is longer than the corresponding plaintext, it remains a challenge to reduce the network load in encrypted cloud-based control systems (Darup et al., 2021). Two approaches that address the challenge of reducing the network load in encrypted cloud-based control systems are given by Alexandru et al. (2020) and Teranishi et al. (2023). In Alexandru et al. (2020), the CKKS cryptosystem given by Cheon et al. (2017) is used to implement a data-driven linear quadratic regulator. Based on the Discrete Fourier Transform (DFT), multiple plaintexts can be packed together into a single plaintext. Then, the single plaintext obtained by the Discrete Fourier Transform can be encrypted by the CKKS cryptosystem into a single ciphertext and transmitted over the network. Hence, the amount of ciphertexts sent over the network is reduced. In Teranishi et al. (2023), before the dynamic feedback controller will be encrypted, it is brought into the form of an input-output history feedback controller to avoid the decryption of the controller state at the plant side. Based on that, the BFV cryptosystem given by Fan and Vercauteren (2012) is applied to carry out the multiplication and addition of the control law with ciphertexts. Moreover, as the BFV cryptosystem employs the Chinese remainder theorem (CRT), multiple plaintexts can be packed together into a single ciphertext before they are sent over the communication channels. Thus, the network load is reduced.

In this chapter, the goals are twofold. At first, the network communication load in encrypted cloud-based control system will be significantly reduced. Secondly, the ability of resilience will be preserved. For this purpose, the RHE scheme proposed in Section 3.3 is further developed to explore the CRT so that multiple plaintexts can be encrypted into a single ciphertext. As a result, the amount of ciphertexts transferred over the network is decreased and thus the network communication load is significantly reduced. It will be proven that the resulting MS-RHE scheme still keeps the ability of resilience. Thus, additive attacks imposed on the ciphertexts can be neutralized and the controller can get the true sensor information and the actuators can get the true control input signals in case of attacks. A simulation example of the well-established quadruple-tank process will be used to demonstrate the proposed MS-RHE scheme for encrypted cloud-based control systems.

The chapter is organized as follows. The MS-RHE scheme is presented in Section 5.1. Moreover, the reduction of the network load achieved by the MS-RHE scheme is analyzed. In Section 5.2, the resilience of the MS-RHE scheme to additive attacks is

analyzed. The security analysis and the parameter selection of the MS-RHE scheme is shown in Section 5.3. Finally, an example of the well-established quadruple-tank system is given in Section 5.4 to show the cloud-based control system encrypted by the MS-RHE scheme.

5.1 Multi-slot resilient homomorphic encryption

In this section, the MS-RHE scheme will be proposed that modifies the RHE scheme given in Section 3.3 to reduce the network load in an encrypted cloud-based control system.

The four functions $\tilde{\mathcal{E}} = (MS.KeyGen,\ MS.Enc,\ MS.Dec,\ MS.Eval)$ are defined for the MS-RHE scheme.

Key Generation ($MS.KeyGen$): At first, select the security parameter κ and choose the parameters ρ, θ, ψ, γ as discussed later in Subsection 5.3.2. Then, select τ prime numbers p_j of bit-size ψ and sample the integer q uniformly from $\{0, 1, \cdots, \lfloor 2^{\gamma}/\pi_{\tau} \rfloor\}$ until q can not be factorised into prime factors smaller than 2^{ψ} and $q\pi_{\tau} \geq 2^{\gamma-1}$, where $\pi_{\tau} = \prod_{j=1}^{\tau} p_j$. Finally, let $\tilde{sk} = (\theta, p_1, \cdots, p_{\tau})$ be the secret key for encryption and decryption and set $\tilde{z}_0 = q\pi_{\tau}$.

Encryption ($MS.Enc$): The lth vector $\boldsymbol{f}_l \in \mathbb{N}^{\tau \times 1}$ is encrypted by

$$\begin{aligned} \tilde{f}_l = MS.Enc(\boldsymbol{f}_l, \tilde{sk}) &= (f_l + d_l \prod_{j=1}^{\tau} p_j) \bmod q \prod_{j=1}^{\tau} p_j \\ &= (f_l + d_l \pi_{\tau}) \bmod \tilde{z}_0 \end{aligned} \tag{5.1}$$

and the lth vector $\boldsymbol{w}_l \in \mathbb{N}^{\tau \times 1}$ is encrypted by

$$\begin{aligned} \tilde{w}_l = MS.Enc(\boldsymbol{w}_l, \tilde{sk}) &= (w_l + r_l \prod_{j=1}^{\tau} p_j) \bmod q \prod_{j=1}^{\tau} p_j \\ &= (w_l + r_l \pi_{\tau}) \bmod \tilde{z}_0 \end{aligned} \tag{5.2}$$

where

$$f_l = \underset{p_1, \cdots, p_{\tau}}{\mathrm{CRT}} \big((e_l)_1 + (f_l)_1 \theta, \cdots, (e_l)_{\tau} + (f_l)_{\tau} \theta \big) \tag{5.3}$$

$$w_l = \underset{p_1, \cdots, p_{\tau}}{\mathrm{CRT}} \big((s_l)_1 + (w_l)_1 \theta, \cdots, (s_l)_{\tau} + (w_l)_{\tau} \theta \big) \tag{5.4}$$

and all the entries $(f_l)_j$ and $(w_l)_j$ in, respectively, the lth vector $\boldsymbol{f}_l \in \mathbb{N}^{\tau \times 1}$ and the the lth vector $\boldsymbol{w}_l \in \mathbb{N}^{\tau \times 1}$ belong to the set $\{0, 1, \cdots, M\}$, $(e_l)_j, (s_l)_j$ and d_l, r_l are integers uniformly chosen, respectively, from $\{-2^{\rho} + 1, \cdots, 2^{\rho} - 1\}$ and $\{0, 1, \cdots, q-1\}$, $l = 1, 2, \cdots, L$, $j = 1, 2, \cdots, \tau$, L and M are known integers.

Decryption ($MS.Dec$): The decryption of a ciphertext $\tilde{c}_{\times} \in \mathbb{N}$ is given by

$$\tilde{\boldsymbol{\nu}} = MS.Dec(\tilde{c}_{\times}, \tilde{sk}) = \begin{bmatrix} MS.Dec_1(\tilde{c}_{\times}, \theta, p_1) \\ \vdots \\ MS.Dec_{\tau}(\tilde{c}_{\times}, \theta, p_{\tau}) \end{bmatrix} \tag{5.5}$$

where $MS.Dec_j(\tilde{c}_\times, \theta, p_j)$ decrypts the same ciphertext $\tilde{c}_\times$ with different prime numbers p_j by

$$MS.Dec_j(\tilde{c}_\times, \theta, p_j) = \frac{\tilde{c}_\times \bmod p_j - (\tilde{c}_\times \bmod p_j) \bmod \theta^2}{\theta^2} \tag{5.6}$$

Evaluation ($\tilde{Eval}$): The evaluation of the ciphertexts $\tilde{f}_l, \tilde{w}_l$, $l = 1, 2, \cdots, L$ by

$$\tilde{c}_\times = \Big(\sum_{l=1}^{L} \tilde{f}_l \tilde{w}_l \Big) \bmod \tilde{z}_0 \tag{5.7}$$

decrypts to $\sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l$.

5.1.1 Conditions for the correct decryption in the MS-RHE scheme

To ensure that the MS-RHE scheme is homomorphic with respect to the Hadamard product, a sufficient condition for the correct decryption is given below.

Theorem 9. *Denote by $(f_l)_j \in \{0, 1, \cdots, M\}$ the jth entry in the lth vector $\boldsymbol{f}_l \in \mathbb{N}^{\tau \times 1}$ and by $(w_l)_j \in \{0, 1, \cdots, M\}$ the jth entry of the lth vector $\boldsymbol{w}_l \in \mathbb{N}^{\tau \times 1}$, where $l = 1, 2, \cdots, L$ and $L \in \mathbb{N} \backslash \{0\}$. Let $p_1, \cdots, p_\tau$ be τ prime numbers of bit-size ψ and θ be a positive integer. Let the vector $\boldsymbol{f}_l$ and the vector $\boldsymbol{w}_l$ be encrypted by*

$$\tilde{f}_l = MS.Enc(\boldsymbol{f}_l, \tilde{sk}) = (f_l + d_l \pi_\tau) \ mod \ \tilde{z}_0 \tag{5.8}$$

$$\tilde{w}_l = MS.Enc(\boldsymbol{w}_l, \tilde{sk}) = (w_l + r_l \pi_\tau) \ mod \ \tilde{z}_0 \tag{5.9}$$

where

$$f_l = \underset{p_1, \cdots, p_\tau}{CRT} \big((e_l)_1 + (f_l)_1 \theta, \cdots, (e_l)_\tau + (f_l)_\tau \theta \big) \tag{5.10}$$

$$w_l = \underset{p_1, \cdots, p_\tau}{CRT} \big((s_l)_1 + (w_l)_1 \theta, \cdots, (s_l)_\tau + (w_l)_\tau \theta \big) \tag{5.11}$$

and $\tilde{z}_0 = q\pi_\tau$, q is an integer uniformly chosen from $\{0, 1, \cdots, \lfloor 2^\gamma / \pi_\tau \rfloor\}$ and $\pi_\tau = \prod_{j=1}^{\tau} p_j$. The noises $(e_l)_j, (s_l)_j$ and d_l, r_l are uniformly chosen, respectively, from $\{-2^\rho + 1, \cdots, 2^\rho - 1\}$ and $\{0, 1, \cdots, q-1\}$. Let $\tilde{c}_\times$ be got by (5.7). If

$$L\big(2^{2\rho} + \theta M 2^{\rho+1}\big) + L\theta^2 M^2 < p_j, \quad \forall j \forall j = 1, 2, \cdots, \tau \tag{5.12a}$$

$$L\big(2^{2\rho} + \theta M 2^{\rho+1}\big) < \theta^2 \tag{5.12b}$$

then the decryption of $\tilde{c}_\times$ carried out by (5.5) delivers the true result of the sum of Hadamard products $\sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l$, i.e.

$$MS.Dec(\tilde{c}_\times, \tilde{sk}) = \sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l \tag{5.13}$$

Proof. Substituting (5.1) and (5.2) into (5.7), the ciphertext $\tilde{c}_\times$ is obtained by

$$\begin{aligned}
\tilde{c}_\times &= \Big(\sum_{l=1}^{L} \tilde{f}_l \tilde{w}_l \Big) \bmod \tilde{z}_0 \\
&= \Big(\sum_{l=1}^{L} \big((f_l + d_l \pi_\tau) \bmod \tilde{z}_0 \big) \big((w_l + r_l \pi_\tau) \bmod \tilde{z}_0 \big) \Big) \bmod \tilde{z}_0 \\
&= \big(\sum_{l=1}^{L} (f_l + d_l \pi_\tau)(w_l + r_l \pi_\tau) \big) \bmod \tilde{z}_0 \\
&= \sum_{l=1}^{L} (f_l + d_l \pi_\tau)(w_l + r_l \pi_\tau) - \Big\lfloor \frac{\sum_{l=1}^{L} (f_l + d_l \pi_\tau)(w_l + r_l \pi_\tau)}{\tilde{z}_0} \Big\rfloor \tilde{z}_0
\end{aligned} \tag{5.14}$$

Note that $\tilde{z}_0 = q\pi_\tau$, $\pi_\tau = \prod_{j=1}^{\tau} p_j$ and

$$\begin{aligned}
\tilde{c}_\times \bmod p_j &= \Big(\sum_{l=1}^{L} (f_l + d_l \prod_{j=1}^{\tau} p^j)(w_l + r_l \prod_{j=1}^{\tau} p^j) \\
&\qquad - \Big\lfloor \frac{\sum_{l=1}^{L} (f_l + d_l \prod_{j=1}^{\tau} p_j)(w_l + r_l \prod_{j=1}^{\tau} p_j)}{q \prod_{j=1}^{\tau} p_j} \Big\rfloor q \prod_{j=1}^{\tau} p_j \Big) \bmod p_j \\
&= \big(\sum_{l=1}^{L} f_l w_l \big) \bmod p_j \\
&= \big(\sum_{l=1}^{L} (f_l \bmod p_j)(w_l \bmod p_j) \big) \bmod p_j
\end{aligned} \tag{5.15}$$

From (5.3)-(5.4) and according to Definition 1, there is

$$f_l \bmod p_j = \underset{p_1, \cdots, p_\tau}{\mathrm{CRT}} \big((e_l)_1 + (f_l)_1 \theta, \cdots, (e_l)_\tau + (f_l)_\tau \theta \big) \bmod p_j = (e_l)_j + (f_l)_j \theta \tag{5.16}$$

$$w_l \bmod p_j = \underset{p_1, \cdots, p_\tau}{\mathrm{CRT}} \big((s_l)_1 + (w_l)_1 \theta, \cdots, (s_l)_\tau + (w_l)_\tau \theta \big) \bmod p_j = (s_l)_j + (w_l)_j \theta \tag{5.17}$$

By taking into account (5.15), it yields

$$\begin{aligned}
\tilde{c}_\times \bmod p_j &= \Big(\sum_{l=1}^{L} \big((e_l)_j + (f_l)_j \theta \big) \big((s_l)_j + (w_l)_j \theta \big) \Big) \bmod p^j \\
&= \big(\sum_{l=1}^{L} (e_l)_j (s_l)_j + \big((s_l)_j (f_l)_j + (e_l)_j (w_l)_j \big) \theta + (f_l)_j (w_l)_j \theta^2 \big) \bmod p_j
\end{aligned} \tag{5.18}$$

Recall that $(e_l)_j, (s_l)_j$ are uniformly chosen from $\{-2^\rho + 1, \cdots, 2^\rho - 1\}$ and $(f_l)_j, (w_l)_j \in \{0, 1, \cdots, M\}$. Let

$$\mathcal{N}_j(\tilde{c}_\times) = \sum_{l=1}^{L} (e_l)_j (s_l)_j + \big((s_l)_j (f_l)_j + (e_l)_j (w_l)_j \big) \theta \tag{5.19}$$

There is

$$\begin{aligned}|\mathcal{N}_j(\tilde{c}_\times)| &= \Big|\sum_{l=1}^{L}(e_l)_j(s_l)_j + \big((s_l)_j(f_l)_j + (e_l)_j(w_l)_j\big)\theta\Big| \\ &< L(2^{2\rho} + \theta M 2^{\rho+1})\end{aligned} \tag{5.20}$$

and

$$\Big|\mathcal{N}_j(\tilde{c}_\times) + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2\Big| < L\big(2^{2\rho} + \theta M 2^{\rho+1}\big) + L\theta^2 M^2 \tag{5.21}$$

If (5.12a) holds, then

$$\tilde{c}_\times \bmod p_j = \mathcal{N}_j(\tilde{c}_\times) + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2 \tag{5.22}$$

If (5.12b) holds and by substituting (5.22) into (5.6) gives

$$\begin{aligned}MS.Dec_j(\tilde{c}_\times, \theta, p_j) &= \frac{\tilde{c}_\times \bmod p_j - (\tilde{c}_\times \bmod p_j) \bmod \theta^2}{\theta^2} \\ &= \frac{\mathcal{N}_j(\tilde{c}_\times) + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2}{\theta^2} \\ &\quad - \frac{\big(\mathcal{N}_j(\tilde{c}_\times) + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2\big) \bmod \theta^2}{\theta^2} \\ &= \frac{\mathcal{N}_j(\tilde{c}_\times) + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2 - \mathcal{N}_j(\tilde{c}_\times)}{\theta^2} \\ &= \sum_{l=1}^{L}(f_l)_j(w_l)_j\end{aligned} \tag{5.23}$$

Thus, the decryption of the ciphertext $\tilde{c}_\times$ by (5.5) delivers

$$\begin{aligned}\tilde{\boldsymbol{\nu}} = MS.Dec(\tilde{c}_\times, \tilde{sk}) &= \begin{bmatrix} MS.Dec_1(\tilde{c}_\times, \theta, p_1) \\ \vdots \\ MS.Dec_\tau(\tilde{c}_\times, \theta, p_\tau)\end{bmatrix} = \begin{bmatrix} \sum_{l=1}^{L}(f_l)_1(w_l)_1 \\ \vdots \\ \sum_{l=1}^{L}(f_l)_\tau(w_l)_\tau\end{bmatrix} \\ &= \sum_{l=1}^{L}\boldsymbol{f}_l \circ \boldsymbol{w}_l\end{aligned} \tag{5.24}$$

As a result, the MS-RHE scheme is homomorphic with respect to the sum of Hadamard products. □

5.1.2 Transformation of the controller

To realize a dynamic output feedback controller in an encrypted environment by making use of the MS-RHE scheme, the dynamic output feedback controller needs to

be brought into the form of the sum of Hadamard products, which can be achieved as follows.

The evaluation process of the dynamic output feedback controller (2.3) include two parts, at first the sum of Hadamard products and then the sum of entries in the resulting vectors. According to Theorem 9, the sum of Hadamard products can be carried out based on ciphertexts. The sum of entries needs to be calculated after the decryption.

Assume that $\beta = \tau L$. The matrix $\boldsymbol{T} \in \mathbb{R}^{\alpha\times\beta}$ and the vector $\boldsymbol{g}(k) \in \mathbb{R}^{\beta\times 1}$ in (2.3) can be partitioned as

$$\boldsymbol{T} = \begin{bmatrix} \boldsymbol{t}_{11} & \cdots & \boldsymbol{t}_{1L} \\ \vdots & \ddots & \vdots \\ \boldsymbol{t}_{\alpha 1} & \cdots & \boldsymbol{t}_{\alpha L} \end{bmatrix}, \quad \boldsymbol{g}(k) = \begin{bmatrix} \boldsymbol{g}_1(k) \\ \vdots \\ \boldsymbol{g}_L(k) \end{bmatrix} \tag{5.25}$$

where $\boldsymbol{t}_{il} \in \mathbb{R}^{1\times\tau}$, $\boldsymbol{g}_l(k) \in \mathbb{R}^{\tau\times 1}$, $i = 1, 2, \cdots, \alpha$; $l = 1, 2, \cdots, L$.

