23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Private State Estimation for Cyber-physical Systems Using Semi-homomorphic Encryption

Mohsen Zamani, Ladan Sadeghikhorrami, Ali Akbar Safavi, and Farhad Farokhi.

Abstract— **This paper is concerned with challenges involved with implementation of a private observer in networked control systems. Here, a secure Luenberger observer over a network is considered. The Paillier encryption, which is a semi-homomorphic encryption method, is employed so that the algebraic calculations required for the estimation can be performed over the encrypted data. This enhances the security of the state estimation process. In particular, we study the challenges associated with implementation of such a private observer on digital processors with limited memory sizes. We provide conditions under which the stability of the implemented private observer is ensured. A numerical example is utilized to demonstrate the theoretical results.**

I. INTRODUCTION

Cyber-security of the networked control system (NCS) associated with industrial and civil infrastructure is a challenging task [1]. Cyber threats can influence confidentiality, integrity or availability of data depending on resources available to attackers [2].

The systems and control community has contributed to handling challenges associated with the security of cyber-physical systems. For instance, network eavesdropping or network sniffing with the aim of capturing the information transmitted over a network between sensors, controller, and actuator is discussed in [3]. Various attack scenarios based on required model knowledge, disruption resources and disclosure resources are discussed in [2]. Replay attacks in noisy environments are considered in [4], [5]. A feedback strategy that allows an attacker to take over the automatic control loop without being detected by the system supervisor is proposed in [6], where it is shown that detection of attacks is impossible if the attacker has complete knowledge of the system model. Zero-dynamics attacks are also discussed in [7]–[9]. False-data injection attack is analyzed in [10]. State estimation in the presence of attacks is considered in [11], where it is proved that state estimates cannot be accurately obtained if more than half of the sensors are compromised. Finally, game-theoretic approaches to capture the conflict of goals between an attacker who aims to maximise damage effects imposed on a plant and a defender who is intended to reduce those effects are considered in [12], [13].

There have been increasing attempts for development of sophisticated control and estimation paradigms that can handle encrypted data in their calculation procedures [14]–[17]. These methodologies significantly improve the secrecy and privacy of signals, such as control commands and sensor measurments. This is because, in such frameworks, sensory information is encrypted prior to its transmission through communication channels decreasing the chance that data get compromised. Furthermore, the control paradigm is also applied to coded data in a way that if a privacy or security breach occurs inside the control unit, a third-party intruder cannot reconstruct the private data. Semi-homomorphic encryption, which is a simpler form of homomorphic encryption and only allow for a category of operations to be performed on the encrypted data, can facilitate this process [14]. In [16], fully homomorphic encryption is employed to obtain a secure linear controller and conditions for ensuring stability and maintaining the closed-loop performance of the system was developed. Moreover, a method for localization of a mobile target based on encrypted sensor measurements is proposed in [18]. In [19], additive homomorphic encryption is exploited to develop a secure Extended Kalman filter paradigm; however, the stability of the proposed setup is not discussed there.

The studies in [14]–[16] are concerned with the control problem. In contrast, in this paper, the objective is to design a secure observer using semi-homomorphic encryption. The problem discussed in this paper is related to that of [17], as the authors of [17], [19] are concerned about secure estimation. In [17], a novel secure observer architecture which integrates multiple observers in the estimation process is discussed; however, due to not using homomorphic encryption techniques, security breaches inside the estimators without a doubt results in (at least) partial information leakage. Unlike [17], in this paper, challenges associated with implementation of secure observers using a homomorphic encryption on a digital processor is examined. This methodology allows for stronger security and privacy guarantees. In particular, an encrypted Luenberger observer using the Paillier encryption method (see [20]) is developed. This enables the proposed observer to not require any private decryption keys. This feature makes the observer robust to privacy and security breaches within the computing units that is responsible for implementing the encrypted observer. Here, we study the deterministic framework, i.e., there is no measurement or process noise. However, this is without

M. Zamani is with the School of Electrical Engineering and Computer Science, The University of Newcastle, Callaghan, NSW 2308, Australia. e-mail:mohsen.zamani@newcastle.edu.au.

L. Sadeghikhorrami and A.A. Safavi are with the Department of Power and Control Engineering, Shiraz University, Shiraz, Iran. e-mails:{l.sadeghikhorram,safavi}@shiraz.ac.ir.