Indeed if $\beta \neq \tau L$, $\boldsymbol{T}\boldsymbol{g}(k)$ can be rewritten as

$$\boldsymbol{T}\boldsymbol{g}(k) = \begin{bmatrix} \boldsymbol{T} & \boldsymbol{O}_{\alpha\times\beta_0} \end{bmatrix} \begin{bmatrix} \boldsymbol{g}(k) \\ \boldsymbol{0}_{\beta_0\times 1} \end{bmatrix} = \boldsymbol{T}'\boldsymbol{g}'(k) \tag{5.26}$$

where $\boldsymbol{T}' \in \mathbb{R}^{\alpha\times(\beta+\beta_0)}$, $\boldsymbol{g}'(k) \in \mathbb{R}^{(\beta+\beta_0)\times 1}$, $\tau = \lceil \beta/L \rceil$ and $\beta_0 = \tau L - \beta$. As $\beta + \beta_0 = \tau L$, the matrix $\boldsymbol{T}'$ and the vector $\boldsymbol{g}'(k)$ can be partitioned in the same way as in (5.25).

Then, the matrix-vector product can be equivalently rewritten as

$$\boldsymbol{T}\boldsymbol{g}(k) = \begin{bmatrix} \sum_{l=1}^{L} \boldsymbol{t}_{1l}\boldsymbol{g}_l(k) \\ \vdots \\ \sum_{l=1}^{L} \boldsymbol{t}_{\alpha l}\boldsymbol{g}_l(k) \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{\tau} h_1^j(k) \\ \vdots \\ \sum_{j=1}^{\tau} h_\alpha^j(k) \end{bmatrix} \tag{5.27}$$

where $(h_i)_j(k)$ denotes the jth entry of the vector $\boldsymbol{h}_i(k)$ given by

$$\boldsymbol{h}_i(k) = \sum\nolimits_{l=1}^{L} \boldsymbol{t}_{il}^T \circ \boldsymbol{g}_l(k) \in \mathbb{N}^{\tau\times 1} \tag{5.28}$$

and $i = 1, \cdots, \alpha$; $j = 1, \cdots, \tau$.

The MS-RHE scheme is able to calculate the vectors $\boldsymbol{h}_1(k), \cdots, \boldsymbol{h}_\alpha(k)$ in (5.28) based on ciphertexts. The sum of the entries in the vector $\boldsymbol{h}_i(k)$ in (5.27) can not be realized directly in the MS-RHE scheme and needs to be carried out after decryption. A smaller value of the parameter L reduces the number of ciphertexts transmitted over the network, but this increases the number of additions that needs to be carried out after decryption. Therefore, the choice of the parameter L depends on the available network and real-time computational capacities.

Remark 1. *Controller structures such as time-delayed control (TDC) widely used in robotics (Lee et al., 2017) and decentralized PI controllers widely used in the industry (Johansson, 2000) can be entirely rewritten as the sum of Hadamard products. In such cases, the matrix* $\boldsymbol{T}$ *in* (2.3) *has the form*

$$\boldsymbol{T} = \begin{bmatrix} \boldsymbol{T}_{11} & \cdots & \boldsymbol{T}_{1L} \\ \vdots & \ddots & \vdots \\ \boldsymbol{T}_{V1} & \cdots & \boldsymbol{T}_{VL} \end{bmatrix} \tag{5.29}$$

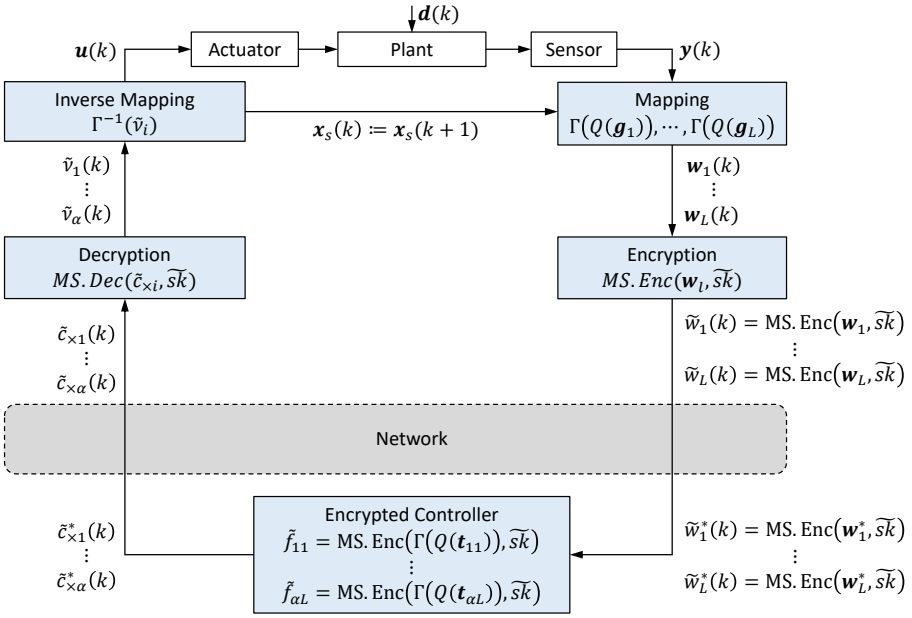

Figure 5.1: Encrypted cloud-based control system with the MS-RHE scheme

where each block $\boldsymbol{T}_{vl} \in \mathbb{R}^{\tau \times \tau}$ *is a diagonal matrix,* $l = 1, 2, \cdots, L$*;* $v = 1, 2, \cdots, V$*;* $V = \alpha/\tau$*. Then, the matrix-vector product* $\boldsymbol{T}\boldsymbol{g}(k)$ *can be equivalently rewritten as*

$$\boldsymbol{T}\boldsymbol{g}(k) = \begin{bmatrix} \sum_{l=1}^{L} \boldsymbol{T}_{1l}\boldsymbol{g}_l(k) \\ \vdots \\ \sum_{l=1}^{L} \boldsymbol{T}_{Vl}\boldsymbol{g}_l(k) \end{bmatrix} = \begin{bmatrix} \sum_{l=1}^{L} \boldsymbol{t}_{1l}^T \circ \boldsymbol{g}_l(k) \\ \vdots \\ \sum_{l=1}^{L} \boldsymbol{t}_{Vl}^T \circ \boldsymbol{g}_l(k) \end{bmatrix} \tag{5.30}$$

where $\boldsymbol{t}_{vl} \in \mathbb{R}^{1 \times \tau}$ *is the vector whose entries are the diagonal entries of the matrix* $\boldsymbol{T}_{vl}$*. As a result, in such cases the controller can be completely evaluated in an encrypted environment.*

5.1.3 Encrypted cloud-based control system

The structure of the encrypted cloud-based control system with the MS-RHE scheme is shown in Fig. 5.1. The controller parameters $\boldsymbol{A}_s$, $\boldsymbol{B}_s$, $\boldsymbol{C}_s$ and $\boldsymbol{D}_s$ are collected in the matrix $\boldsymbol{T}$ by (2.3). Consider the general case and partition the matrix $\boldsymbol{T}$ into αL vectors $\boldsymbol{t}_{il}$, $i = 1, 2, \cdots, \alpha$; $l = 1, 2, \cdots, L$ according to (5.25). Since the MS-RHE scheme allows only positive integer from the interval $\{0, 1, \cdots, M\}$, each entry of the vector $\boldsymbol{t}_{il}$ is transformed from real values to integers by using the quantization function in (3.11) and the mapping function in (3.12). Then each vector $\bar{\boldsymbol{t}}_{il}$ is encrypted by (5.1) into a single ciphertext $\tilde{f}_{il}$. Before the sensor output signals $\boldsymbol{y}(k)$ and the state vector of the controller $\boldsymbol{x}_s(k)$ are sent over the communication network, $\boldsymbol{y}(k)$ and $\boldsymbol{x}_s(k)$ are stacked together by (2.3), partitioned into L vectors $\boldsymbol{g}_1(k), \cdots, \boldsymbol{g}_L(k)$ and then mapped element-wise with the quantization function in (3.11) and the mapping function in (3.12) to $\boldsymbol{w}_1(k), \cdots, \boldsymbol{w}_L(k)$. Each vector $\boldsymbol{w}_l(k)$ is encrypted by (5.2) into a single ciphertext $\tilde{w}_l(k)$ and then transmitted over the net-

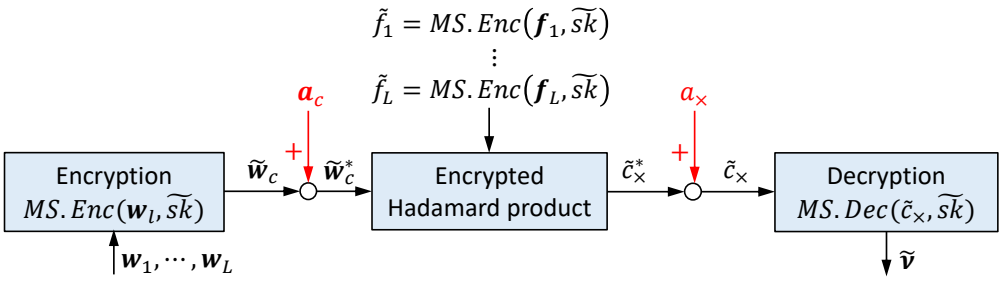

Figure 5.2: Attacks on the signals encrypted by the MS-RHE scheme

work. On the controller side, each ciphertext $\tilde{w}_l^*(k)$ is processed by the evaluation procedure $\tilde{c}_{\times i}^*(k) = \left(\sum_{l=1}^{L} \tilde{f}_{il}\tilde{w}_l^*(k)\right) \bmod \tilde{z}_0$ in (5.7). The ciphertexts $\tilde{c}_{\times 1}(k), \cdots, \tilde{c}_{\times\alpha}(k)$ arriving at the plant side will be decrypted by (5.5) and then the sum of the entries is calculated to obtain $\tilde{\nu}_1(k), \cdots, \tilde{\nu}_\alpha(k)$. By applying the inverse mapping function in (3.13) on each value $\tilde{\nu}_1(k), \cdots, \tilde{\nu}_\alpha(k)$, the state vector of the controller $\boldsymbol{x}_s(k+1)$ and the control input signals $\boldsymbol{u}(k)$ are obtained. For the next controller cycle, the state vector $\boldsymbol{x}_s(k)$ is set to $\boldsymbol{x}_s(k+1)$, i.e. $\boldsymbol{x}_s(k) := \boldsymbol{x}_s(k+1)$.

5.1.4 Network capacity needed by the MS-RHE scheme

In this subsection, the reduction of the network load achieved by the MS-RHE scheme will be analyzed.

The MS-RHE scheme encrypts τ plaintexts into a single ciphertext. Therefore, the number of ciphertexts transferred over the network can be reduced to $1/\tau = L/\beta$ (If $\beta \neq \tau L$, then $1/\tau = L/(\beta+\beta_0)$) of the previous number of ciphertexts. As the length of the ciphertexts keeps unchanged when multiple plaintexts are encrypted into a single ciphertext, the network communication load in the sensor output channels is decreased to $1/\tau$ of the former network load. For the controller structures mentioned in Remark 1, as the number of signals obtained after the evaluation of the controller is decreased to $V = \alpha/\tau$, the network communication load in both the sensor output channels and the control input channels is reduced to $1/\tau$ of the previous network load.

5.2 Resilience of multi-slot homomorphic encryption

In this section, it will be shown that, even though multiple plaintexts are encrypted into a single ciphertext, the MS-RHE scheme is resilient to additive attacks. For this purpose, assume that two attacks are imposed on the ciphertexts going through the communication channels as shown in Fig. 5.2. The first additive attack $\boldsymbol{a}_c$ is injected into the signal $\tilde{\boldsymbol{w}}_c = [\tilde{w}_1 \cdots \tilde{w}_L]^T$ obtained due to (5.2). The second additive attack $a_\times$ is injected into the ciphertext $\tilde{c}_\times^*$ obtained after carrying out the sum of Hadamard products encrypted in (5.7). Now the behaviour of the result $\tilde{\boldsymbol{\nu}}$ obtained after the

decryption (5.5) will be analyzed.

Theorem 10. *Assume that the vector* $\boldsymbol{f}_l = [(f_l)_1 \cdots (f_l)_\tau]^T \in \mathbb{N}^{\tau\times 1}$ *is encrypted by* (5.1) *to the scalar* $\tilde{f}_l$ *and the vector* $\boldsymbol{w}_l = [(w_l)_1 \cdots (w_l)_\tau]^T \in \mathbb{N}^{\tau\times 1}$ *is encrypted by* (5.2) *to the scalar* $\tilde{w}_l$*, where* $l = 1, 2, \cdots, L$ *and* $L \in \mathbb{N}\backslash\{0\}$*. Let* $\boldsymbol{a}_c = [a_1, \cdots, a_L]^T$ *and* $a_\times$ *denote additive attacks on, respectively, the ciphertexts* $\tilde{\boldsymbol{w}}_c = [\tilde{w}_1 \cdots \tilde{w}_L]^T$ *and* $\tilde{c}_\times$*, i.e.*

$$\begin{aligned} \tilde{\boldsymbol{w}}_c^* &= \tilde{\boldsymbol{w}}_c + \boldsymbol{a}_c \\ \tilde{c}_\times &= \tilde{c}_\times^* + a_\times \end{aligned} \tag{5.31}$$

where $\tilde{c}_\times^* = (\sum_{l=1}^{L} \tilde{f}_l \tilde{w}_l')$ *mod* $\tilde{z}_0$ *is got by* (5.7) *and* $\tilde{w}_l' = \tilde{w}_l + a_l$ *denotes the* l*th entry of the vector* $\tilde{\boldsymbol{w}}_c^*$*. Then, the result* $\tilde{\boldsymbol{\nu}}$ *obtained by the decryption in* (5.5) *is* $\tilde{\boldsymbol{\nu}} = \sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l$ *as long as*

$$\delta p_j - \mathcal{N}_j(\tilde{c}_\times) \le \mathcal{N}_j(a_l) + a_\times < \delta p_j + \theta^2 - \mathcal{N}_j(\tilde{c}_\times) \tag{5.32}$$

where $\mathcal{N}_j(\tilde{c}_\times) = \sum_{l=1}^{L}(e_l)_j(s_l)_j + \big((s_l)_j(f_l)_j + (e_l)_j(w_l)_j\big)\theta$*,* $\mathcal{N}_j(\tilde{a}_l) = \sum_{l=1}^{L}\big((e_l)_j + (f_l)_j\theta\big)a_l$ *and* $\delta \in \{0, 1, \cdots, q-1\}$*.*

Proof. According to (5.2), the encryption of $\boldsymbol{w}_l$ gives

$$\tilde{w}_l = MS.Enc(\boldsymbol{w}_l, \tilde{sk}) = (w_l + r_l\pi_\tau) \bmod \tilde{z}_0 \tag{5.33}$$

where $\tilde{z}_0 = q\pi_\tau$, q is an integer and $\pi_\tau = \prod_{j=1}^{\tau} p_j$. In consequence of $\boldsymbol{a}_c = [a_1 \cdots a_L]^T$,

$$\begin{aligned} \tilde{w}_l' = \tilde{w}_l + a_l &= MS.Enc(\boldsymbol{w}_l, \tilde{sk}) + a_l \\ &= (w_l + r_l\pi_\tau) \bmod \tilde{z}_0 + a_l \end{aligned} \tag{5.34}$$

Due to (5.1) and (5.7), the ciphertext $\tilde{c}_\times^*$ is

$$\tilde{c}_\times^* = \big(\sum_{l=1}^{L} \tilde{f}_l \tilde{w}_l'\big) \bmod \tilde{z}_0 \tag{5.35}$$

Because of the attack $a_\times$ and considering (5.14), there is

$$\begin{aligned} \tilde{c}_\times &= \tilde{c}_\times^* + a_\times = \big(\sum_{l=1}^{L} \tilde{f}_l \tilde{w}_l'\big) \bmod \tilde{z}_0 + a_\times \\ &= \sum_{l=1}^{L}(f_l + d_l\pi_\tau)(w_l + r_l\pi_\tau + a_l) - \Big\lfloor \frac{\sum_{l=1}^{L}(f_l + d_l\pi_\tau)(w_l + r_l\pi_\tau + a_l)}{\tilde{z}_0} \Big\rfloor \tilde{z}_0 + a_\times \\ &= \sum_{l=1}^{L}(f_l + d_l q\prod_{j=1}^{\tau} p_j)(w_l + a_l + r_l q\prod_{j=1}^{\tau} p_j) \\ &\quad - \Big\lfloor \frac{\sum_{l=1}^{L}(f_l + d_l q\prod_{j=1}^{\tau} p_j)(w_l + a_l + r_l q\prod_{j=1}^{\tau} p_j)}{q\prod_{j=1}^{\tau} p_j} \Big\rfloor q\prod_{j=1}^{\tau} p_j + a_\times \end{aligned} \tag{5.36}$$

Note that

$$\begin{aligned}
\tilde{c}_\times \bmod p_j &= \Big(\big(\sum_{l=1}^{L} f_l(w_l + a_l) \big) + a_\times \Big) \bmod p_j \\
&= \Big(\Big(\sum_{l=1}^{L} \big((e_l)_j + (f_l)_j\theta\big)\big((s_l)_j + (w_l)_j\theta + a_l\big) \Big) + a_\times \Big) \bmod p_j \\
&= \Big(\Big(\sum_{l=1}^{L} (e_l)_j(s_l)_j + \big((s_l)_j(f_l)_j + (e_l)_j(w_l)_j\big)\theta + \sum_{l=1}^{L} \big((e_l)_j + (f_l)_j\theta\big)a_l \\
&\quad + \sum_{l=1}^{L} (f_l)_j(w_l)_j\theta^2 \Big) + a_\times \Big) \bmod p_j
\end{aligned} \tag{5.37}$$

If the lth entry a_l of the attack $\boldsymbol{a}_c$ and the attack $a_\times$ satisfy (5.32), then $\delta p_j \leq \mathcal{N}_j(\tilde{c}_\times) + \mathcal{N}_j(a_l) + a_\times < \delta p_j + \theta^2$, where $\mathcal{N}_j(\tilde{c}_\times) = \sum_{l=1}^{L}(e_l)_j(s_l)_j + \big((s_l)_j(f_l)_j + (e_l)_j(w_l)_j\big)\theta$, $\mathcal{N}_j(a_l) = \sum_{l=1}^{L}\big((e_l)_j + (f_l)_j\theta\big)a_l$ and $\delta \in \{0, 1, \cdots, q-1\}$. Let

$$\mathcal{N}_j(\tilde{c}_\times) + \mathcal{N}_j(a_l) + a_\times = \delta p_j + \Delta \tag{5.38}$$

where $\Delta \in \{0, 1, \cdots, \theta^2\}$. Thus,

$$\begin{aligned}
\tilde{c}_\times \bmod p_j &= (\mathcal{N}_j(\tilde{c}_\times) + \mathcal{N}_j(a_l) + a_\times + \textstyle\sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2) \bmod p_j \\
&= (\delta p_j + \Delta + \textstyle\sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2) \bmod p_j \\
&= \Delta + \textstyle\sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2
\end{aligned} \tag{5.39}$$

Due to the decryption (5.5), it yields

$$\begin{aligned}
MS.Dec_j(\tilde{c}_\times, \theta, p_j) &= \frac{\tilde{c}_\times \bmod p_j - (\tilde{c}_\times \bmod p_j) \bmod \theta^2}{\theta^2} \\
&= \frac{\Delta + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2 - (\Delta + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2) \bmod \theta^2}{\theta^2} \\
&= \frac{\Delta + \sum_{l=1}^{L}(f_l)_j(w_l)_j\theta^2 - \Delta}{\theta^2} \\
&= \sum_{l=1}^{L}(f_l)_j(w_l)_j
\end{aligned} \tag{5.40}$$

i.e. each entry $MS.Dec_j(\tilde{c}_\times, \theta, p_j)$ of the vector $\tilde{\boldsymbol{\nu}} \in \mathbb{N}^{\tau\times 1}$ delivers the correct result of $\sum_{l=1}^{L}(f_l)_j(w_l)_j$. Thus, $\tilde{\boldsymbol{\nu}} = \sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l$. □

Theorem 10 tells us that additive attacks imposed on the ciphertexts obtained by the MS-RHE can still be neutralized so that the controller can get the true sensor information and the actuators can get the true control input signals.

5.3 Security proof and parameter selection

In this section, a guideline for the parameter selection of the MS-RHE scheme will be provided. Moreover, the security requirement of IND-CPA with the MS-RHE scheme will be discussed.

5.3.1 Security analysis

The difference in the parameter selection of the RHE scheme in Section 3.3 and the MS-RHE scheme in Section 5.1 is the divisor in the modulo operations, namely, $z_0 = qp$ and $\tilde{z}_0 = q\prod_{j=1}^{\tau} p_j$. It has been proven in Section 3.5.1 that the RHE scheme satisfies the security requirement of IND-CPA. Because the divisor $\tilde{z}_0 = q\prod_{j=1}^{\tau} p_j$ in the modulo operations in the MS-RHE scheme is chosen as in the batched AGCD distribution given in Definition 6 and there does not exist an algorithm that can figure out the prime numbers $p^1, \cdots, p^\tau$ used in the divisor $\tilde{z}_0 = q\prod_{j=1}^{\tau} p_j$ in the modulo operations in polynomial time (Benarroch et al., 2017), it could be believed that the MS-RHE scheme also satisfies IND-CPA. However, it remains a challenge to formally prove the security requirement of IND-CPA for the MS-RHE in a similar manner as shown in Section 3.5.1 for the RHE scheme.

5.3.2 Selection of parameters

Now, a guideline for the selection of the parameters ρ, θ, ψ and γ in the MS-RHE scheme will be given. By following this guideline, the MS-RHE scheme is homomorphic with respect to the sum of Hadamard products and simultaneously secure against the main families of known attacks introduced in Section 3.5.2.

To obtain the true result of the sum of Hadamard products $\sum_{l=1}^{L} \boldsymbol{f}_l \circ \boldsymbol{w}_l$ after the decryption (5.5), the integer θ and the prime numbers $p_1, \cdots, p_\tau$ in the secret key $sk = (\theta, p_1, \cdots, p_\tau)$ need to satisfy (5.12). Moreover, in order to ensure the main families of known attacks are not able to gain access to the secret key $sk = (\theta, p_1, \cdots, p_\tau)$, the bit-size ρ of the noises in (5.1) and (5.2), the bit-size ψ of the prime numbers $p_1, \cdots, p_\tau$ and the bit-size γ of the ciphertext space should satisfy further conditions.

The parameters ρ, θ, ψ and γ of the MS-RHE scheme in Section 5.1 can be systematically determined as follows.

Step 1: Choose the security level κ according to National Institute of Standards and Technology (2020).

Step 2: Set $\rho = 2\kappa$ to satisfy (3.65) and select the integer θ so that (5.12b) holds.

Step 3: Select the bit-size ψ and the prime numbers $p_1, \cdots, p_\tau$ so that condition (3.68a) and condition (5.12a) are fulfilled simultaneously.

Step 4: Choose the bit-size γ of the ciphertext to satisfy condition (3.68b) and condition (3.69) simultaneously.

5.4 Simulation example

In this section, an example will be given to illustrate the cloud-based control system encrypted by the MS-RHE scheme. In the simulation, the quadruple-tank system and the dynamic output feedback controller introduced in Section 2.3 are used.

To reduce the network communication load by 50%, τ is set as $\tau = 2$. The bound of the plaintext is $M = 2^{\lambda_1+\lambda_2+1} = 2^{21}$, where $\lambda_1 = 4$ and $\lambda_2 = 16$.

At first, the security level κ is required. In the simulation, the security level is chosen as $\kappa = 128$ according to National Institute of Standards and Technology (2020). Then, the bit-size ρ of the noises $(e_l)_j, (s_l)_j$ in the ciphertexts (5.1), (5.2) is $\rho = 2\kappa = 256$ to satisfy (3.65). In order to fulfil (5.12) and achieve a correct decryption, select $\theta = 2^{303}$. The bit-size ψ of the prime numbers p_1, p_2 is selected as $\psi = 697$ to satisfy simultaneously condition (3.68a) and condition (5.12a). Finally, the bit-size γ of the ciphertext space is chosen as $\gamma = 353056$ to satisfy simultaneously condition (3.68b) and condition (3.69).

Recall that the controller parameters of the dynamic output feedback controller in (2.3) are

$$\boldsymbol{T} = \begin{bmatrix} \boldsymbol{A}_s & \boldsymbol{B}_s \\ \boldsymbol{C}_s & \boldsymbol{D}_s \end{bmatrix} = \left[\begin{array}{cc|cc} 1 & 0 & 0.0625 & 0 \\ 0 & 1 & 0 & 0.01563 \\ \hline 0.032 & 0 & 1 & 0 \\ 0 & -0.0192 & 0 & -0.3 \end{array}\right] \tag{5.41}$$

The controller parameters $\boldsymbol{A}_s$, $\boldsymbol{B}_s$, $\boldsymbol{C}_s$, $\boldsymbol{D}_s$ stacked together in $\boldsymbol{T} \in \mathbb{R}^{4\times4}$ consists of the diagonal matrices $\boldsymbol{T}_{11}, \boldsymbol{T}_{12}, \boldsymbol{T}_{21}, \boldsymbol{T}_{22} \in \mathbb{R}^{2\times2}$. Therefore, the vectors

$$\begin{aligned} \boldsymbol{t}_{11} &= \begin{bmatrix} 1 & 1 \end{bmatrix}, \ \boldsymbol{t}_{12} = \begin{bmatrix} 0.0625 & 0.01563 \end{bmatrix} \\ \boldsymbol{t}_{21} &= \begin{bmatrix} 0.032 & -0.0192 \end{bmatrix}, \ \boldsymbol{t}_{22} = \begin{bmatrix} 1 & -0.3 \end{bmatrix} \end{aligned} \tag{5.42}$$

can be obtained, which are mapped element-wise to integers by (3.11), (3.12) and then encrypted by (5.1) to $\tilde{f}_{11}, \tilde{f}_{12}, \tilde{f}_{21}, \tilde{f}_{22} \in \mathbb{N}$.

In each controller cycle, the state vector of the controller $\boldsymbol{x}_s(k) \in \mathbb{R}^{2\times1}$ and the sensor output signals $\boldsymbol{y}(k) \in \mathbb{R}^{2\times1}$ are mapped element-wise to integers by using the mapping functions in (3.11), (3.12) and then encrypted by (5.2) to the ciphertexts $\tilde{w}_1(k), \tilde{w}_2(k) \in \mathbb{N}$ and then sent to the encrypted controller. That means, only two ciphertexts instead of four ciphertexts are sent over the sensor output channels at each sampling time. After the evaluation of the encrypted controller, only the two ciphertexts $\tilde{c}^*_{\times1}(k) = \left(\sum_{l=1}^{2} \tilde{f}_{1l}\tilde{w}^*_l(k)\right) \bmod \tilde{z}_0$ and $\tilde{c}^*_{\times2}(k) = \left(\sum_{l=1}^{2} \tilde{f}_{2l}\tilde{w}^*_l(k)\right) \bmod \tilde{z}_0$ instead of four ciphertexts are transferred over the control input channels.

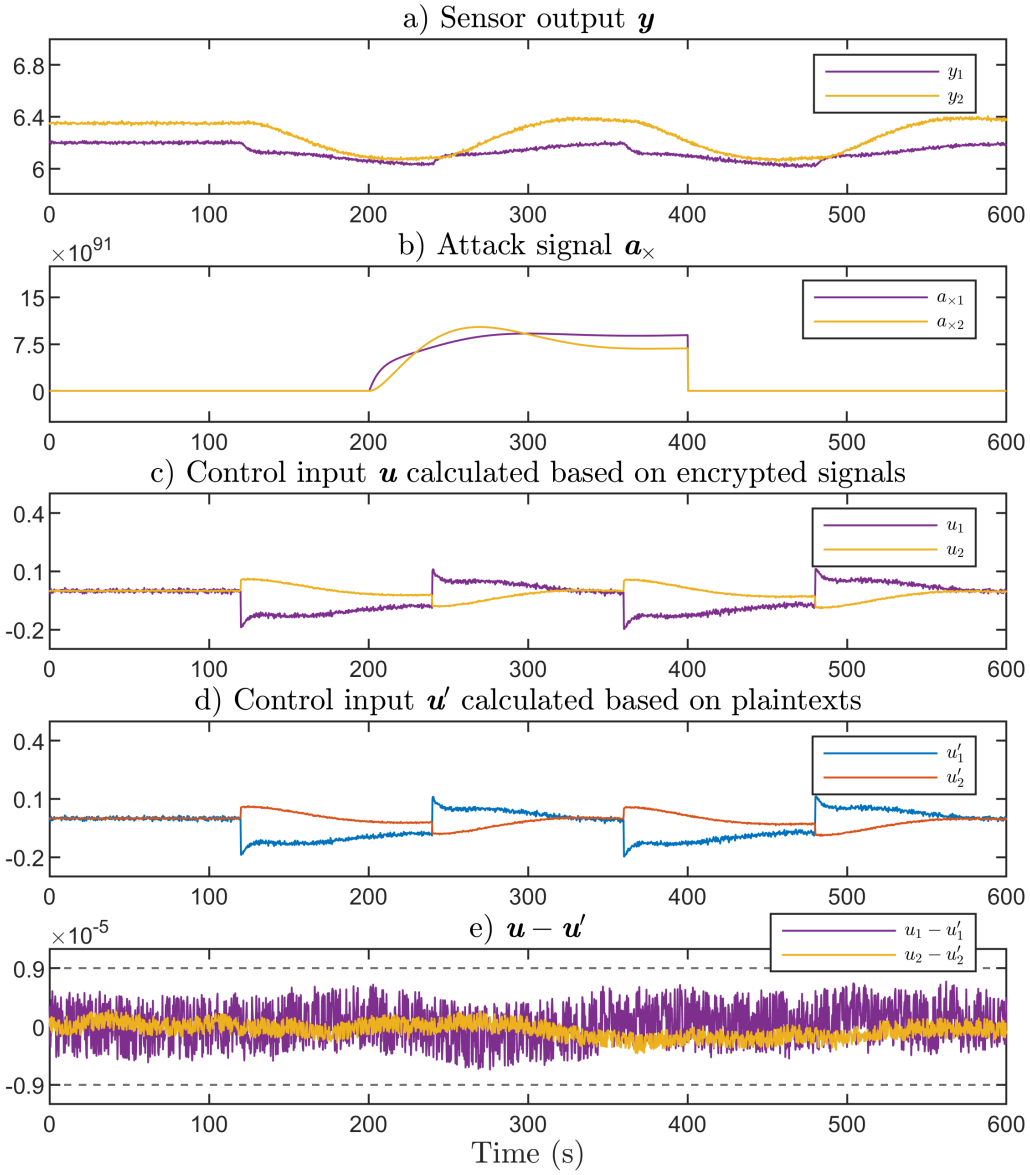

Figure 5.3: Encrypted cloud-based control system with the MS-RHE scheme

Due to the bit-size $\gamma = 353056$ of the ciphertexts, the ciphertexts $\tilde{w}_1(k)$, $\tilde{w}_2(k)$ and the ciphertexts $\tilde{c}^*_{\times 1}(k)$, $\tilde{c}^*_{\times 2}(k)$ got after the evaluation process of the controller are omitted here.

During the simulation, an attack is imposed on the encrypted control input signals (i.e. $\boldsymbol{a}_\times(k) = [0\ 0\ a_{\times 1}(k)\ a_{\times 2}(k)]^T$) from $k = 200s$ to $k = 400s$ (see Fig. 5.3b), while there is no attack on the sensor output channels (i.e. $\boldsymbol{a}_c(k) = \boldsymbol{0}$). Fig. 5.3c shows the control input signals $\boldsymbol{u}(k)$ received by the actuators got after the decryption. For comparison, the control input signals $\boldsymbol{u}'(k)$ generated by the classical feedback controller in the form of (2.2) and (2.7) is shown in Fig. 5.3d, which is got based on the controller parameters and the sensor output signals in plaintexts. Between $k = 200s$ and $k = 400s$, the attacks $a_{\times 1}(k), a_{\times 2}(k)$ shown in Fig. 5.3b are imposed, respectively,

on the ciphertexts $\tilde{c}^*_{\times 1}(k), \tilde{c}^*_{\times 2}(k)$ got after the evaluation process. However, no difference between $\boldsymbol{u}'(k)$ and $\boldsymbol{u}(k)$ can be observed, because the attacks $a_{\times 1}(k), a_{\times 2}(k)$ are inside of the resilience range $a_{\times i} < p_j + \theta^2 - \mathcal{N}_j(\tilde{c}_{\times i})$ and are neutralized thanks to the MS-RHE scheme, where $\mathcal{N}_j(\tilde{c}_{\times i}) = \sum_{l=1}^{2}(e_l)_j(s_l)_j + \big((s_l)_j(f_l)_j + (e_l)_j(w_l)_j\big)\theta$ and $i, j = 1, 2$. That means, the true values of the control input signals $\boldsymbol{u}(k)$ are available to the actuators even in the case of the attacks $a_{\times 1}(k)$, $a_{\times 2}(k)$. The slight difference between $\boldsymbol{u}(k)$ obtained after the decryption and $\boldsymbol{u}'(k)$ calculated directly based on plaintexts (see Fig. 5.3e) is only caused by the transformation (3.11) between the real values and the quantized values. The quantization error is bounded by $\forall k$, $|u_i(k) - u'_i(k)| \leq 0.9 \times 10^{-5}$, $i = 1, 2$ (see Fig. 5.3e).

In summary, the MS-RHE scheme not only reduces the network communication load but also neutralizes the effect of additive attacks imposed on the ciphertexts transmitted over the communication channels. The control performance of the encrypted cloud-based control system is almost the same as achieved by the controller which is calculated with plaintexts.

5.5 Discussion

In this chapter, the MS-RHE scheme is proposed, which not only reduces the network load of an encrypted cloud-based control system but also neutralizes additive attacks imposed on the ciphertexts. The key idea is to explore the CRT to generate ciphertexts that contain the information of multiple plaintexts, while the length of the ciphertext keeps unchanged. Thus, the network load is significantly reduced. The MS-RHE scheme is homomorphic with respect to the sum of Hadamard products. It is shown how to bring a dynamic output feedback controller into the form of the sum of Hadamard products to operate with ciphertexts. Moreover, it is proven that the MS-RHE scheme still neutralizes additive attacks injected into the encrypted control system. To achieve the desired security level against the main families of known attacks by making use of the MS-RHE scheme, a procedure for the selection of the parameters in the MS-RHE scheme is provided.

The MS-RHE scheme is validated with the help of the well-established quadruple-tank system. The simulation results demonstrate the significant network load reduction of the MS-RHE scheme. Furthermore, an additive attack imposed on the ciphertexts sent over the network has no influence on the control input signals received by the actuators. Therefore, the cloud-based control system encrypted by the MS-RHE scheme can still operate even in the case of an attack.

6 Practical Aspects of Homomorphic Encryption Schemes

The main objective of this chapter is to investigate important aspects, such as network load and cloud storage, relevant to practical applications utilizing encrypted cloud-based control systems. In practical applications, the controller should react to the changes in the sensor output signals in pre-defined time, mostly inside one sampling period. The networks have usually limited bandwidth. The required storage needs to be reserved beforehand. Therefore, the proposed encryption schemes, namely, the RHE scheme in Section 3.3, the PQS-RHE scheme in Section 4.1 and the MS-RHE scheme in Section 5.1 are analyzed theoretically and practically. Moreover, the learning with errors (LWE)-based HE scheme given by Kim et al. (2020) is employed in this investigation.

The proposed encryption schemes will be theoretically analysed in terms of the network capacity required to transmit the ciphertexts over the communication channels and the cloud storage needed by the encrypted controller parameters. In order to check whether the real-time requirements can be satisfied by these encryption schemes, the execution time of the encrypted controller, the network load and the used cloud storage of the encrypted controller parameters under different security levels will be analyzed. Moreover, the proposed encryption schemes will be compared to the LWE-based HE scheme given by Kim et al. (2020) in these aspects.

This chapter is organized as follows. In Section 6.1, the requirement of network capacity and the usage of cloud storage of the encryption schemes proposed in this doctoral study are analyzed. In Section 6.2, the influence of the security level on computational efforts, network load and used cloud storage is shown and the proposed encryption schemes are also compared in these aspects. Moreover, the LWE-based HE scheme is considered in this investigation.

6.1 Theoretical analysis

In this section, the network capacity required to transmit the ciphertexts over the communication channels and the used cloud storage needed by the encrypted controller parameters will be theoretically analyzed. These aspects play an essential role for the practical applicability of an encryption scheme.