F. Farokhi is with the Department of Electrical and Electronic Engineering at the University of Melbourne, Australia. e-mail:ffarokhi@unimelb.edu.au. The work of F. Farokhi was supported by a McKenzie Fellowship from the University of Melbourne.

loss of generality as the results can be readily extended to stochastic setups with slight modifications. In this paper, we further introduce conditions under which the proposed observer can be implemented on an embedded system with finite memory. The computational aspects, such as memory management and numerical stability of observer, are missing from [19].

The structure of the paper is as follows. First, some background materials in relation to fixed-point arithmetic and semi-homomorphic encryptions are introduced in Section II. The main result of the paper, which is a novel encrypted observer and the required convergence analysis, is given in Section III. A numerical example to illustrate the theoretical findings is provided in Section IV. Finally, the paper is concluded in Section V.

II. Background Materials

In this section, some basic results from fixed-point rational numbers and encryption theory literature are reviewed.

A. Fixed-Point Arithmetic

In this paper, signed fixed-point rational numbers in base 2 are considered. Integers $n, m \in \mathbb{N}$ determine the length and the resolution of the fixed-point rationals. The set of all such numbers are given by

$$\mathbb{Q}_{(n,m)} := \Big\{ b \in \mathbb{Q} \,|\, b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} 2^{i-m-1} b_i, \\ b_i \in \{0,1\}\, \forall i \in \{1,\dots,n\} \Big\},$$

which contains all rational numbers in $[-2^{n-m-1}, 2^{n-m-1} - 2^{-m}]$ separated from each other by 2^{-m}.

In order for these fixed-point rationals to be exploited in a digital processor, they require to be transformed into integers. To do so, the mapping $f_{n,m} : \mathbb{Q}_{(n,m)} \to \mathbb{Z}_{2^n}$, which is defined by $f_{n,m}(b) = 2^m b \bmod 2^n$ for all $b \in \mathbb{Q}_{(n,m)}$ is used. Here, $\mathbb{Z}_q$ denotes the set of integers modulo $q \in \mathbb{N}$. The inverse mapping $f_{n,m}^{-1} : \mathbb{Z}_{2^n} \to \mathbb{Q}_{(n,m)}$ can also be expressed (see [14] for proof) as $f_{n,m}^{-1}(a) = (a - 2^n \mathbb{1}_{a \geq 2^{n-1}})/2^m$ for all $a \in \mathbb{Z}_{2^n}$, where

$$\mathbb{1}_p = \begin{cases} 1 & \text{if the statement } p \text{ holds true,} \\ 0 & \text{otherwise.} \end{cases}$$

Some essential results from [14] needs to be recited. The following proposition studies elementary operations in the set of fixed-point rationals.

Lemma 2.1: The following identities hold:

1) For all $b, b' \in \mathbb{Q}_{(n,m)}$ such that $b + b' \in \mathbb{Q}_{(n,m)}$, $f_{n,m}(b + b') = (f_{n,m}(b) + f_{n,m}(b')) \bmod 2^n$;
2) For all $b \in \mathbb{Q}_{(n,m)}$ such that $-b \in \mathbb{Q}_{(n,m)}$, $f_{n,m}(-b) = 2^n - f_{n,m}(b)$;
3) For all $b, b' \in \mathbb{Q}_{(n,m)}$ such that $b - b' \in \mathbb{Q}_{(n,m)}$, $f_{n,m}(b - b') = (2^n + f_{n,m}(b) - f_{n,m}(b')) \bmod 2^n$;
4) For all $b, b' \in \mathbb{Q}_{(n,m)}$ such that $bb' \in \mathbb{Q}_{(n,m)}$, $f_{n,m}(bb') = ((f_{n,m}(b) - 2^n \mathbb{1}_{b<0})(f_{n,m}(b') - 2^n \mathbb{1}_{b'<0})/2^m) \bmod 2^n$.

As implied by the fourth item in Lemma 2.1, multiplication is a more difficult operation to implement compared to summation because it requires the sign of the operands. However, this need can be eliminated using the following proposition [14].

Lemma 2.2: For all $b, b' \in \mathbb{Q}_{(n,m)}$ if $bb' \in \mathbb{Q}_{(n,m)}$, $f_{n+2m,0}(2^{2m}\ bb') = (f_{n+2m,0}(2^m b))(f_{n+2m,0}(2^m b'))$.

This lemma essentially states that it is possible to multiply two rational numbers without checking their sign if they are first transformed into integers.

B. Semi-Homomorphic Encryption

In this subsection, the Paillier encryption technique, which is a semi-homomorphic encryption scheme, is introduced. The semantic security of technique relies on Decisional Composite Residuosity Assumption [20]. The encryption and decryption schemes are as follows.