Table 6.1: Network load and used cloud storage of the encryption schemes

Practical aspect	**RHE scheme** (Sec. 3.3)	**PQS-RHE scheme** (Sec. 4.1)	**MS-RHE scheme** (Sec. 5.1, Eq. (5.25) / Eq. (5.29))
Network load of all control inputs in (Bit)	$\gamma\alpha$	$\gamma\alpha$	$\gamma\alpha$ / $\gamma\alpha\frac{1}{\tau}$
Network load of all sensor outputs in (Bit)	$\gamma\beta$	$\gamma\beta$	$\gamma\beta\frac{1}{\tau}$ / $\gamma\beta\frac{1}{\tau}$
Used cloud storage for controller parameters in (Bit)	$\gamma\alpha\beta$	$\gamma\alpha\beta\phi$	$\gamma\alpha\beta\frac{1}{\tau}$ / $\gamma\alpha\beta\frac{1}{\tau^2}$

6.1.1 Network load

The network capacity needed to send ciphertexts over the network is summarized in Table 6.1.

The network load is calculated by counting the number of bits going through the sensor output channels and the control input channels in a single controller cycle.

RHE scheme: The RHE scheme transmits the vector $\boldsymbol{w}_c \in \mathbb{N}^{\beta\times 1}$ (3.35) over the sensor output channels and the vector $\boldsymbol{c}_\times \in \mathbb{N}^{\alpha\times 1}$ (3.37) over the control input channels. The network load is given by the number of ciphertexts and the bit-size of each ciphertext. Thus, the network load in the RHE scheme is $\beta \log_2(z_0)$ bits and $\alpha \log_2(z_0)$ bits, where $\log_2(z_0) = \gamma$.

PQS-RHE scheme: The encrypted vectors obtained by the PQS-RHE scheme transmitted over the sensor output channels and the control input channels are denoted, respectively, by $\overline{\boldsymbol{w}}_c \in \mathbb{N}^{\beta\times 1}$ (4.15) and $\overline{\boldsymbol{c}}_\times \in \mathbb{N}^{\alpha\times 1}$ (4.17). Thus, the total amount of bits going through the sensor output channels and the control input channels is given, respectively, by $\gamma\beta$ and $\gamma\alpha$.

MS-RHE scheme: The MS-RHE scheme transmits the ciphertexts $\tilde{w}_1, \cdots, \tilde{w}_L$ obtained by (5.2) and the ciphertexts $\tilde{c}_{\times 1}, \cdots, \tilde{c}_{\times\alpha}$ obtained by (5.7) over the communication channels, which gives the network load of, respectively, $\gamma\beta/\tau$ bits and $\gamma\alpha$ bits, where $L = \beta/\tau$. Assume that the controller can be brought into the form (5.29), then the MS-RHE scheme transmits the ciphertexts $\tilde{w}_1, \cdots, \tilde{w}_L$ obtained by (5.2) and the ciphertexts $\tilde{c}_{\times 1}, \cdots, \tilde{c}_{\times V}$ obtained by (5.7) over the communication channels, where $V = \alpha/\tau$. As a result, the network load can be further reduced by the MS-RHE scheme, i.e. $\gamma\beta/\tau$ bits going through the sensor output channels and $\gamma\alpha/\tau$ bits going through the control input channels.

If we take a look at Table 6.1, it can be seen that the lowest network capacity required to transmit the ciphertexts over the communication channels can be achieved with the MS-RHE scheme. Considering the MS-RHE scheme in the form of (5.29), the network load in the MS-RHE scheme is reduced to $1/\tau$ of the network load required

by both the RHE scheme and the PQS-RHE scheme.

6.1.2 Cloud storage

The cloud storage used for the encrypted controller parameters is summarized in Table 6.1.

The used cloud storage of the encrypted parameter matrix of the controller in the cloud depends mainly on the number of integers and the bit-size of each integer.

RHE scheme: The encrypted parameter matrix of the controller in the RHE scheme is denoted by $\boldsymbol{F}_c \in \mathbb{N}^{\alpha\times\beta}$ (3.34). Hence, the number of integers is $\alpha\beta$ and the bit-size of each integer is $\gamma = \log_2(z_0)$, which gives the total used cloud storage of $\gamma\alpha\beta$ bits.

PQS-RHE scheme: The matrix $\overline{\boldsymbol{F}}_c \in \mathbb{N}^{\alpha\times\beta\phi}$ (4.14) is the encrypted controller parameters in the PQS-RHE scheme and consists of γ bit-sized ciphertexts. Thus, the total used cloud storage of the PQS-RHE scheme is $\gamma\alpha\beta\phi$ bits.

MS-RHE scheme: Considering the general case (5.25), the ciphertexts $\tilde{f}_{11}, \cdots, \tilde{f}_{\alpha L}$ (5.1) of bit-size γ are the encrypted parameter matrix of the controller in the MS-RHE scheme, where $L = \beta/\tau$. Hence, the reserved cloud storage is $\gamma\alpha\beta/\tau$ bits. If the controller parameters can be brought into the form (5.29), then the ciphertexts $\tilde{f}_{11}, \cdots, \tilde{f}_{VL}$ (5.1) of bit-size γ are the encrypted controller parameters, where $V = \alpha/\tau$. Consequently, the total used cloud storage of the MS-RHE scheme is $\gamma\alpha\beta/\tau^2$ bits.

If we take a look at Table 6.1, it can be seen that the MS-RHE scheme needs the least amount of cloud storage for the encrypted controller parameters. It is worth noticing that, if the controller can be brought into the form (5.29), the cloud storage needed by the MS-RHE scheme is significantly less than compared to the RHE scheme and the PQS-RHE scheme.

6.2 Practical analysis

In this section, the execution time of the encrypted controller, the requirement on network capacity and the usage of cloud storage of the encryption schemes proposed in this doctoral study under different security levels will be analyzed. Moreover, the LWE-based HE scheme given by Kim et al. (2020) will also be considered in this investigation.

6.2.1 Execution time

In this subsection, the execution time of the controller encrypted by the RHE scheme, the PQS-RHE scheme, the MS-RHE scheme and the LWE-based HE scheme given by Kim et al. (2020) will be analyzed.

In the simulations, the plant is described by (2.6) and the parameters of the dynamic output feedback controller are given by (2.7). The simulations have been executed on a PC with an Intel Core i7-8565U processor and 16 GB Ram running Windows 10. The algorithms of the RHE scheme, the PQS-RHE scheme, the MS-RHE scheme and the LWE-based HE scheme given by Kim et al. (2020) have been implemented using the same programming language Python. In addition, the external library GMPY2 has been utilized, because GMPY2 can handle large integer arithmetic faster than pure Python. The time limit for executing an algorithm, such as encryption, evaluation, and decryption, is set to 60s. For this investigation, assume that there is no attack.

Table 6.2 sums up the parameters used in the simulations for the encryption schemes proposed in this doctoral study. Moreover, the mean execution time of the encryption, the decryption and the evaluation function of the proposed encryption schemes and the LWE-based HE scheme given by Kim et al. (2020) are provided. Algorithms exceeding the time limit of 60s are identified with a "-" in the row of the corresponding security level κ.

It can be seen in Table 6.2 that the MS-RHE scheme outperforms the other encryption schemes in terms of evaluating the control law in ciphertexts. For low- and mid-sized security levels (i.e. $\kappa = \{80, 112, 128\}$), the MS-RHE scheme has the lowest mean execution time for encryption. For a high security level (i.e. $\kappa = \{192, 256\}$), the PQS-RHE scheme has the lowest mean executing time for encryption. Considering the mean execution time for decryption, the RHE scheme performs best for low- and mid-sized security level (i.e. $\kappa = \{80, 112, 128\}$), while the PQS-RHE scheme outperforms the other encryption schemes for a high security level (i.e. $\kappa = \{192, 256\}$). It is worth noticing that for any security level κ the mean time to execute a control cycle (i.e. the sum of encryption, decryption and controller calculation) using any encryption scheme proposed in this doctoral study is much less than that for the LWE-based HE scheme.

The above analysis shows that the encryption schemes proposed in this doctoral study can be applied in practice to increase the cyber security of cloud-based control systems. As the proposed encryption schemes offer various benefits for the cloud-based control system, the choice of an encryption scheme for a practical application depends on the security level κ and the available real-time computational capacity.

Table 6.2: Execution time of the encryption schemes

Security level κ	Parameters / Mean time of encryption, decryption, evaluation in (ms) **RHE scheme** (Sec. 3.3)	**PQS-RHE scheme** (Sec. 4.1)	**MS-RHE scheme** (Sec. 5.1)	**LWE-based HE scheme** (Kim et al. (2020))
80	$\rho, \theta, \psi, \gamma$ 160, 207, 505, 276160 / 0.93, 0.47, 40.88	$\log_2(b), \rho, \theta, \psi, \gamma$ 128, 160, 345, 778, 494559 / 1.74, 0.97, 7.15×10^3	$\rho, \theta, \psi, \gamma$ 160, 207, 505, 276160 / 0.85, 0.95, 8.49	5.63, 1.58, -
112	$\rho, \theta, \psi, \gamma$ 224, 271, 633, 327424 / 1.13, 0.62, 49.92	$\log_2(b), \rho, \theta, \psi, \gamma$ 128, 224, 410, 908, 547423 / 2.00 , 1.13, 9.23×10^3	$\rho, \theta, \psi, \gamma$ 224, 271, 633, 327424 / 0.99, 1.25, 9.97	7.37, 2.11, -
128	$\rho, \theta, \psi, \gamma$ 256, 303, 697, 353056 / 1.27, 0.70, 56.85	$\log_2(b), \rho, \theta, \psi, \gamma$ 128, 256, 445, 978, 577856 / 2.48, 1.52, 12.35×10^3	$\rho, \theta, \psi, \gamma$ 256, 303, 697, 353056 / 1.12, 1.41, 11.05	8.83, 2.40, -
192	$\rho, \theta, \psi, \gamma$ 384, 431, 1252, 694784 / 2.85, 1.84, 130.30	$\log_2(b), \rho, \theta, \psi, \gamma$ 128, 384, 570, 1228, 675584/ 2.75, 1.69, 16.99×10^3	$\rho, \theta, \psi, \gamma$ 384, 431, 1252, 694784 / 4.85, 2.91, 23.06	12.58, 3.69, -
256	$\rho, \theta, \psi, \gamma$ 512, 560, 2089, 1262112 / 5.28, 4.27, 248.32	$\log_2(b), \rho, \theta, \psi, \gamma$ 128, 512, 698, 1484, 778112 / 3.23, 2.08, 21.14×10^3	$\rho, \theta, \psi, \gamma$ 512, 560, 2089, 1262112 / 12.66, 7.29, 31.16	15.87, 4.82, -

Table 6.3: Network load and used cloud storage of the encryption schemes

	Network load of all inputs, outputs in (MB/s) / Cloud storage needed by the encrypted controller in (MB)			
Security level κ	**RHE scheme** (Sec. 3.3)	**PQS-RHE scheme** (Sec. 4.1)	**MS-RHE scheme** (Sec. 5.1)	**LWE-based HE scheme** (Kim et al. (2020))
80	0.14, 0.14 / 0.56	0.25, 0.25 / 3821.70	0.07, 0.07 / 0.14	0.11, 0.11 / 11306.47
112	0.17, 0.17 / 0.66	0.28, 0.28 / 4682.38	0.09, 0.09 / 0.17	0.15, 0.15 / 22201.74
128	0.18, 0.18 / 0.71	0.29, 0.29 / 5217.47	0.09, 0.09 / 0.18	0.18, 0.18 / 31873.71
192	0.35, 0.35 / 1.39	0.34, 0.34 / 7131.47	0.18, 0.18 / 0.35	0.27, 0.27 / 71818.94
256	0.64, 0.64 / 2.53	0.39, 0.39 / 9460.29	0.32, 0.32 / 0.64	0.37, 0.37 / 139975.42

6.2.2 Network load and cloud storage

The network capacity needed to send ciphertexts over the network and the used cloud storage of the encrypted controller parameters are shown in Table 6.3, which are obtained following the analysis given in Section 6.1.

As can be seen in Table 6.3, under all security level κ, the network capacity needed by the MS-RHE scheme is less than compared to the other encryption schemes. By comparing the used cloud storage of the encrypted controller parameters, the MS-RHE scheme has the lowest demand for cloud storage, while the LWE-based HE scheme has the highest demand for cloud storage.

Table 6.3 shows that the amount of data going through the communications channels for all encryption schemes can be handled by standard communication networks. For instance, Ethernet can have a bit-rate ranging from 1 Gbit/s to 10 Gbit/s. It should be no problem to store the controller parameters encrypted by the RHE scheme and the MS-RHE on a cloud provided by a third party, as the used cloud storage under all security level κ is less than 2.6 MB. The demand for cloud storage in the PQS-RHE scheme and the LWE-based HE scheme can be very high, posing challenges for a cloud-based control system that operates with multiple controllers in the cloud.

6.3 Discussion

In this chapter, the cloud-based control system encrypted by the encryption schemes proposed in this doctoral study, namely, the RHE scheme, the PQS-RHE scheme and the MS-RHE scheme are analyzed theoretically and practically. Moreover, the LWE based HE scheme given by Kim et al. (2020) is considered in the practical analysis.

In the theoretical analysis, a comparison is made between the proposed encryption schemes by taking into account the network capacity required to transmit the ciphertexts over the communication channels and the cloud storage needed by the encrypted controller parameters. In the practical analysis, the cloud-based control system is encrypted by the proposed encryption schemes and the LWE-based HE scheme given by Kim et al. (2020) considering the well-established quadruple-tank system.

The theoretical and practical analysis give us some valuable insights into the practical applicability of the proposed encryption schemes, which can be summarized as follows.

Execution time. The mean time for executing a controller cycle (i.e. the sum of encryption, decryption and evaluation) with the encryption schemes proposed in this doctoral study is much less than with the LWE-based HE scheme. If the prime numbers increase, the mean executing time in the MS-RHE scheme for the encryption rises notably, which is due to the integration of the CRT into the encryption. Hence, the mean execution time in the RHE scheme and the PQS-RHE scheme for the encryption and the decryption, for large security levels, is less than compared to the MS-RHE scheme. The PQS-RHE scheme transforms the parameter matrix of the controller in plaintext into a high-dimensional matrix in ciphertext, leading to the following results. Using the RHE scheme and the MS-RHE scheme for evaluating the control law in ciphertexts is faster than using the PQS-RHE scheme, since the number of operations done in the cloud by the MS-RHE scheme and the RHE scheme is much smaller than by the PQS-RHE scheme.

Network load and cloud storage. As the MS-RHE scheme makes use of the CRT to encrypt multiple plaintexts into a single ciphertext, the MS-RHE scheme requires the least network capacity to transmit the ciphertexts over the network. Moreover, the storage used in the cloud by the MS-RHE scheme is much smaller than that used by the RHE scheme, the PQS-RHE scheme and the LWE-based HE scheme, as the amount of ciphertexts stored in the cloud is notably smaller in the MS-RHE scheme than that in the other encryption schemes.

As the proposed encryption schemes are beneficial in different practical aspects for the cloud-based control system, the choice of an encryption scheme for a practical application depends on the security level κ and the resources (i.e. real-time computational capacity, available network capacity and cloud storage).

7 Attack Detection

In this chapter, a detection approach will be presented that reveals attacks injected into the signals encrypted by the RHE scheme given in Section 3.3. That means, the RHE scheme can be combined with the proposed detection approach to ensure the integrity of the signals obtained after the decryption.

An important aspect in cyber security is the detection of cyber attacks. In the context of a cloud-based control system, it must be ensured that the control input signals obtained after the decryption are completely trustable. A detection approach for a cloud-based control system encrypted by the ElGamal cryptosystem (Elgamal, 1985) is introduced by Baba et al. (2018). By exploiting the sensitivity of the ElGamal cryptosystem to additive attacks, the attack injected into the ciphertexts strongly influences the control input signals obtained after the decryption. Then the attack is detected by comparing the control input with a threshold. In Cheon et al. (2018), the linearly homomorphic authenticated encryption (LinHAE) scheme is proposed. By making use of a hash function in the encryption and the decryption, a residual signal can be formulated. In case that the ciphertexts has been corrupted, the residual signal deviates from zero. An anomaly detector for faulty sensors and false data injection attacks is given by Alexandru et al. (2022), where the calculations for the linear quadratic Gaussian regulator and the anomaly detection are done encrypted in the cloud. For anomaly detection, a residual signal is defined by the difference between the measured output signals and the expected output signals and integrated into a change detection statistic known as the non-parametric cumulative sum statistic. An alarm is triggered when the statistic value exceeds a predefined threshold.

The question now is how to detect an attack imposed on the cloud-based control system encrypted by the RHE scheme, if the ciphertexts transmitted over the network are manipulated. Especially, if the attack is outside of the resilience range, how to generate an alarm to alert plant operators.

The chapter is organized as follows. In Section 7.1, the basic idea of the detection approach is proposed. Moreover, the detection process for both attacks inside and outside the resilience range is provided. In Section 7.2, an analysis of the behaviour of the warning signal and the alarm signal is given. The influence of an attack outside of the resilience range is analyzed in Section 7.3. Finally, an example of the well-established quadruple-tank process is given in Section 7.4 to illustrate the proposed detection approach.

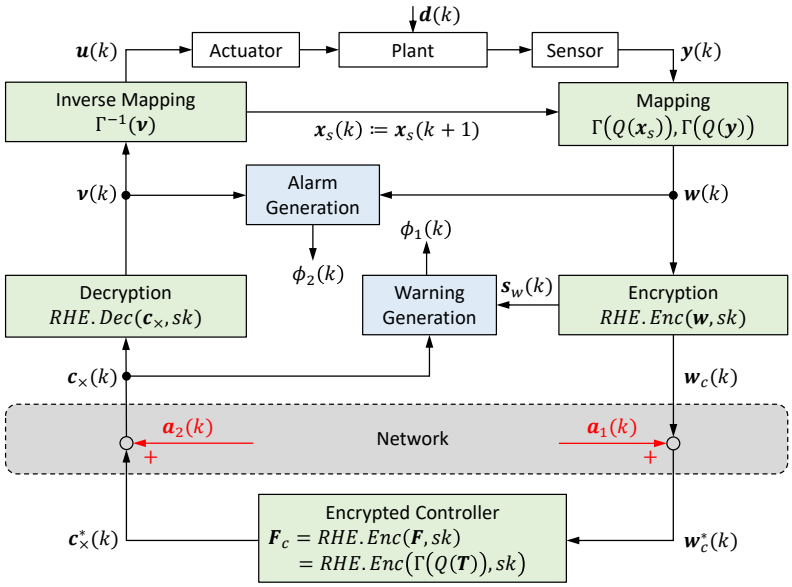

Figure 7.1: Encrypted cloud-based control system with the RHE scheme and equipped with the detection approach

7.1 Detection process

A detection approach will be presented that reveals attacks injected into the signals encrypted by the RHE scheme. By exploiting the symmetric property of the inner product, two residual signals can be formulated. In case that the attack is inside of the resilience range, the first residual signal deviates from zero and a warning is generated. As soon as the attack is outside of the resilience range, the second residual signal deviates from zero and an alarm is triggered. That means, we go one step further to prevent attacks that want to break the resilience of the RHE scheme by using the proposed detection approach. The basic idea of the detection process is schematically illustrated in Fig. 7.1. The attack detection system is composed of a warning generator and an alarm generator.

The *warning signal* $\phi_1(k)$ aims to detect the existence of an attack injected into the ciphertexts sent over the network. It is generated based on the noise $\boldsymbol{s}_w(k)$ used in the encryption (3.35) and the received ciphertext $\boldsymbol{c}_\times(k)$ by

$$\hat{\boldsymbol{s}}(k) = (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta \tag{7.1}$$

$$e_1(k) = \langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \hat{\boldsymbol{s}}(k) \rangle \tag{7.2}$$

where $e_1(k)$ is the residual signal, $\langle \cdot \rangle$ is the inner product and $\boldsymbol{s}_{pre} \in \mathbb{N}^{\alpha \times 1}$ is a predefined vector that has to be kept secret whose entries are $s_{pre,i} \neq 0$, $i \in \{1, 2, \cdots, \alpha\}$. A warning is triggered based on the following decision logic

$$\begin{cases} e_1(k) = 0 \Rightarrow \text{ attack-free, } \phi_1(k) = 0 \\ e_1(k) \neq 0 \Rightarrow \text{ under attack, } \phi_1(k) = 1, \end{cases} \tag{7.3}$$

where $\phi_1(k)$ is the warning signal.

The *alarm signal* $\phi_2(k)$ aims to reveal attacks that break the resilience range. It is generated based on the vector $\boldsymbol{w}(k) = [\boldsymbol{x}_s^T(k)\, \boldsymbol{y}^T(k)]^T$ and the vector $\boldsymbol{\nu}(k)$ got after the decryption in (3.36) by

$$e_2(k) = \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\nu}(k) \rangle \tag{7.4}$$

An alarm is triggered based on the following decision logic

$$\begin{cases} e_2(k) = 0 \Rightarrow \nu(k) \text{ is not influenced, } \phi_2(k) = 0 \\ e_2(k) \neq 0 \Rightarrow \nu(k) \text{ is influenced, } \phi_2(k) = 1, \end{cases} \tag{7.5}$$

where $\phi_2(k)$ is the alarm signal.

7.2 Analysis of warning signal and alarm signal

Depending on the attacks $\boldsymbol{a}_1(k)$ and $\boldsymbol{a}_2(k)$, there are three different cases.

Case I: No attacks in the cloud-based control system, i.e. $\boldsymbol{a}_1(k) = \boldsymbol{0}$, $\boldsymbol{a}_2(k) = \boldsymbol{0}$. In this case, $\boldsymbol{w}_c^*(k) = \boldsymbol{w}_c(k)$ and $\boldsymbol{c}_\times(k) = \boldsymbol{c}_\times^*(k)$. If $\|\boldsymbol{S}_f \boldsymbol{s}_w(k)\|_\infty < \theta$ and (3.39) holds, substituting (3.37) into (7.1) gives

$$\begin{aligned} \hat{\boldsymbol{s}}(k) &= (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta \\ &= \big((\boldsymbol{F}_c \boldsymbol{w}_c(k) \bmod z_0) \bmod p\big) \bmod \theta \\ &= \big((\boldsymbol{S}_f \boldsymbol{s}_w(k) + \theta(\boldsymbol{S}_f \boldsymbol{w}(k) + \boldsymbol{F}\boldsymbol{s}_w(k)) + \theta^2 \boldsymbol{F}\boldsymbol{w}(k) + p(\boldsymbol{S}_f \boldsymbol{r}_w(k) + \boldsymbol{R}_f \boldsymbol{s}_w(k) \\ &\quad + \theta(\boldsymbol{F}\boldsymbol{r}_w(k) + \boldsymbol{R}_f \boldsymbol{w}(k)) + p\boldsymbol{R}_f \boldsymbol{r}_w(k)) \bmod z_0) \bmod p\big) \bmod \theta \\ &= \boldsymbol{S}_f \boldsymbol{s}_w(k) \end{aligned} \tag{7.6}$$

As a result,

$$\begin{aligned} e_1(k) &= \langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \hat{\boldsymbol{s}}(k) \rangle \\ &= \langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{S}_f \boldsymbol{s}_w(k) \rangle \end{aligned} \tag{7.7}$$

Due to the symmetric property of the inner product, it holds

$$\langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle = \langle \boldsymbol{s}_{pre}, \boldsymbol{S}_f \boldsymbol{s}_w(k) \rangle \tag{7.8}$$

Therefore,

$$e_1(k) = 0 \text{ and } \phi_1(k) = 0. \tag{7.9}$$

According to (3.36), the vector $\boldsymbol{\nu}(k)$ is given by

$$\begin{aligned} \boldsymbol{\nu}(k) &= RHE.Dec(\boldsymbol{c}_\times(k), sk) \\ &= \frac{\boldsymbol{c}_\times(k) \bmod p - (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta^2}{\theta^2} \\ &= \boldsymbol{F}\boldsymbol{w}(k) \end{aligned} \tag{7.10}$$

From (7.4) and the decision logic (7.5), we get

$$\begin{aligned} e_2(k) &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\nu}(k) \rangle = 0 \\ &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T s_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{F}\boldsymbol{w}(k) \rangle = 0 \\ \phi_2(k) &= 0 \end{aligned} \tag{7.11}$$

Case II: The attacks $\boldsymbol{a}_1(k)$, $\boldsymbol{a}_2(k)$ are inside of the resilience range, i.e. $\boldsymbol{G}\boldsymbol{a}_1(k) + \boldsymbol{h}(k) + \boldsymbol{a}_2(k) \in [\boldsymbol{\delta}p,\, \boldsymbol{\delta}p + \theta^2\mathbf{1})$. As shown in Section 3.4, in this case, the influence of the attacks $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ is cancelled out of the vector $\boldsymbol{\nu}(k)$ obtained after decryption, i.e. $\boldsymbol{\nu}(k) = \boldsymbol{F}\boldsymbol{w}(k)$. Let

$$\boldsymbol{G}\boldsymbol{a}_1(k) + \boldsymbol{h}(k) + \boldsymbol{a}_2(k) = \boldsymbol{\delta}p + \boldsymbol{\Delta} \tag{7.12}$$

and $\boldsymbol{\Delta} \in \mathbb{N}^{\alpha \times 1}$ whose entries are $\Delta_i \in \{0, 1, \cdots, \theta^2 - 1\}$. Substituting (3.58) into (7.1) yields

$$\hat{\boldsymbol{s}}(k) = (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta = (\boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}(k)) \bmod \theta = \boldsymbol{\Delta}_\theta(k) \tag{7.13}$$

where $\boldsymbol{\Delta}_\theta(k) \in \mathbb{N}^{\alpha \times 1}$ whose entries are $\Delta_{\theta i}(k) \in \{0, 1, \cdots, \theta - 1\}$. Taking into account (7.2), we get

$$e_1(k) = \langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\Delta}_\theta(k) \rangle \tag{7.14}$$

Therefore,

$$e_1(k) \neq 0 \text{ and } \phi_1 = 1, \tag{7.15}$$

as long as $\boldsymbol{\Delta}_\theta(k) \neq \boldsymbol{S}_f \boldsymbol{s}_w(k) + \boldsymbol{\Delta}_a(k)$, where $\langle \boldsymbol{s}_{pre}, \boldsymbol{\Delta}_a(k) \rangle = 0$. Recall that the entries of the vector $\boldsymbol{s}_w(k)$ in (7.14) are randomly chosen integers and change with time, its impossible for the attacker to reach $\boldsymbol{\Delta}_\theta(k) = \boldsymbol{S}_f \boldsymbol{s}_w(k) + \boldsymbol{\Delta}_a(k)$ at each time step. Since $\boldsymbol{\nu}(k) = \boldsymbol{F}\boldsymbol{w}(k)$, there is

$$\begin{aligned} e_2(k) &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\nu}(k) \rangle \\ &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{F}\boldsymbol{w}(k) \rangle = 0 \\ \phi_2(k) &= 0 \end{aligned} \tag{7.16}$$

Case III: The attacks $\boldsymbol{a}_1(k)$, $\boldsymbol{a}_2(k)$ are outside of the resilience range, i.e. $\boldsymbol{G}\boldsymbol{a}_1(k) + \boldsymbol{h}(k) + \boldsymbol{a}_2(k) \notin [\boldsymbol{\delta}p,\, \boldsymbol{\delta}p + \theta^2\mathbf{1})$. Let

$$\boldsymbol{G}\boldsymbol{a}_1(k) + \boldsymbol{h}(k) + \boldsymbol{a}_2(k) = \boldsymbol{\delta}p + \boldsymbol{l}(k)\theta^2 + \boldsymbol{\Delta} \tag{7.17}$$

where $\boldsymbol{l}(k) \in \mathbb{N}^{\alpha \times 1}$ whose entries are $l_i(k) \in [-\nu_i(k),\, \lfloor \frac{p}{\theta^2} \rfloor - \nu_i(k)]$ and $\nu_i(k)$ are the entries of the vector $\boldsymbol{\nu}(k) = \boldsymbol{F}\boldsymbol{w}(k)$. Because of the attacks $\boldsymbol{a}_1(k)$ and $\boldsymbol{a}_2(k)$, it holds

$$\begin{aligned} \boldsymbol{c}_\times(k) \bmod p &= (\underbrace{\boldsymbol{G}\boldsymbol{a}_1(k) + \boldsymbol{h}(k) + \boldsymbol{a}_2(k)}_{\notin [\boldsymbol{\delta}p,\, \boldsymbol{\delta}p + \theta^2\mathbf{1})} + \theta^2 \boldsymbol{F}\boldsymbol{w}(k)) \bmod p \\ &= (\boldsymbol{\delta}p + \boldsymbol{l}(k)\theta^2 + \boldsymbol{\Delta} + \theta^2 \boldsymbol{F}\boldsymbol{w}(k)) \bmod p \\ &= \boldsymbol{\Delta} + \theta^2 \big(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k)\big), \end{aligned} \tag{7.18}$$

where $\|\boldsymbol{\Delta} + \theta^2(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k))\|_\infty < p$. By taking into account (7.1), it yields

$$\begin{aligned} \hat{\boldsymbol{s}}(k) &= (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta \\ &= (\boldsymbol{\Delta} + \theta^2(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k))) \bmod \theta = \boldsymbol{\Delta}_{\boldsymbol{l}}(k) \\ e_1(k) &= \langle \boldsymbol{s}_w(k), \boldsymbol{S}_f^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\Delta}_l(k) \rangle \end{aligned} \tag{7.19}$$

where $\boldsymbol{\Delta}_l(k) \in \mathbb{N}^{\alpha \times 1}$ whose entries are $\Delta_{li}(k) \in \{0, 1, \cdots, \theta - 1\}$. If $\boldsymbol{\Delta}_l(k) \neq \boldsymbol{S}_f \boldsymbol{s}_w(k) + \boldsymbol{\Delta}_a(k)$, where $\langle \boldsymbol{s}_{pre}, \boldsymbol{\Delta}_a(k) \rangle = 0$, then

$$e_1(k) \neq 0 \text{ and } \phi_1(k) = 1. \tag{7.20}$$

Due to (7.18), the decryption of $\boldsymbol{c}_\times(k)$ by (3.36) gives

$$\begin{aligned} \boldsymbol{\nu}(k) &= RHE.Dec(\boldsymbol{c}_\times(k), sk) \\ &= \frac{\boldsymbol{c}_\times(k) \bmod p - (\boldsymbol{c}_\times(k) \bmod p) \bmod \theta^2}{\theta^2} \\ &= \frac{\boldsymbol{\Delta} + \theta^2(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k)) - (\boldsymbol{\Delta} + \theta^2(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k))) \bmod \theta^2}{\theta^2} \\ &= \frac{\boldsymbol{\Delta} + \theta^2(\boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k)) - \boldsymbol{\Delta}}{\theta^2} = \boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k) \end{aligned} \tag{7.21}$$

From (7.4) and (7.21), it yields

$$\begin{aligned} e_2(k) &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{\nu}(k) \rangle \\ &= \langle \boldsymbol{w}(k), \boldsymbol{F}^T \boldsymbol{s}_{pre} \rangle - \langle \boldsymbol{s}_{pre}, \boldsymbol{F}\boldsymbol{w}(k) + \boldsymbol{l}(k) \rangle \\ &= \langle \boldsymbol{s}_{pre}, \boldsymbol{l}(k) \rangle \end{aligned} \tag{7.22}$$

Thus, if $\langle \boldsymbol{s}_{pre}, \boldsymbol{l}(k) \rangle \neq 0$, then

$$e_2(k) \neq 0 \text{ and } \phi_2(k) = 1. \tag{7.23}$$

7.3 Influence of attacks outside of resilience range

As can be seen from (7.21), if the attacks $\boldsymbol{a}_1(k)$, $\boldsymbol{a}_2(k)$ break the resilience range, then the vector $\boldsymbol{\nu}(k)$ obtained after the decryption is not equal to the true value of the vector $\boldsymbol{F}\boldsymbol{w}(k)$ any more. Now we check how big $\boldsymbol{l}(k)$ (i.e. the difference between $\boldsymbol{\nu}(k)$ and the true value of $\boldsymbol{F}\boldsymbol{w}(k)$) is.

If $\boldsymbol{\delta}p + \theta^2\boldsymbol{1} - \boldsymbol{h} \leq \boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{a}_2 < \boldsymbol{\delta}p + 2\theta^2\boldsymbol{1} - \boldsymbol{h}$, then $\boldsymbol{l} = \boldsymbol{1}$. If $\boldsymbol{\delta}p - \theta^2\boldsymbol{1} - \boldsymbol{h} \leq \boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{a}_2 < \boldsymbol{\delta}p - \boldsymbol{h}$, then $\boldsymbol{l} = -\boldsymbol{1}$. That means, the entries of the vector $\boldsymbol{\nu}$ obtained by decryption differ from the true values by 1.

According to (7.17), there is

$$\boldsymbol{l} = \frac{\boldsymbol{G}\boldsymbol{a}_1 + \boldsymbol{a}_2 + \boldsymbol{h} - \boldsymbol{\Delta} - \boldsymbol{\delta}p}{\theta^2} \tag{7.24}$$

Recall that θ is the security parameter prespecified during the key generation and is usually a large number, $\mathbf{0} \leq \boldsymbol{\Delta} \leq \theta^2\mathbf{1}-\mathbf{1}$ and $\|\boldsymbol{h}\|_\infty = \|\boldsymbol{S}_f\boldsymbol{s}_w+\theta(\boldsymbol{S}_f\boldsymbol{w}+\boldsymbol{F}\boldsymbol{s}_w)\|_\infty < \theta^2$. It holds

$$-(\theta^2\mathbf{1}-\mathbf{1}) \leq \boldsymbol{h}-\boldsymbol{\Delta} \leq \theta^2\mathbf{1}-\mathbf{1} \;\Leftrightarrow\; -\mathbf{1} < \frac{\boldsymbol{h}-\boldsymbol{\Delta}}{\theta^2} < \mathbf{1} \tag{7.25}$$

If $\boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2 \geq \boldsymbol{\delta}p+2\theta^2\mathbf{1}-\boldsymbol{h}$, then $\boldsymbol{l}$ is a vector with positive integer entries that always satisfies

$$\boldsymbol{l} \leq \frac{\boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2-\boldsymbol{\delta}p}{\theta^2}+1 \ll \boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2 \tag{7.26}$$

If $\boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2 < \boldsymbol{\delta}p-\mathbf{1}\theta^2-\boldsymbol{h}$, then $\boldsymbol{l}$ is a vector with negative integer entries and satisfy

$$\boldsymbol{l} \geq \frac{\boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2-\boldsymbol{\delta}p}{\theta^2}-\mathbf{1} \tag{7.27}$$

In these two scenarios, the difference between the value $\boldsymbol{\nu}$ got after the decryption and the true value of $\boldsymbol{F}\boldsymbol{w}$ is $\boldsymbol{l} = \boldsymbol{\nu}-\boldsymbol{F}\boldsymbol{w}$. Because θ is a large number, $|\boldsymbol{l}| \ll |\boldsymbol{G}\boldsymbol{a}_1+\boldsymbol{a}_2|$. That means, *the influence of attacks outside of the resilience range will be significantly reduced.*

In summary, as soon as the attacks $\boldsymbol{a}_1(k)$ and $\boldsymbol{a}_2(k)$ are injected into the encrypted signals, the residual signal $e_1(k)$ got by (7.2) will deviate from zero and the warning signal $\phi_1(k)$ will be triggered to signify the existence of the attacks. If the attacks $\boldsymbol{a}_1(k)$, $\boldsymbol{a}_2(k)$ are outside of the resilience range (i.e. $\boldsymbol{G}\boldsymbol{a}_1(k)+\boldsymbol{h}(k)+\boldsymbol{a}_2(k) \notin [\boldsymbol{\delta}p,\, \boldsymbol{\delta}p+\theta^2\mathbf{1})$), the residual signal $e_2(k)$ obtained by (7.4) will deviate from zero and triggers the alarm signal $\phi_2(k)$. Note that, because $|\boldsymbol{l}(k)| \ll |\boldsymbol{G}\boldsymbol{a}_1(k)+\boldsymbol{a}_2(k)|$, the difference between $\boldsymbol{\nu}(k)$ obtained after the decryption and the true value of $\boldsymbol{F}\boldsymbol{w}(k)$ caused by the attacks $\boldsymbol{a}_1(k)$ and $\boldsymbol{a}_2(k)$ is significantly reduced. As a result, the control system can still keep much of the control performance.