Encryption: Assume $N = pq$, where p and q are two independently generated random prime numbers to ensure that $\gcd(pq, (1-p)(1-q)) = 1$ with gcd stands for the greatest common divisor. The public key N is required for encrypting the data and can be shared publicly among participating parties (as it cannot be used by anyone for prying on the encrypted messages). The encryption of a message $t \in \mathbb{Z}_N$ is

$$E(t; r) = (N+1)^t r^N \bmod N^2,$$

where r is randomly selected from the set $\mathbb{Z}_N^* := \{x \in \mathbb{Z}_N | \gcd(x, N) = 1\}$.

Decryption: Set $\lambda = \mathrm{lcm}(p-1, q-1)$, where lcm refers to the least common multiple and $\mu = \lambda^{-1} \bmod N$. The pair (λ, μ) is the private key and needs to be retained by the entity that can legitimately decrypt the data. For any ciphertext $c \in \mathbb{Z}_{N^2}$, the plain text is given by

$$D(c) = ((c^\lambda \bmod N^2) - 1)\mu / N \bmod N.$$

An important property of the Paillier encryption is that there is an invertible relationship between the encrypted texts and the plain text, i.e., $D(E(t; r)) = t$ for all $t \in \mathbb{Z}_N$ and all $r \in \mathbb{Z}_N^*$. The following properties demonstrates that the Paillier scheme is a semi-homomorphic encryption method.

Proposition 2.3: The following properties hold:

i) For all $r, r' \in \mathbb{Z}_N^*$ and $t, t' \in \mathbb{Z}_N$ such that $t + t' \in \mathbb{Z}_N$, $E(t; r)E(t'; r') \bmod N^2 = E(t + t'; rr')$;
ii) For all $r \in \mathbb{Z}_N^*$ and $t, t' \in \mathbb{Z}_N$ such that $tt' \in \mathbb{Z}_N$, $E(t; r)^{t'} \bmod N^2 = E(t't; r^{t'})$.

The above proposition from [20] permits calculations such as addition and multiplication to be performed on the encrypted data.

In the next section, we utilize the reviewed background materials to propose a novel encrypted Luenberger observer.

III. Main results

In this section we propose a secure observer setup as shown in Fig. 1. Specifically, we apply the semi-homomorphic encryption studied in the previous section for dealing with encrypted data within the Luenberger observer.

As can be seen from Fig. 1, the observer admits encrypted parameters and signals. Moreover, as the observer does not have access to the private decryption key, all observer calculations are done over the encrypted data. Hence, even if the security of the observer is compromised, the confidentially of information remains intact. This is further discussed in this section.

Consider a discrete linear time-invariant system given by

$$\begin{aligned} \bar{x}_{k+1} &= \bar{A}\bar{x}_k + \bar{B}\bar{u}_k,\ \bar{x}_0 = \bar{x}(0) \\ \bar{y}_k &= \bar{C}\bar{x}_k, \end{aligned} \tag{1}$$

where $\bar{x}_k \in \mathbb{R}^{p_x}$ is the state, $\bar{y}_k \in \mathbb{R}^{p_y}$ is the output, and $\bar{u}_k \in \mathbb{R}^{p_u}$ is the input. The Luenberger observer is a standard method for observing the states of the system (1) and takes the form of

$$\begin{aligned} \hat{x}_{k+1} &= \bar{A}\hat{x}_k + \bar{B}\bar{u}_k + \bar{W}(\bar{y}_k - \hat{y}_k), \\ \hat{y}_k &= \bar{C}\hat{x}_k. \end{aligned} \tag{2}$$

The following assumption is made throughout the paper.

Assumption 3.1: The system in (1) is stable and the pair $(\bar{A}, \bar{C})$ is observable.

One should note that the stability assumption is imposed just to ensure that the size of the state variables do not exceed the memory length of the digital processor.