7.4 Simulation example

In this section, the cloud-based control system encrypted by the RHE scheme and equipped with the detection approach will be illustrated. In the simulation, the quadruple-tank system and the dynamic output feedback controller introduced in Section 2.3 are used. Moreover, the parameters λ_1, λ_2 in the mapping function and the parameters $\rho, \theta, \psi, \gamma$ in the RHE scheme are chosen to be the same as in Section 3.7.2 and thus are just briefly summarized here.

The stability of the closed-loop system can be guaranteed by selecting the range λ_1 and the resolution λ_2 in the mapping function as $\lambda_1 = 4$ and $\lambda_2 = 16$, respectively. Thus, the bound of the plaintexts is $M = 2^{21}$ and $\mu = \beta 2^{2(\lambda_1+\lambda_2)+1}+1 = 4\times 2^{41}+1$. In order to prevent the main families of known attacks and achieve the security level $\kappa = 80$, the bit-size of the noises is selected as $\rho = 2\kappa = 160$, the integer θ is from the interval $(2^{207}, 2^{208})$, the bit-size ψ of the prime number p is $\psi = 505$ and the bit-size γ of the ciphertext space is selected as $\gamma = 276160$.

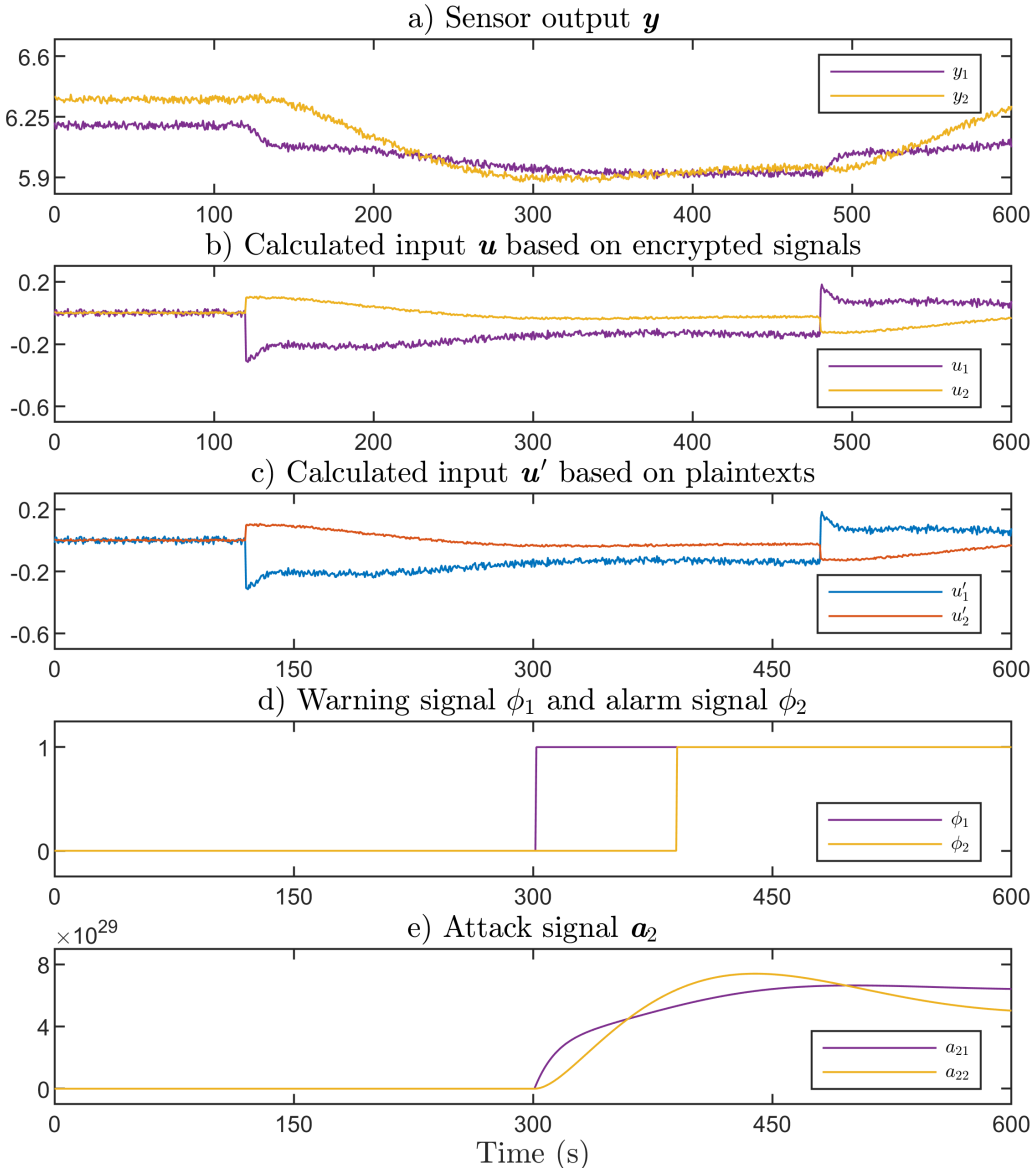

Figure 7.2: Encrypted cloud-based control system with the RHE scheme and equipped with the detection approach

The controller parameters (2.7) are mapped by (3.11), (3.12) and then encrypted by (3.34). Due to the bit-size $\gamma = 276160$ of the ciphertext space, the encrypted controller parameters are large integers and thus omitted here.

The entries of the vector $\boldsymbol{s}_{pre}$ of the residual signals (7.2), (7.4) are randomly chosen from the interval $\{0, 1, \cdots, 2^{\rho}\}$.

During the simulation, an attack is imposed on the encrypted control input signals (i.e. $\boldsymbol{a}_2(k) = [0\ 0\ a_{21}(k)\ a_{22}(k)]^T$) from $k = 300s$ to $k = 600s$ (see Fig. 7.2e), while there is no attack on the sensor output channels (i.e. $\boldsymbol{a}_1(k) = \boldsymbol{0}$). The adversary is not able to estimate the resilience range of the RHE scheme, because only ciphertexts are sent over the network. In order to show the effect of attacks inside of the resilience range and attacks outside of the resilience range, the attack signal $\boldsymbol{a}_2(k)$ shown in

Fig. 7.2e are imposed on the ciphertexts.

In the encrypted cloud-based control system, the sensor output signal $\boldsymbol{y}(k)$ (see Fig. 7.2a) and the state vector $\boldsymbol{x}_s(k)$ of the controller are stacked together, mapped into the integer vector $\boldsymbol{w}(k)$ and then encrypted by the RHE scheme which leads to the ciphertext $\boldsymbol{w}_c(k)$. Due to the bit-size $\gamma = 276160$ of the ciphertext space, the ciphertext $\boldsymbol{w}_c(k)$ and the ciphertext $\boldsymbol{c}_\times(k)$ got after the evaluation process of the controller are omitted here. Fig. 7.2b shows the control input signal $\boldsymbol{u}(k)$ received by the actuators got after the decryption process. For comparison, the control input signal $\boldsymbol{u}'(k)$ generated by the classical feedback controller in the form of (2.2) and (2.7) is shown in Fig. 7.2c which is got based on the unencrypted signals (i.e. the plaintexts of controller parameters and outputs). Before the attack happens at $k = 300s$, no difference between $\boldsymbol{u}'(k)$ and $\boldsymbol{u}(k)$ can be observed. Both the warning signal and the alarm signal keep to be 0, i.e. $\phi_1(k) = 0$, $\phi_2(k) = 0$ (see Fig. 7.2d).

Now let us check the behaviour of the system after the attack happens at $k = 300s$. During the time interval from $k = 300s$ to $k = 380s$, the attack signal $\boldsymbol{a}_2(k)$ is inside of the resilience range, because $\boldsymbol{a}_2(k) < \theta^2\mathbf{1} - \boldsymbol{h}(k)$, where $\boldsymbol{h}(k) = \boldsymbol{S}_f\boldsymbol{s}_w(k) + \theta(\boldsymbol{S}_f\boldsymbol{w}(k) + \boldsymbol{F}\boldsymbol{s}_w(k))$. Due to the neutralization effect of the RHE scheme, the attack signal has no influence of the control input signal $\boldsymbol{u}(k)$ got after the decryption (see Fig. 7.2b). That means, the true values of the control input signal $\boldsymbol{u}(k)$ are available to the actuators. Furthermore, the warning signal $\phi_1(k)$ (see Fig. 7.2d) changes from 0 to 1 at $k = 300$, which signifies the presence of the attack signal $\boldsymbol{a}_2(k)$. Beginning from $k = 380s$, the attack signal $\boldsymbol{a}_2(k) \geq \theta^2\mathbf{1} - \boldsymbol{h}(k)$ is outside of the resilience range and influences the control input signal $\boldsymbol{u}(k)$ obtained by decryption. The alarm signal $\phi_2(k)$ (see Fig. 7.2d) changes from 0 to 1 at $k = 380s$ and reveals that the resilience range is broken by the attack signal $\boldsymbol{a}_2(k)$. Fortunately, the influence of the attack signal $\boldsymbol{a}_2(k)$ on the control input signal $\boldsymbol{u}(k)$ is strongly reduced by the factor $\frac{1}{2^{2\lambda_2}\,\theta^2} > \frac{1}{2^{32}\times 2^{414}}$. Hence, the influence of the attack signal $\boldsymbol{a}_2(k)$ is almost not visible in Fig. 7.2b.

In summary, the detection approach gives a twofold protection to cloud-based control systems encrypted by the RHE scheme. A warning signal is triggered as soon as an additive attack is imposed on the ciphertexts transmitted over the network, while an alarm signal is triggered when the attack is outside of the resilience range. As the plant can still operate when an attack takes place, the availability of the signals in a cloud-based control system is increased.

7.5 Discussion

Though the RHE scheme is able to neutralize the effect of additive attacks injected into the encrypted cloud-based control system, the resilience range has still some limits. Therefore, a detection approach is proposed to protect the cloud-based control systems encrypted with the RHE scheme in two levels. Two residual signals are generated by exploiting the symmetric property of the inner product. If the additive

attack injected into the signals sent over the network is inside of the resilience range, the control input signals obtained after the decryption are completely trustable and only a warning signal will be delivered. As soon as the attack breaks the resilience range and influences the control input signals obtained after the decryption, an alarm is triggered and countermeasures should be taken. A cloud-based control system encrypted by the RHE scheme and equipped with the proposed detection approach can not only make the control system to be resilient to additive attacks in a large resilience range, but also protect the control system from attacks that break the resilience range by giving alarms to alert plant operators.

8 Conclusion

8.1 Summary

A cloud-based control system is an innovative approach that takes advantage of cloud computing technology. This technology offers computing services and resources over the internet, such as data outsourcing and flexible and scalable control solutions. Moreover, a cloud-based control system can be more cost-effective and energy-efficient compared to establishing and maintaining dedicated control systems. However, storing and processing sensitive data in a cloud platform making it vulnerable for malicious adversaries. If an adversary bypasses the security measurements, the adversary can obtain confidential data stored in the cloud platform. Moreover, an adversary could attempt to get access to the communication channels of the cloud to tamper the data of the control system so that the data are changed in an unauthorized manner or the data are not accessible when needed. Therefore, the cloud resources need to be protected against malicious adversaries with respect to confidentiality, integrity and availability. In this thesis, approaches are provided that achieve multiple security objectives such as confidentiality, integrity and availability so that a wide range of cyber attacks can be prevented.

While the security objective of ensuring the confidentiality of the signals in cloud-based control systems can be achieved through the use of homomorphic encryption (HE) schemes, the integrity and availability of the signals may still be disrupted. An adversary can still manipulate the ciphertexts transmitted over the network in a way that the signals needed by the controller and the actuators can no longer be trusted or may become unavailable when needed. Going one step further, it is shown in Chapter 3 that an adversary can still implement a covert attack on an encrypted cloud-based control system in a similar ways as in an unencrypted cloud-based control system. That means, the adversary can manipulate the plant behaviour in the encrypted cloud-based control system without being detected by a conventional monitoring system. To cope with this vulnerability, the resilient homomorphic encryption (RHE) scheme proposed in Chapter 3 is developed. Compared with the existing HE schemes, the RHE scheme can cancel the influence of an additive attack out of the control system so that the controller can get the true sensor information and the actuators can get the true control input signals even in case of an attack. In order to ensure that an adversary can not gain any useful information from the ciphertexts generated by the RHE scheme, it is proven that the RHE scheme satisfies indistinguishability under chosen plaintext attack (IND-CPA). As the transformation between real values and quantized values causes the so-called quantization error and may affect the plant

behaviour, a condition for the stability of the closed-loop system is derived.

In the post-quantum era, the quantum computer poses a serious threat to the RHE scheme introduced in Chapter 3, because the secret key could be efficiently retrieved from the divisor in the modulo operations used in the encryption of the RHE scheme. To achieve post-quantum security and preserve the ability of resilience, the RHE scheme in Chapter 3 is further developed in Chapter 4 to obtain the post-quantum secure resilient homomorphic encryption (PQS-RHE) scheme. The key changes in the RHE schemes are twofold. At first, the divisor in the modulo operations are chosen suitably so that an adversary can not gain access to the secret key even with a quantum computer. Secondly, to keep the homomorphism, a decomposition technique is integrated into the process of evaluating the control law in ciphertexts. An analysis shows that the PQS-RHE scheme keep the ability of resilience and attacks imposed on the ciphertexts can still be neutralized.

As the size of a ciphertext generated by encryption schemes is much larger than the corresponding plaintext, approaches to reduce the network load in encrypted cloud-based control systems are required. To reduce the requirement on network capacity and keep the ability of resilience, the RHE scheme proposed in Chapter 3 is further developed in Chapter 5 to obtain the multi-slot resilient homomorphic encryption (MS-RHE) scheme. By making use of the Chinese remainder theorem (CRT), multiple plaintexts can be packed together into a single ciphertexts before they are sent over the communication channels. Moreover, the size of the ciphertext in the MS-RHE scheme is the same as in the RHE scheme. Thus, the network load is reduced. It is shown that, even through the CRT is employed for the MS-RHE scheme, the MS-RHE scheme is still resilient to additive attacks.

In order to provide more insights into the practical applicability of encrypted cloud-based control systems, the encryption schemes proposed in this doctoral study are analyzed theoretically and practically and compared to each other in Chapter 6. Moreover, a learning with errors (LWE)-based HE scheme is considered in the practical analysis. In the theoretical analysis, the proposed encryption schemes are compared in terms of the network capacity required to transmit ciphertexts over the network and the usage of cloud storage. In the practical analysis, the mean execution time of the encrypted controller, the requirements on network capacity and the used cloud storage of the encryption schemes under different security levels are investigated. Due to different encryption mechanism, the encryption schemes are beneficial in different practical aspects under different security level. For instance, the RHE scheme and PQS-RHE scheme need less execution time for encryption and decryption for large security level, while the MS-RHE scheme leads to a smaller amount of data sent over the network and a smaller storage space for the encrypted controller parameters.

Although the RHE scheme in Chapter 3 is able to neutralize the effect of additive attacks imposed on the ciphertexts transmitted over the network, the resilience range has still some limits. Therefore, a detection approach is proposed in Chapter 7 to give a twofold protection to cloud-based control systems encrypted by the RHE scheme. Two residual signals are generated by exploiting the symmetric property of the inner product. A warning signal is triggered as soon as an additive attack is injected into

the ciphertexts transmitted over the network, while an alarm signal is triggered when the attack is outside of the resilience range. Therefore, the RHE scheme can be combined with the proposed detection approach to ensure the integrity of the signals obtained after decryption in case of additive attacks.

The proposed approaches offer a significant improvement in the ability to fully outsource control laws to a cloud hosted by a third party while ensuring the confidentiality, integrity and availability of data.

8.2 Outlook

As encrypted control is a young field of research, there are several interesting directions for future research. In this thesis, the structure under consideration consists of a linear system. Hence, it would be of great interest how the proposed approaches can be adapted to encrypt more complex control laws, such as nonlinear control laws. As techniques for ensuring safety in control are often nonlinear, the proposed encryption schemes could achieve both safety and security in cloud-based control systems. Another direction of future research is to investigate how a detection approach as in Chapter 7 can be integrated into the PQS-RHE scheme proposed in Chapter 4. A cloud-based control system equipped with this approach could not only ensure the integrity of the signals transmitted over the network, but also protect it from adversaries that want to retrieve the confidential information from the ciphertexts in the post-quantum era. Using an encryption scheme in a cloud-based control system causes additional computational burden for sensors, actuators and in the cloud. Although the MS-RHE proposed in Chapter 5 can reduce the computational burden, further reductions are required to increase the practical applicability of encryption schemes. The encrypted state of the encrypted controller are decrypted and encrypted again in every controller cycle, because the number of arithmetic operations on ciphertexts based on the proposed encryption schemes is limited. Therefore, calculating the encrypted state in the cloud for an infinite number of controller cycles without feeding it back to the plant side is an interesting research field. As the issue is caused by the recursive calculations of dynamic controllers, a possible starting point could be to reformulate the recursive process into an equivalent (or approximated) iterative process while avoiding a design for restrictive applicability.

9 Extended Summary in German - Zusammenfassung in deutscher Sprache

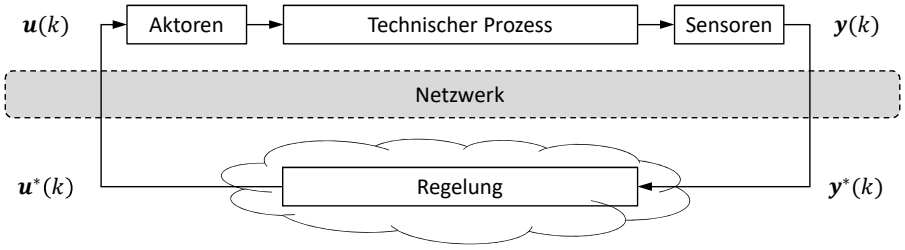

Figure 9.1: Cloudbasiertes Regelungssystem

Im Zuge der Industrie 4.0 findet die Kommunikation zwischen der Regelstrecke und dem Regler zunehmend über eine vernetzte Struktur statt, sodass Anlagen flexibler und kostengünstiger realisiert werden können. Um stets ausreichende Speicherkapazität und Rechenleistung für die steigenden Datenmengen bereitzuhalten, werden Regelungskonzepte verstärkt in Clouds betrieben. Ein solches System wird als cloudbasiertes Regelungssystem bezeichnet und ist in Abbildung 9.1 dargestellt. Jedoch können cloudbasierte Regelungssysteme Ziele von Cyberangriffen sein, die sowohl die Kommunikation als auch die Regelung angreifen. Cyberangriffe zielen mit steigender Tendenz nicht nur darauf ab Informationen zu gewinnen, sondern auch um Sensor-, Aktorsignale und Regelparameter so zu manipulieren, dass der Informationsfluss innerhalb des Regelungsprozesses gestört wird. Aus diesen Gründen gewinnen Verfahren, die dem Schutz der Vertraulichkeit und Integrität der Prozessdaten dienen sowie zur Erhöhung der Anlagenverfügbarkeit beitragen, zunehmend an Bedeutung. In dieser Arbeit werden Verfahren zur Prävention und Detektion von Cyberangriffen vorgestellt. Die präventiven Verfahren werden im Rahmen einer Analyse auf ihre Anwendbarkeit in Echtzeit untersucht.

In den letzten Jahren wurde zunehmend das Konzept von homomorphen Verschlüsselungsverfahren und deren Integration in cloudbasierte Regelungssysteme untersucht. Ein homomorphes Verschlüsselungsverfahren kann sowohl Signale verschlüsseln als auch mathematische Operationen mit verschlüsselten Signalen ausführen. Aus diesem Konzept lässt sich ein präventives Verfahren ableiten, das die Vertraulichkeit sensibler Daten wie Sensorsignale, Stellgrößen und Regelungsparameter gewährleistet. Dies geschieht durch die Umwandlung der Daten in Chiffretexte und die Durchführung von Berechnungen des Reglers mit diesen Chiffretexten. Die Struktur einer

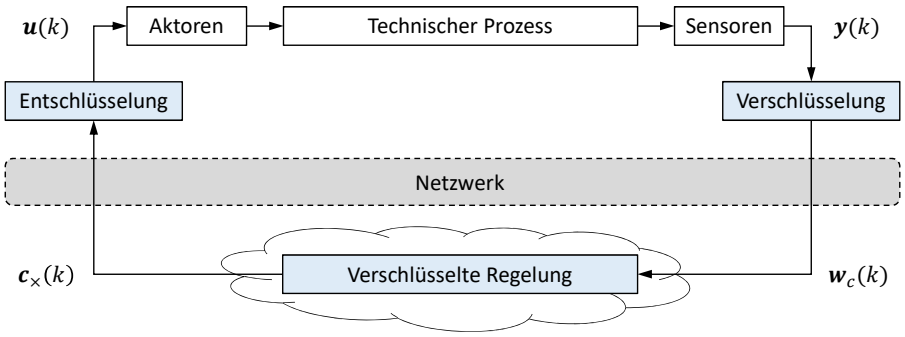

Figure 9.2: Verschlüsselung der cloudbasierten Regelungssysteme

Verschlüsselung der cloudbasierten Regelungssysteme ist in Abbildung 9.2 dargestellt. Ein homomorphes Verschlüsselungsverfahren schützt die Vertraulichkeit eines cloudbasierten Regelungssystems, verhindert jedoch nicht die Manipulation der Chiffretexte. In dieser Arbeit wird auf eine konkrete Schwachstelle in homomorphen Verschlüsselungsverfahren durch Manipulation der Chiffretexte hingewiesen. Ein Angreifer kann, auch wenn das cloudbasierte Regelungssystem mit Chiffretexten arbeitet, einen Covert-Angriff durchführen. Der Angreifer manipuliert so den technischen Prozess, ohne von einem konventionellen Verfahren der Anomalieerkennung entdeckt zu werden. Um solchen Angriffen in Zukunft vorzubeugen, wurde das Resiliente Homomorphe Verschlüsselungsverfahren (RHV) entwickelt. Im Unterschied zu den existierenden homomorphen Verschlüsselungsverfahren zeichnet sich das RHV durch seine Eigenschaft der Resilienz aus. Bei einem Angriff auf die Chiffretexte eines verschlüsselten, cloudbasierten Regelungssystem neutralisiert ein RHV den Angriff vollständig und die unverfälschte Stellgrößen erreichen den technischen Prozess. Dadurch kann der Betrieb der Anlage aufrechterhalten werden, auch wenn ein Cyberangriff auf das cloudbasierte Regelungssystem stattfindet.

Die Security Anforderungen an Verschlüsselungsverfahren sind eng mit der Rechenleistung verknüpft, die einem potenziellen Angreifer zur Verfügung steht. Mit der Entwicklung eines Quantencomputers würde einem Angreifer ausreichende Rechenleistung zur Verfügung stehen, um die Sicherheit des RHV sowie gängiger Verschlüsselungsverfahren zu gefährden. Aus diesem Grund wurde in dieser Arbeit das Post-Quantensichere Resiliente Homomorphe Verschlüsselungsverfahren (PQS-RHV) entwickelt, welches die Cybersicherheit von cloudbasierten Regelungssystemen in der Post-Quanten-Ära erhöht. Das PQS-RHV wird primär durch zwei Änderungen am RHV erlangt. Zum einen wird eine Zufallszahl auf den Divisor der Modulo-Operation addiert. Hierdurch ergibt sich eine mathematische Struktur, die einem mathematischen Problem gleicht, das selbst von Angreifern mit Zugriff auf einen Quantencomputer nicht effektiv gelöst werden kann. Zum anderen wird die homomorphe Eigenschaft im PQS-RHV sichergestellt, indem eine Zerlegungstechnik in der Berechnung der Stellgrößen mit Chiffretexten integriert wird. Das PQS-RHV bewahrt nachweislich die Eigenschaft der Resilienz und erlaubt es weiterhin Cyberangriffe zu neutralisieren.

Eine Herausforderung bei der Integration von homomorphen Verschlüsselungsver-

fahren in reale Anwendungen ist die erhöhte Netzwerklast durch Chiffretexte. In dieser Arbeit wird gezeigt, wie die Netzwerklast signifikant reduziert werden kann und die Eigenschaft der Resilienz beibehalten wird, indem der Chinesische Restsatz (CR) in die Verschlüsselungsvorschrift des RHV integriert wird. Das daraus resultierende Multi-Slot Resiliente Homomorphe Verschlüsselungsverfahren (MS-RHV) kann mehrere Signale in einem einzigen Chiffretext zusammenfassen, bevor diese über die Kommunikationskanäle gesendet werden. Zudem ist die Länge der Chiffretexte im MS-RHV identisch mit der im RHV, wodurch die Netzwerklast reduziert wird. Es wird gezeigt, dass das MS-RHV trotz der Verwendung des CR resistent gegen additive Angriffe bleibt.

Die in dieser Doktorarbeit vorgeschlagenen Verschlüsselungsverfahren werden hinsichtlich Netzwerklast, Cloud-Speicher und Rechenressourcen untersucht, um einen tieferen Einblick in die praktische Anwendbarkeit von verschlüsselten, cloudbasierten Regelungssystemen zu geben. In den Analysen wird zudem das Lernen mit Fehlern Homomorphe Verschlüsselungsverfahren (LFHV) berücksichtigt. Aufgrund unterschiedlicher Verschlüsselungsvorschriften erweisen sich die Verschlüsselungsverfahren in verschiedenen praktischen Bereichen je nach Security Level als vorteilhaft. Zum Beispiel benötigt das RHV und das PQS-RHV die geringste Ausführungszeit für Ver- und Entschlüsselung bei hohen Security Level. Die Netzwerklast und der Cloudspeicher sind bei Verwendung des MS-RHV am geringsten. Zusammenfassend liegt der Schluss nahe, dass die in dieser Doktorarbeit vorgeschlagenen Verschlüsselungsverfahren eine Integration in ein cloudbasiertes Regelungssystem rechtfertigen.

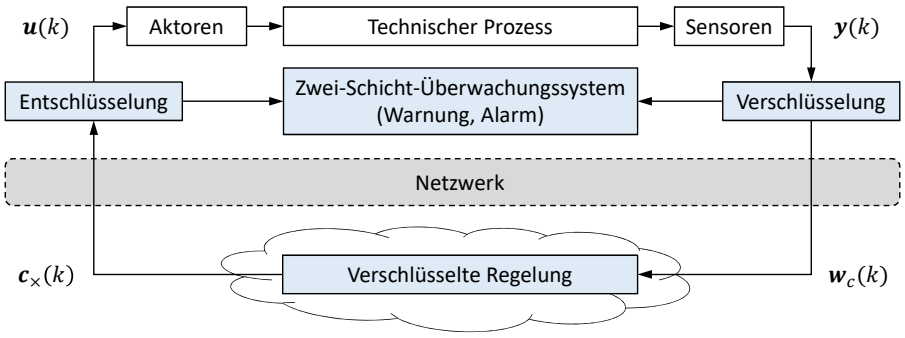

Figure 9.3: Ein mittels RHV verschlüsseltes, cloudbasiertes Regelungssystem mit integriertem Zwei-Schicht-Überwachungssystem

Ein wichtiger Aspekt der Cybersicherheit ist die Erkennung von Cyberangriffen. In dieser Arbeit wird dieser Anforderung mit Hilfe eines Zwei-Schicht-Überwachungssystems entsprochen, welches die Integrität der Stellgrößen sicherstellt und maßgeblich zur Erhöhung der Anlagenverfügbarkeit beiträgt. Das Zwei-Schicht-Überwachungssystem wird in das mittels RHV verschlüsselte Regelungssystem integriert und ist in Abbildung 9.3 dargestellt. Das Zwei-Schicht-Überwachungssystem gibt zwei Arten von Signalen aus: das Warnsignal und das Alarmsignal. Das Warnsignal weist auf eine unautorisierte Manipulation der Chiffretexte hin, wobei diese Manipulation aufgrund der Resilienz des RHV keinen Einfluss auf die Stellgrößen hat. Das Alarmsignal wird ausgegeben, sobald eine Manipulation an den Chiffretexten Auswirkungen auf die Stellgrößen hat. Die Unterscheidung, ob ein Cyberangriff Einfluss auf die

Stellgrößen nimmt oder nicht, ermöglicht zwei gewinnbringende Schlüsse. Zum einen wird jeder Cyberangriff auf das cloudbasierte Regelungssystem erkannt, sodass ein Anlagenbetreiber rechtzeitig Gegenmaßnahmen einleiten kann. Zum anderen kann die Produktion auch im Falle eines Cyberangriffs fortgeführt werden, solange nur ein Warnsignal vorliegt und kein unerwünschter Einfluss auf die Stellgrößen stattfindet.

Die Methoden in dieser Arbeit bieten einen umfassenden Schutz vor Cyberangriffen auf Regelungssysteme. Durch die Existenz von Chiffretexten im Netzwerk und auf Seiten der Regelung ist die Vertraulichkeit sensibler Daten gewährleistet. Die Weiterentwicklung vom RHV zum PQS-RHV sichert die Vertraulichkeit der Informationen in cloudbasierten Regelungssystemen auch in Zeiten eines Quantencomputers. Die Weiterentwicklung vom RHV zum MS-RHV zeigt Möglichkeiten auf, die Netzwerklast von verschlüsselten, cloudbasierten Regelungssystemen zu reduzieren. Die Resilienzeigenschaften der Verschlüsselungsverfahren erlauben Manipulationskorrekturen an den Chiffretexten, sodass die wahren, unverfälschten Stellgrößen den technischen Prozess erreichen. Das Zwei-Schicht-Überwachungssystem erkennt den Einfluss eines Cyberangriffs, wodurch rechtzeitig Gegenmaßnahmen eingeleitet werden können. Zusammengefasst sind in dieser Arbeit Verfahren entwickelt worden, die die Verfügbarkeit der Anlage durch die Eigenschaft der Resilienz erhöhen, die Vertraulichkeit sensibler Daten gewährleisten und die Integrität der Daten bewahren.

A Notation

General notations

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integers
$\mathbb{R}$	Set of real numbers
$\lfloor \cdot \rfloor$	Floor operator
$\lceil \cdot \rfloor$	Rounding operator
$\lceil \cdot \rceil$	Ceiling operator
mod	Modulo operator
$\langle \boldsymbol{f}, \boldsymbol{w} \rangle$	Inner product of the vectors $\boldsymbol{f}, \boldsymbol{w}$
$\boldsymbol{f} \otimes \boldsymbol{w}$	Kronecker product of the vectors $\boldsymbol{f}, \boldsymbol{w}$
$\boldsymbol{f} \circ \boldsymbol{w}$	Hadamard product of vectors $\boldsymbol{f}, \boldsymbol{w}$
$\mathcal{F} \oplus \mathcal{W}$	Minkowski addition of the sets $\mathcal{F}, \mathcal{W}$
$\bigoplus_{k=1}^{K} \mathcal{F}_k$	Minkowski addition of the sequence of sets $\mathcal{F}_k$
$\|\boldsymbol{f}\|_1$	1-norm of the vector $\boldsymbol{f}$
$\|\boldsymbol{f}\|_2$	Euclidean norm of the vector $\boldsymbol{f}$
$\|\boldsymbol{F}\|_{max}$	Maximum norm of the matrix $\boldsymbol{F}$
$\|\boldsymbol{f}\|_\infty$	Infinity norm of the vector $\boldsymbol{f}$
$\mathbf{1}_{n \times 1}$	Column vector of ones of dimensions $n \times 1$
$\boldsymbol{I}_n$	Identity matrix of dimensions $n \times n$
$\boldsymbol{O}_n$	Zero matrix of dimensions $n \times n$
$negl$	Negligible function
$KeyGen$	Key generation function
sk	Secret key
Enc	Encryption function
Dec	Decryption function
$Eval$	Evaluation function
κ	Security level
φ	Mean value
σ	Standard deviation
ρ	Bit-size of the noise
ψ	Bit-size of the prime number p
γ	Bit-size of the ciphertexts
q, p	Integer q and prime number p of bit-size ψ
$\mathcal{D}_{\gamma,\rho}(q, p)$	Approximate greatest common divisor (AGCD) distribution
$\mathcal{U}_\gamma$	Uniform distribution over the interval $[0, 2^\gamma - 1]$
$\mathcal{A}$	Adversary
$\mathcal{E}$	Encryption scheme
$\mathcal{M}$	Plaintext space

Notations in Chapter 3

z_0	Divisor in the modulo operation
λ_1	Range of the quantization
λ_2	Resolution of the quantization
M	Bound of the plaintext
Q	Quantization function
$\mathcal{Q}$	Set of quantized values
Γ	Mapping function
Γ^{-1}	Inverse mapping function
$\mathcal{H}$	Distribution over the set of integers $\mathbb{Z}$
$\mathcal{H}^{(<h_0)}$	Distribution right-truncated over the interval $(-\infty, h_0)$
$\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$	Right-truncated AGCD distribution
$\mathcal{U}_{\gamma}^{(<u_0)}$	Right-truncated uniform distribution
$f_H(h)$	Probability mass function of the distribution $\mathcal{H}$
$f_H(h \mid H < h_0)$	Probability mass function of the distribution $\mathcal{H}^{(<h_0)}$
$f_H(h \mid H \geq h_0)$	Probability mass function of the distribution $\mathcal{H}^{(\geq h_0)}$
$f_U(u)$	Probability mass function of the uniform distribution $\mathcal{U}_{\gamma}$
$f_U(u \mid U < u_0)$	Probability mass function of the distribution $\mathcal{U}_{\gamma}^{(<u_0)}$
$f_Z(z)$	Probability mass function of the AGCD distribution $\mathcal{D}_{\gamma,\rho}(q,p)$
$f_Z(z \mid Z < z_0)$	Probability mass function of the distribution $\mathcal{D}_{\gamma,\rho}^{(<z_0)}(q,p)$
$F(h_0)$	Cumulative distribution function
$\max_i$	Maximum with respect to all variables i
$\emptyset$	Empty set
$\mathcal{F}$	Non-empty robust positively invariant set
$\mathcal{G}$	Set of the quantization error
$\mathcal{S}$	Robust positively invariant set
$\mathcal{S}_{\infty}$	Minimal robust positively invariant set
$\mathcal{X}_{\Sigma}$	Set of the state vector of the closed-loop system
$h_{\mathcal{G}}$	Support function of the set $\mathcal{G}$
$h_{\mathcal{S}}$	Support function of the set $\mathcal{S}$

Notations in Chapter 4

$\overline{z}_0$	Divisor in the modulo operation
$g_f^{-1}(\boldsymbol{w}_c)$	Base-b decomposition of the vector $\boldsymbol{w}_c$
$\mathcal{H}^{(\geq h_0)}$	Distribution left-truncated over the interval $[h_0, \infty)$
$\mathcal{D}_{\gamma,\rho}^{(\geq 2^{\gamma-1})}(q,p)$	Left-truncated AGCD distribution
$\mathcal{U}_{\gamma}^{(\geq 2^{\gamma-1})}$	Left-truncated uniform distribution
$\mathcal{D}_{\gamma,\rho}^{(<\overline{z}_0)}(q,p)$	Right-truncated AGCD distribution
$\mathcal{U}_{\gamma}^{(<u_0)}$	Right-truncated uniform distribution

Notations in Chapter 5

$\tilde{z}_0$	Divisor in the modulo operation
τ	The number of prime numbers $p_1, \cdots, p_\tau$
$(f_l)_j$	The jth entry of the lth vector $\boldsymbol{f}_l$
$(w_l)_j$	The jth entry of the lth vector $\boldsymbol{w}_l$

Notations in Chapter 7

ϕ_1	Warning signal
ϕ_2	Alarm signal
e_1	Residual signal of the warning signal ϕ_1
e_2	Residual signal of the alarm signal ϕ_2

B Acronyms

HE	Homomorphic encryption	3
RHE	Resilient homomorphic encryption	3
PQS-RHE	Post-quantum secure resilient homomorphic encryption	3
CRT	Chinese remainder theorem	3
MS-RHE	Multi-slot resilient homomorphic encryption	3
LWE	Learning with errors	3
LTI	Linear time-invariant	8
IND-CPA	Indistinguishability under chosen-plaintext attack	4
KPA	Known plaintext attacks	12
AGCD	Approximate greatest common divisor	13
EF-AGCD	Error-free approximate greatest common divisor	13
RSA	Rivest-Shamir-Adleman	15
PHE	Partially homomorphic encryption	15
MPC	Model predictive control	15
FHE	Fully homomorphic encryption	15
CKKS	Cheon-Kim-Kim-Song	16
GSW	Gentry-Sahai-Waters	16
FIR	Finite impulse response	16
IOHFC	Input-output history feedback controller	16
BFV	Brakerski/Fan-Vercauteren	16
PMF	Probability mass function	30
CDF	Cumulative distribution function	30
ECM	Elliptic-curve method	34
NFS	Number field sieve	34
RPI	Robust positively invariant	39
DFT	Discrete Fourier Transform	67
LinHAE	Linearly homomorphic authenticated encryption	89
RHV	Resiliente Homomorphe Verschlüsselungsverfahren	3
PQS-RHV	Post-Quantesichere Resiliente Homomorphe Verschlüsselungsverfahren	3
CR	Chinesischer Restsatz	3
MS-RHV	Multi-Slot Resiliente Homomorphe Verschlüsselungsverfahren	3
LFHV	Lernen mit Fehlern Homomorphe Verschlüsselungsverfahren	105

C List of Publications

Several articles related to encrypted control systems have been finished during the doctoral studies. In a part of these, extracts of the thesis results has been published. At first, a chronological list of the articles with a relation to this thesis is given below.