The observability assumption in 3.1 ensure that there exists $\bar{W} \in \mathbb{R}^{p_x \times p_y}$ such that $\lim_{k\to\infty} \|\bar{x}_k - \hat{x}_k\| \to 0$. To be able to implement the observer law in (2) on digital computers, one needs to restrict parameters of the dynamics and the observer, which are referred to with A ,B, C, and W, to be, respectively, in the sets $\mathbb{Q}_{(n,m)}^{p_x \times p_x}$, $\mathbb{Q}_{(n,m)}^{p_x \times p_u}$, $\mathbb{Q}_{(n,m)}^{p_y \times p_x}$, and $\mathbb{Q}_{(n,m)}^{p_x \times p_y}$, which have the obvious relation with the set $\mathbb{Q}(n, m)$, for some appropriately selected parameters $n, m \in \mathbb{N}$. Methods for selecting these parameters is discussed later in the paper. In what follows, we select the quantized model parameters as

$$\begin{aligned} A &\in \underset{A' \in \mathbb{Q}_{(n,m)}^{p_x \times p_x}}{\arg\min} \left\|A' - \bar{A}\right\|_F, \\ B &\in \underset{B' \in \mathbb{Q}_{(n,m)}^{p_x \times p_u}}{\arg\min} \left\|B' - \bar{B}\right\|_F, \\ C &\in \underset{C' \in \mathbb{Q}_{(n,m)}^{p_y \times p_x}}{\arg\min} \left\|C' - \bar{C}\right\|_F, \\ W &\in \underset{W' \in \mathbb{Q}_{(n,m)}^{p_x \times p_y}}{\arg\min} \left\|W' - \bar{W}\right\|_F. \end{aligned}$$

The input and output signals also need to be appropriately quantized for digital implementation of the observer law in (2). Let $u_k \in \mathbb{Q}_{(n,m)}^{p_u}$, $y_k \in \mathbb{Q}_{(n,m)}^{p_y}$, and $x_0 \in \mathbb{Q}_{(n,m)}^{p_x}$ be the quantized versions of the input, the output, the initial condition, which are defined as

$$\begin{aligned} u_k &\in \underset{u_k' \in \mathbb{Q}_{(n,m)}^{p_u}}{\arg\min} \|u_k' - \bar{u}_k\|_F, \\ y_k &\in \underset{y_k' \in \mathbb{Q}_{(n,m)}^{p_y}}{\arg\min} \|y_k' - \bar{y}_k\|_F, \\ x_0 &\in \underset{x_0' \in \mathbb{Q}_{(n,m)}^{p_x}}{\arg\min} \|x_0' - \bar{x}_0\|_F. \end{aligned}$$

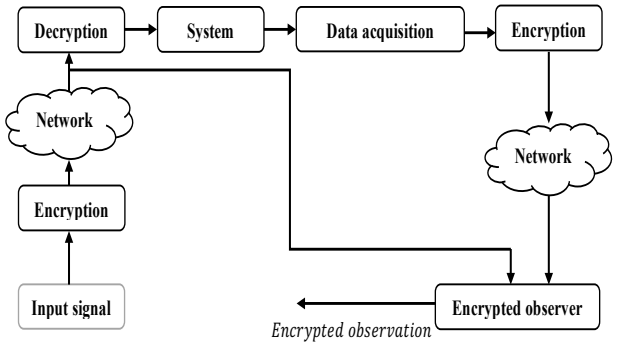


Fig. 1. The structure of the secure observer.

Note that the quantization of the output is always possible because the system is stable and thus its inputs and outputs remain bounded. In fact, let $M(x_0)$ be such that, for the system (1), $\bar{y}_k \in [-M(x_0), M(x_0)]^{p_y}$ and $\bar{u}_k \in [-M(x_0), M(x_0)]^{p_u}$. The fact that $M(x_0)$ is the same for both the output and the input does not introduce any conservatism as it can be selected large enough.

Now, one can utilize a variation of Luenberger observer in (2) in which the variables and the model matrices are both discretized. That observer is given by

$$\begin{aligned} \hat{\zeta}_{k+1} &= A\hat{\zeta}_k + Bu_k + W(y_k - \hat{\phi}_k), \\ \hat{\phi}_k &= C\hat{\zeta}_k, \end{aligned} \tag{3}$$

where $\hat{\zeta}_k \in \mathbb{Q}_{(n',m')}^{p_x}$ denotes the state estimate for an appropriately selected n', m'. Note that, naturally, $n' > n$ and $m' > m$ as multiplication and addition can at least increase the number of fractional bits. In fact, n' and m' should be also selected based on T (as it determines the number of multiplications and summations that occur overall). This issue is discussed in more detail later (see Theorem 3.3).