[1] M. Fauser and P. Zhang. "Resilience of Cyber-Physical Systems to Covert Attacks by Exploiting an Improved Encryption Scheme". In: *Proceedings of the 59th IEEE Conference on Decision and Control (CDC)*, pp. 5489-5494, 2020. (**Chapter 3**)

[2] M. Fauser and P. Zhang. "Resilient Homomorphic Encryption Scheme for Cyber-Physical Systems". In: *Proceedings of the 60th IEEE Conference on Decision and Control (CDC)*, pp. 5489-5494, 2021. (**Chapter 3**)

[3] M. Fauser and P. Zhang. "Detection of Cyber Attacks in Encrypted Control Systems". In: *IEEE Control Systems Letters*, vol. 6, pp. 2365-2370, 2022. (**Chapter 7**)

[4] M. Fauser and P. Zhang. "Multi-Slot Resilient Homomorphic Encryption of Dynamic Feedback Controllers". In: *Proceedings of the 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, Valletta, Malta, 2024. (**Chapter 5**)

[5] M. Fauser and P. Zhang. "Practical Aspects of Homomorphic Encryption Schemes for Dynamic Feedback Controllers". In: *Proceedings of the 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, Valletta, Malta, 2024. (**Chapter 6**)

[6] M. Fauser and P. Zhang. "A Secure Resilient Homomorphic Encryption Scheme for Control Systems". *Accepted by IEEE Transactions on Automatic Control*. (**Chapter 3**)

[7] M. Fauser and P. Zhang. "A Post-Quantum Secure Resilient Homomorphic Encryption Scheme for Cloud-Based Control Systems". *Submitted to Automatica*. (**Chapter 4**)

Secondly, a chronological list of articles that have been successfully published but are not included in this doctoral study is provided.

[8] R. Fritz, M. Fauser and P. Zhang. "Controller Encryption for Discrete Event Systems". In: *Proceedings of the 2019 American Control Conference (ACC)*, pp. 5633 - 5638, Philadelphia, USA, 2019.

[9] M. Fauser and P. Zhang. "Resilience of Cyber-Physical Systems to Covert Attacks by exploiting Frequency Hopping Spread Spectrum". In: *Proceedings of the 2021 American Control Conference (ACC)*, pp. 4631-4636, 2021.

[10] M. Fauser, P. Zhang, S. Wadle and J. Hirtz. "Improved Action Potential Detection for Imaging Techniques by exploiting Fuzzy C-Means Clustering". In: *Proceedings of the 2023 American Control Conference (ACC)*, pp. 349-354, San Diego, USA, 2023.

[11] J. E. B. Costales, D. G. Munoz, O. Yadgar, M. Fauser, P. Zhang. "Application of Digital Signature to Attack Detection in a DC Motor Control System". In: *Proceedings of the 12th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)*, Ferrara, Italy, 2024.

Bibliography

Alexandru, A. B., Morari, M., and Pappas, G. J. (2018). "Cloud-based MPC with encrypted data". In: *Proceedings of the 57th IEEE Conference on Decision and Control*. Miami Beach, USA, pp. 5014–5019.

Alexandru, A. B., Tsiamis, A., and Pappas, G. J. (2020). "Towards private data-driven control". In: *Proceedings of the 59th IEEE Conference on Decision and Control*, pp. 5449–5456.

Alexandru, A. B. et al. (2022). "Private Anomaly Detection in Linear Controllers: Garbled Circuits vs. Homomorphic Encryption". In: *Proceedings of the 61st IEEE Conference on Decision and Control*. Cancún, Mexico, pp. 7746–7753.

Baba, R., Kogiso, K., and Kishida, M. (2018). "Detection Method of Controller Falsification Attacks against Encrypted Control System". In: *Proceedings of the SICE Annual Conference*. Nara, Japan, pp. 244–248.

Benarroch, D., Brakerski, Z., and Lepoint, T. (2017). "FHE over the integers: decomposed and batched in the post-quantum regime". In: *Fehr, S. (Ed.) Public-Key Cryptography*. Vol. 10175. Springer, Berlin, pp. 271–301.

Chen, Y. and Nguyen, P. Q. (2012). "Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers". In: *Pointcheval, D., Johansson, T. (Ed.) Advances in Cryptology–EUROCRYPT*. Vol. 7237. Springer, Berlin, pp. 502–519.

Cheon, J. H., Kim, A., Kim, M., and Song, Y. (2017). "Homomorphic encryption for arithmetic of approximate numbers". In: *Takagi, T., Peyrin, T. (Ed.) Advances in Cryptology–ASIACRYPT*. Vol. 10624. Springer, Cham, pp. 409–437.

Cheon, J. H., Kim, J., Lee, M. S., and Yun, A. (2015). "CRT–based fully homomorphic encryption over the integers". In: *Information Sciences* 310, pp. 149–162.

Cheon, J. H. and Stehlé, D. (2015). "Fully homomophic encryption over the integers revisited". In: *Oswald, E., Fischlin, M. (Ed.) Advances in Cryptology–EUROCRYPT*. Vol. 9056. Springer, Berlin, pp. 513–536.

Cheon, J. H. et al. (2018). "Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption". In: *IEEE Access* 6, pp. 24325–24339.

CISA (2017). *Malware analysis report mar-17-352-01 HatMan - safety system targeted malware*. Tech. rep. Cybersecurity & infrastructure security Agency (CISA).

Cominetti, E. L. and Simplicio, M. A. (2020). "Fast additive partially homomorphic encryption from the approximate common divisor problem". In: *IEEE Transactions on Information Forensics and Security* 15, pp. 2988–2998.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C. (2001). *Introduction to Algorithms*. MIT Press, Cambridge.

Coron, J.-S., Lepoint, T., and Tibouchi, M. (2014). "Scale-invariant fully homomorphic encryption over the integers". In: *Krawczyk, H. (Ed.) Public–Key Cryptography*. Vol. 8383. Springer, Berlin, pp. 311–328.

Coron, J.-S., Mandal, A., Naccache, D., and Tibouchi, M. (2011). "Fully homomorphic encryption over the integers with shorter public keys". In: *Rogaway, P. (Ed.) Advances in Cryptology–CRYPTO*. Vol. 6841. Springer, Berlin, pp. 487–504.

Coron, J.-S., Naccache, D., and Tibouchi, M. (2012). "Public key compression and modulus switching for fully homomorphic encryption over the integers". In: *Pointcheval, D., Johansson, T. (Ed.) Advances in Cryptology–EUROCRYPT*. Vol. 7237. Springer, Berlin, pp. 446–464.

CRA (2022). *Cyber Resilience Act: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*.

Darup, M. S., Alexandru, A. B., Quevedo, D. E., and Pappas, G. J. (2021). "Encrypted control for networked systems: An illustrative introduction and current challenges". In: *IEEE Control Systems Magazine* 41, 3, pp. 58–78.

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

Darup, M. S., Redder, A., Shames, I., Farokhi, F., and Quevedo, D. (2018). "Towards encrypted MPC for linear constrained systems". In: *IEEE Control Systems Letters* 2, 2, pp. 195–200.

Ding, S. X. (2013). *Model-Based Fault Diagnosis Techniques*. Springer, London.

Dyer, J., Dyer, M., and Xu, J. (2019). "Practical homomorphic encryption over the integers for secure computation in the cloud". In: *International Journal of Information Security* 18, 5, pp. 549–579.

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

Fan, J. and Vercauteren, F. (2012). "Somewhat practical fully homomorphic encryption". In: *Cryptology ePrint Archive, Report 2012/144*.

Farokhi, F., Shames, I., and Batterham, N. (2016). "Secure and private cloud-based control using semi-homomorphic encryption". In: *IFAC-PapersOnLine* 49, 22, pp. 163–168.

Faruque, M. A. A. and Vatanparvar, K. (2015). "Energy Management-as-a-Service Over Fog Computing Platform". In: *IEEE Internet of Things Journal* 3, 2.

Fritz, R., Fauser, M., and Zhang, P. (2019). "Controller encryption for discrete event systems". In: *Proceedings of the 2019 American Control Conference*. Philadelphia, USA, pp. 5633–5638.

Galbraith, S. D., Gebregiyorgis, S. W., and Murphy, S. (2016). "Algorithms for the approximate common divisor problem". In: *LMS Journal of Computation and Mathematics* 19, pp. 58–72.

Gayek, J. E. (1991). "A survey of techniques for approximating reachable and controllable sets". In: *Proceedings of the 30th IEEE Conference on Decision and Control*. Brighton, England, pp. 1724–1729.

Gentry, C. (2009). "A Fully Homomorphic Encryption Scheme". PhD thesis. Standford University.

Gentry, C., Sahai, A., and Waters, B. (2013). "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *Canetti, R., Garay, J.A. (Ed.) Advances in Cryptology–CRYPTO*. Vol. 8042. Springer, Berlin, pp. 75–92.

Givehchi, O., Imtiaz, J., Trsek, H., and Jasperneite, J. (2014). "Control-as-a-service from the cloud: A case study for using virtualized PLCs". In: *Proceedings of the 10th IEEE Workshop on Factory Communication Systems*, pp. 1–4.

Johansson, K. H. (2000). "The Quadruple-Tank Process: A Multivariable Laboratory Process with an Adjustable Zero". In: *IEEE Transactions Control Systems Technology* 8, 3, pp. 456–465.

Katz, J. and Lindell, Y. (2020). *Introduction to modern cryptography*. CRC press.

Kim, J., Shim, H., and Han, K. (2020). "Design Procedure for Dynamic Controllers based on LWE-based Homomorphic Encryption to Operate for Infinite Time Horizon". In: *Proceedings of the 59th IEEE Conference on Decision and Control*, pp. 5463–5468.

Kim, J., Shim, H., and Han, K. (2023). "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon". In: *IEEE Transactions on Automatic Control* 68, 2, pp. 660–672.

Kim, J. et al. (2016). "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems". In: *IFAC-PapersOnLine* 49, 22, pp. 175–180.

Kishida, M. (2018). "Encrypted average consensus with quantized control law". In: *Proceedings of the 57th IEEE Conference on Decision and Control*. Miami Beach, USA, pp. 5850–5856.

Kogiso, K. and Fujita, T. (2015). "Cyber-Security Enhancement of Networked Control Systems Using Homomorphic Encryption". In: *Proceedings of the 54th IEEE Conference on Decision and Control*. Osaka, Japan, pp. 6836–6843.

Kosieradzki, S., Zhao, X., Kawase, H., Qiu, Y., Kogiso, K., and Ueda, J. (2022). "Secure Teleoperation Control Using Somewhat Homomorphic Encryption". In: *IFAC-PapersOnLine* 55, 37, pp. 593–600.

Langner, R. (2013). *To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve*. Tech. rep. The Langner Group.

Lee, J., Chang, P. H., and Jin, M. (2017). "Adaptive integral sliding mode control with time-delay estimation for robot manipulators". In: *IEEE Transactions on Industrial Electronics* 64, 8, pp. 6796–6804.

Lee, R., Assante, M., and Conway, T. (2016). *Analysis of the cyber attackon the ukrainian power grid*. Tech. rep. SANS Industrial Control Systems.

Lenstra, A. K., Lenstra, H. W., Manasse, M. S., and Pollard, J. M. (1993). "The number field sieve". In: *Lecture Notes in Mathematics*. Vol. 9056, pp. 11–42.

Lenstra, H. W. (1987). "Factoring Integers with Elliptic Curves". In: *The Annals of Mathematics* 126, 3, p. 649.

Lepoint, T. (2014). "Design and implementation of lattice-based cryptography". PhD thesis. Université du Luxembourg and École Normale Supérieure.

Limnios, N. and Nikulin, M., eds. (2000). *Recent Advances in Reliability Theory: Methodology, Practice and Inference*. CRC Press, Boca Raton, USA.

Liu, K.-Z. and Yao, Y. (2016). *Robust Control: Theory and Applications*. John Wiley & Sons, New York, USA.

Mittelbach, A. and Fischlin, M. (2021). *The Theory of Hash Functions and Random Oracles*. Springer, Cham.

National Institute of Standards and Technology (2020). *Recommendation for Key Management*. Tech. rep. NIST Special Publication 800-57 Part 1, Rev. 5. Washington, D.C.: U.S. Department of Commerce.

National Security Agency (2020). *Mitigating cloud vulnerabilities*. Tech. rep.

NIS2-Directive (2022). *Network and Information Security: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148*.

Paillier, P. (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *Stern, J. (Ed.) Advances in Cryptology–EUROCRYPT*. Vol. 1592. Springer, Berlin, pp. 223–238.

Pei, D., Salomaa, A., and Ding, C. (1996). *Chinese Remainder Theorem: Applications In Computing, Coding, Cryptography*. World Scientific, Singapur.

Pereira, H. V. L. (2020). "Efficient AGCD-based homomorphic encryption for matrix and vector arithmetic". In: *Conti, M., Zhou, J., Casalicchio, E., Spognardi, A. (Ed.) Applied Cryptography and Network Security*. Vol. 12146. Springer, Berlin, pp. 110–129.

Pereira, H. V. L. (2021). "Bootstrapping Fully Homomorphic Encryption over the Integers in Less than One Second". In: *Oswald, J.A. (Ed.) Public-Key Cryptography*. Vol. 12710. Springer, Cham, pp. 331–359.

Rakovic, S. V., Kerrigan, E. C., Kouramas, K. I., and Mayne, D. Q. (2005). "Invariant approximations of the minimal robust positively invariant set". In: *IEEE Transactions on Automatic Control* 50, 3, pp. 406–410.

RED (2014). *Radio Equipment Directive: Directive (EU) 2014/53 of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive (EU) 1999/5*.

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

Romagnoli, R., Weerakkody, S., and Sinopoli, B. (2019). "A Model Inversion Based Watermark for Replay Attack Detection with Output Tracking". In: *Proceedings of the American Control Conference*. Philadelphia, USA, pp. 384–390.

Ruan, M., Gao, H., and Wang, Y. (2019). "Secure and privacy-preserving consensus". In: *IEEE Transactions on Automatic Control* 64, 10, pp. 4035–4049.

Schlüter, N., Neuhaus, M., and Darup, M. S. (2021). "Encrypted dynamic control with unlimited operating time via FIR filters". In: *Proceedings of the 2021 European Control Conference*, pp. 952–957.

Shor, P. W. (1999). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *Society for Industrial and Applied Mathematics* 41, 2, pp. 303–332.

Shoukry, Y. et al. (2016). "Privacy-aware quadratic optimization using partially homomorphic encryption". In: *Proceedings of the 55th IEEE Conference on Decision and Control*. Las Vegas, USA, pp. 5053–5058.

Siderska, J. and Jadaan, K. S. (2018). "Cloud manufacturing: a service-oriented manufacturing paradigm. A review paper". In: *Engineering Management in Production and Services* 10, 1, pp. 22–31.

Smith, R. S. (2011). "A Decoupled Feedback Structure for Covertly Appropriating Networked Control Systems". In: *Proceedings of the18th IFAC Workshop on Distributed Estimation and Control in Networked Systems* 44, 1, pp. 90–95.

Suh, J. and Tanaka, T. (2021). "Encrypted value iteration and temporal difference learning over leveled homomorphic encryption". In: *Proceedings of the 2021 American Control Conference*, pp. 2555–2561.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K. H. (2012). "Revealing stealthy attacks in control systems". In: *Proceedings of the 50th Annual Allerton Conference on Communication, Control and Computing*. Monticello, USA, pp. 1806 –1813.

Teranishi, K., Kogiso, K., and Ueda, J. (2020). "Encrypted Feedback Linearization and Motion Control for Manipulator with Somewhat Homomorphic Encryption". In: *Proceedings of the 2020 International Conference on Advanced Intelligent Mechatronics*, pp. 613–618.

Teranishi, K., Sadamoto, T., and Kogiso, K. (2023). "Input-Output History Feedback Controller for Encrypted Control With Leveled Fully Homomorphic Encryption". In: *IEEE Transactions on Control of Network Systems* 11, 1, pp. 271–283.

Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010). "Fully Homomorphic Encryption over the Integers". In: *Gilbert H. (Ed.) Advances in Cryptology–EUROCRYPT*. Vol. 6110. Springer, Berlin, pp. 24–43.

Wang, C. and Ong, C.-J. (2011). "Support function of minimal disturbance invariant set and its derivative: Application in designing feedback gain". In: *Proceedings of the 8th Asian Control Conference*. Kaohsiung, Taiwan, pp. 1000–1005.

About the author

Moritz Fauser was born on November 5, 1991, in Neuwied, Germany. He earned a diploma degree in Automation Control from the Faculty of Electrical Engineering and Computer Engineering at the University of Kaiserslautern, Rheinland-Pfalz, Germany, in 2019. After graduating, Moritz Fauser joined the Institute of Automatic Control at Technische Universität Kaiserslautern under the supervision of Prof. Ping Zhang. His primary research areas included encryption schemes, cloud-based control systems, and the analysis of cyber attacks. Since May 2024, Moritz Fauser has been working as a Shopfloor Security Expert at Mercedes-Benz AG in Germersheim, Germany.