As stated earlier, the main objective is to implement the observer paradigm depicted in Fig. 1 such that its estimates remain inside a small ball centred at the actual state $\bar{x}_k$ with radius δ over a finite horizon $T \in \mathbb{N}$. Note that finite horizon T is necessary as with multiplication over time the size of the integers required for representing the state estimate goes to infinity since the number of fractional bits increases (i.e., the state estimate converges to a real number). As computers are incapable of working with real numbers, the observer needs to be reset every once in a while (determined by the horizon T). We need to write the dynamics of the error $\hat{\zeta}_{k+1} - \bar{x}_{k+1}$ given by

$$\begin{aligned} \hat{\zeta}_{k+1} - \bar{x}_{k+1} =& A\hat{\zeta}_k - \bar{A}\bar{x}_k + Bu_k - \bar{B}\bar{u}_k \\ &+ W(y_k - \bar{y}_k) + W(\bar{C}\bar{x}_k - C\hat{\zeta}_k) \\ =& (\bar{A} - \bar{W}\bar{C})(\hat{\zeta}_k - \bar{x}_k) + W(y_k - \bar{y}_k) \\ &+ (A - \bar{A})\hat{\zeta}_k + (B - \bar{B})u_k + \bar{B}(u_k - \bar{u}_k) \\ &+ (W - \bar{W})\bar{C}(\bar{x}_k - \hat{\zeta}_k) + W(\bar{C} - C)\hat{\zeta}_k. \end{aligned}$$

Set κ to be an integer larger than all the entries of matrices $\bar{A}$, $\bar{B}$, $\bar{C}$, and $\bar{W}$ and vectors $\bar{y}_k$ and $\bar{u}_k$.

Assumption 3.2: $n \geq m + 1 + \log_2(\kappa)$.

This condition is to make sure that the mesh of the quantization is large enough to capture every possible element of the aforementioned matrices and vectors with a small error in the scale of 2^{-m}. Define g_k for all k to be a disturbance signal equal to

$$\begin{aligned} g_k =& W(y_k - \bar{y}_k) + (A - \bar{A})\hat{\zeta}_k + (B - \bar{B})u_k + \bar{B}(u_k - \bar{u}_k) \\ &+ (W - \bar{W})\bar{C}(\bar{x}_k - \hat{\zeta}_k) + W(\bar{C} - C)\hat{\zeta}_k. \end{aligned}$$

By triangular inequality and the definition of the norm, it can be shown that

$$\begin{aligned} \|g_k\| \leq& \|W\|\|y_k - \bar{y}_k\| + \|A - \bar{A}\|\|\hat{\zeta}_k\| + \|B - \bar{B}\|\|u_k\| \\ &+ \|\bar{B}\|\|u_k - \bar{u}_k\| + \|W - \bar{W}\|\|\bar{C}\|\|\bar{x}_k - \hat{\zeta}_k\| \\ &+ \|W\|\|\bar{C} - C\|\|\hat{\zeta}_k\|. \end{aligned}$$

Therefore, there exists a large enough constant $\vartheta > 0$ (in virtue of the stability of the system by Assumption 3.1) such that $\|g_k\| \leq \vartheta 2^{-m}$. Now, we can prove that, if the horizon T is selected large enough, the error term $\hat{\zeta}_{k+1} - \bar{x}_{k+1}$ enters inside a ball which its radius is proportional to 2^{-m}. Therefore, the quality of the observer can be fine-tuned by the selection of m.

Theorem 3.3: Under Assumptions 3.1 and 3.2, there exists a $T \in \mathbb{N}$ such that $\|\hat{\zeta}_T - \bar{x}_T\|^2 \leq \varrho 2^{-m}$ for some constant $\varrho > 0$ if $m' \geq 10Tm$ and $n' \geq 5T(2n+1)$.

Proof: Let $e_k := \hat{\zeta}_k - \bar{x}_k$. Then, we get

$$e_{k+1} = (\bar{A} - \bar{W}\bar{C})e_k + g_k.$$

Since $\bar{A} - \bar{W}\bar{C}$ is Schur, there exists positive definite matrix P such that $(\bar{A} - \bar{W}\bar{C})^\top P(\bar{A} - \bar{W}\bar{C}) - P = -I$. Now, note that

$$\begin{aligned} e_{k+1}^\top P e_{k+1} - & e_k^\top P e_k \\ =& e_k^\top((\bar{A} - \bar{W}\bar{C})^\top P(\bar{A} - \bar{W}\bar{C}) - P)e_k \\ &+ 2e_k^\top(\bar{A} - \bar{W}\bar{C})^\top P g_k + g_k^\top g_k \\ =& -e_k^\top e_k + 2e_k^\top(\bar{A} - \bar{W}\bar{C})^\top P g_k + g_k^\top g_k. \end{aligned}$$

Let $E > 0$ be such that the set $e_k^\top e_k \leq E$ is an invariant set. Such E exists as the error e_k is, by definition, bounded. This is because the state of the system $\bar{x}_k$ is bounded (due to Assumption 3.1) and the estimates $\hat{\zeta}_k$ belong to $\mathbb{Q}_{(n',m')}^{p_x}$ (which is a bounded set). Moreover, note that the disturbance term g_k is also bounded (recall that $\|g_k\| \leq \vartheta 2^{-m}$). Then, there exists a constant $c'(E)$ such that $e_{k+1}^\top P e_{k+1} - e_k^\top P e_k \leq -e_k^\top e_k + c'(E)2^{-m}$. Now, we need to establish that there exists T for which $\|\hat{\zeta}_T - \bar{x}_T\|^2 = \|e_T\|^2 \leq 2c'(E)2^{-m}$. This is done by *reductio ad absurdum*. Suppose that the statement of theorem does not hold i.e. for all k such that $\|e_k\|^2 > 2c'(E)2^{-m}$. It can be shown that

$$\begin{aligned} e_{k+1}^\top P e_{k+1} - e_k^\top P e_k &\leq -e_k^\top e_k + c'(E)2^{-m} \\ &\leq -c'(E)2^{-m}, \end{aligned}$$

and as a result of the above inequality one can write

$$\begin{aligned} e_T^\top P e_T &= e_1^\top P e_1 + \sum_{k=1}^{T-1}(e_{k+1}^\top P e_{k+1} - e_k^\top P e_k) \\ &\leq e_1^\top P e_1 - (T-2)c'(E)2^{-m}. \end{aligned}$$

If we choose T as $1 \leq T \leq T_{\max} := \lceil \big(2^m e_1^\top P e_1 / c'(E)\big) + 2 \rceil$. Then it is easy to see that $e_T^\top P e_T < 0$. This is in contradiction with the fact that $e_T^\top P e_T \geq 0$ as P is a positive definite matrix. The statement of the theorem thus holds with the choice of $\varrho := 2c'(E)$ and if n' and m' are selected such that $\hat{\zeta}_k \in \mathbb{Q}_{(n',m')}^{p_x}$ under the update law (3) over the horizon T. It can be verified that under the update role (3) by selecting $m' \geq 10Tm$ and $n' \geq 5T(2n+1)$ the statement of theorem holds. ∎

We propose Algorithm 1 to ensure secure implementation of the dynamic observer law in (3).

The following theorem determines the minimum memory size required so that the computations in encrypted observer associated with (3) remain valid.

Theorem 3.4: Under conditions of Theorem 3.3, there exists a $T \in \mathbb{N}$ such that $\|\hat{\zeta}_T - \bar{x}_T\|^2 \leq \varrho 2^{-m}$ for some constant $\varrho > 0$ if $N \geq 2^{n'+m'}$.

Proof: The results follow from the application of Theorem 3.3 and the preliminary results on the Paillier's encryption technique. In fact, we must select $N \geq 2^{n'+m'}$ as the encryption is only valid (i.e., it is invertible) if its size N is larger than the largest integer that needs to be encrypted $2^{n'+m'}$. ∎

IV. Numerical example

The Tennessee-Eastman process is a realistic simulation of a chemical system that has been widely used in process control studies [21]. In the following we exploit the simplified model of this process [22] and [23].

$$\begin{bmatrix} F_4 \\ P \\ y_{A3} \\ V_L \end{bmatrix} = \begin{bmatrix} h_{11} & 0 & 0 & h_{14} \\ h_{21} & 0 & h_{23} & 0 \\ 0 & h_{32} & 0 & 0 \\ 0 & 0 & 0 & h_{44} \end{bmatrix} \begin{bmatrix} u^1 \\ u^2 \\ u^3 \\ u^4 \end{bmatrix} \tag{4}$$

The individual transfer functions are given as

$$\begin{aligned} h_{11} =& \frac{1.7}{0.75s+1}, \\ h_{21} =& \frac{45(5.667s+1)}{2.5s^2+10.25s+1}, \\ h_{23} =& \frac{-15s-11.25}{2.5s^2+10.25s+1}, \\ h_{32} =& \frac{1.5}{10s+1}e^{-0.1s}, \\ h_{14} =& \frac{-3.4s}{0.1s^2+1.1s+1}, \\ h_{44} =& \frac{1}{s+1}. \end{aligned}$$

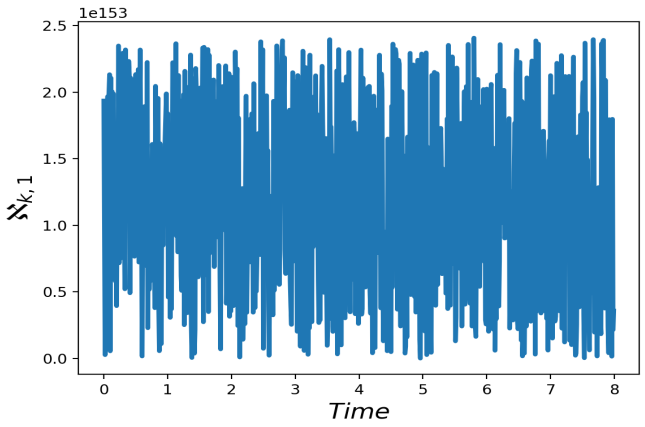
Algorithm 1 Secure Luenberger observer.

Input: $n', m', T, (y_k)_{k=1}^{T}, A, B, C, W$
Output: $(\hat{\zeta}_k)_{k=1}^{T}$

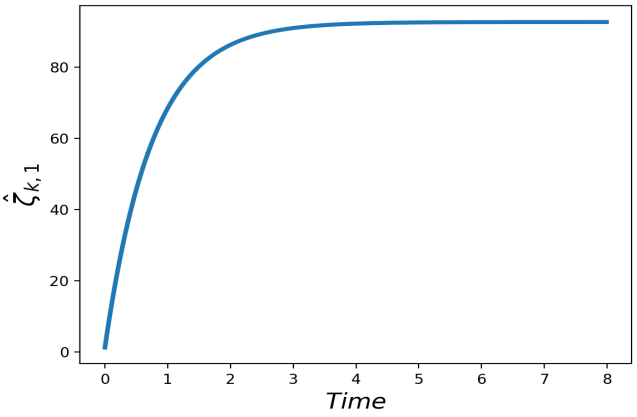
# **sensor**
for $i = 1, ..., p_y$ **do**
  transmit $Z_{k,i} = E(f_{n'+2m',0}(2^{m'} y_{k,i}); r)$ to the observer, where $y_{k,i}$ denotes the i-th element of y_k
end for
# **controller**
for $j = 1, ..., p_u$ **do**
  transmit $L_{k,j} = E(f_{n'+2m',0}(2^{m'} u_{k,j}); r)$ to the observer
end for
# **observer**
at $k = 0$, initialize $\aleph_{0,i} = E(0; r)$ for all i
for $k = 1, \ldots, T$ **do**
  for $i = 1, ..., p_x$ **do**
    set $\aleph_{k,i} = \aleph_{k-1,i}^{f_{n'+2m',0}(2^{m'} A_{i1})} \bmod N^2$
    for $j = 2, ..., p_x$ **do**
      $\aleph_{k,i} = \aleph_{k,i}(\aleph_{k,j}^{f_{n'+2m',0}(2^{m'} A_{ij})} \bmod N^2) \bmod N^2$
    end for
    for $j = 1, ..., p_u$ **do**
      $\aleph_{k,i} = \aleph_{k,i}(L_{k,j}^{f_{n'+2m',0}(2^{m'} B_{ij})} \bmod N^2) \bmod N^2$
    end for
    for $j = 1, ..., p_y$ **do**
      $\aleph_{k,i} = \aleph_{k,i}(Z_{k,j}^{f_{n'+2m',0}(2^{m'} W_{ij})} \bmod N^2) \bmod N^2$
    end for
    for $j = 1, ..., p_x$ **do**
      $\aleph_{k,i} = \aleph_{k,i}(Z_{k,j}^{f_{n'+2m',0}(-2^{m'} \sum_\ell W_{i\ell} C_{\ell j})} \bmod N^2) \bmod N^2$
    end for
  end for
  transmit $\aleph_k$
end for
# monitoring node
$\hat{\zeta}_{k,i} = D(\aleph_{k,i})$ for all i

In (4), F_4 is product flow measurement $(kmol.h^{-1})$, P is pressure (kPa), y_{A3} is amount of in purge $(mol\ \%)$, V_L is liquid inventory $(\%\ of\ max)$. Nominal values for steady state operation of the eight states, four manipulated inputs and four outputs variables of the system are given in [24].

To evaluate the performance of the proposed setup, first we discretize the TE-PCS. By considering $m = 4$ and $n = 8$ and exploiting the Algorithm 1, the encrypted estimation of states are obtained. Fig. 2 shows the encrypted estimation of the first state i.e. $\hat{\aleph}_{k,1}$, attained from Algorithm 1 , and its associated decrypted copy i.e. $\hat{\zeta}_{k,1}$. The error between the real valued state i.e. $\bar{x}_{k,1}$ in this example, and its associated estimation from secure observer after applying the proper encryption i.e. $\hat{\zeta}_{k,1}$ is depicted in Fig. 3. As expected the latter quantity remains within a ball of an arbitrarily small radial from the former. The size of this ball depends on the accuracy of quantization.



(a) encrypted estimation of the first state.



(b) decrypted estimation of the first state.

Fig. 2. encrypted and decrypted estimation of the first state

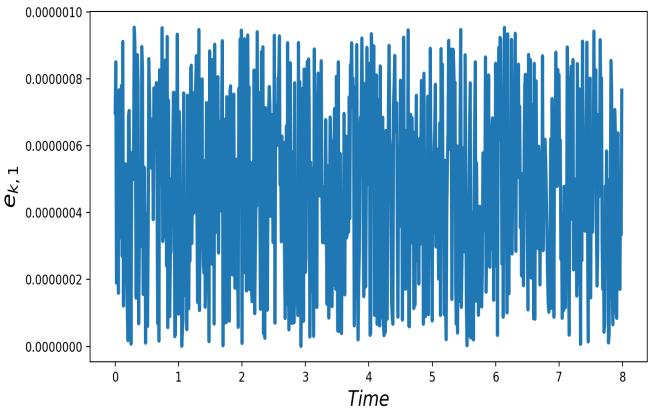


Fig. 3. The error term $\hat{\zeta}_{k,1} - \bar{x}_{k,1}$

V. Conclusions

We proposed a novel setup for secure state estimation. This suggested framework is effective for maintaining the confidentiality of observation data in a networked control environment. To this end, we exploited Paillier encryption

method to realize the encrypted observer. We also provided conditions under which the observed states from the encrypted observer remain arbitrarily close to the actual ones. A numerical example was given that supports the theoretical results.

REFERENCES

[1] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems*, vol. 35, no. 1, pp. 20–23, 2015.

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

[3] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. IEEE, 2009, pp. 911–918.

[4] ——, "Secure control against replay attacks," in *Proc Annual Allerton Conference on Communication, Control, and Computing*, 2009, pp. 911–918.

[5] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[6] R. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, Feb 2015.

[7] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110–127, 2015.

[8] M. Zamani, U. Helmke, and B. D. O. Anderson, "Zeros of networked systems with time-invariant interconnections,," *Automatica*, pp. 97–105, 2015.

[9] A. Teixeira, I. Shames, H. Sandberg, and K. Johansson, "Revealing stealthy attacks in control systems," in *Allerton Conference on Communication, Control, and Computing*, 2012, pp. 1806–1813.

[10] Y. iu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.

[12] M. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, p. 25, 2013.

[13] T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[14] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.

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

[16] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 6836–6843.

[17] S. Mishra, N. Karamchandani, P. Tabuada, and S. Diggavi, "Secure state estimation and control using multiple (insecure) observers," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE, 2014, pp. 1620–1625.

[18] A. Al-Anwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. B. Srivastava, "Proloc: resilient localization with private observers using partial homomorphic encryption," in *International Conference on Information Processing in Sensor Networks*, 2017, pp. 41–52.

[19] F. J. Gonzalez-Serrano, A. Amor-Martın, and J. Casamayon-Anton, "State estimation using an extended kalman filter with privacy-protected observed inputs," in *IEEE International Workshop on Information Forensics and Security*. IEEE, 2014, pp. 54–59.

[20] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.

[21] B. C. Juricek, D. E. Seborg, and W. E. Larimore, "Identification of the tennessee eastman challenge process with subspace methods," *Control Engineering Practice*, vol. 9, no. 12, pp. 1337–1351, 2001.

[22] N. L. Ricker, "Model predictive control of a continuous, nonlinear, two-phase reactor," *Journal of Process Control*, vol. 3, no. 2, pp. 109–123, 1993.

[23] R. Chabukswar, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 11 239–11 244, 2011.

[24] A. Termehchy and A. Afshar, "A novel design of unknown input observer for fault diagnosis in non-minimum phase systems," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 8552–8557, 2014.