

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:

Lin, Y;Farokhi, F;Shames, I;Nešić, D

Title:

Secure Networked Control Systems Design Using Semi-homomorphic Encryption

Date:

2021-01-01

Citation:

Lin, Y., Farokhi, F., Shames, I. & Nešić, D. (2021). Secure Networked Control Systems Design Using Semi-homomorphic Encryption. Ferrari, RMG (Ed.). Teixeira, AMH (Ed.). Safety, Security and Privacy for Cyber-Physical Systems, (1), 486, pp.257-285. Springer.

Persistent Link:

<https://hdl.handle.net/11343/276523>

Secure networked control systems design using semi-homomorphic encryption

Yankai Lin Farhad Farokhi Iman Shames
Dragan Nešić

Abstract

A secure and private nonlinear networked control systems (NCSs) design using semi-homomorphic encryption is studied. Static feedback controllers are used and network architectures are provided to enable control signal computation using encrypted signals directly. As a result, the security of the NCSs is further enhanced by preserving the privacy of information flowing through the whole network. Whereas in traditional encryption techniques, encrypted signals are decrypted before control computation and are encrypted again after computation for transmission. While this is highly desirable from privacy point of view, additional technical difficulties in the design and analysis of NCSs are induced compared to standard NCSs. In this paper, we provide sufficient conditions on the encryption parameters that guarantee robust stability of the NCS in the presence of disturbances in a semi-global practical sense, and discuss the trade-offs between the required computational resources, security guarantees and the closed-loop performance. The proof technique is based on Lyapunov methods.

1 Introduction

Networked control systems is an emerging technology that differs from traditional control systems. Shared communication channels are employed to transmit the sensor and actuation data instead of traditional point-to-point connections [5]. This leads to many advantages including easier installation and maintenance as well as lower cost, weight and less volume. Moreover, it allows the control of large scale and distributed systems such as power systems and irrigation networks. On the other hand, some undesirable phenomena are also induced by the use of a shared network including quantization, scheduling, packet dropouts and so on. Dealing with these issues results in extra technical difficulties in the analysis of the system. Hybrid system [11] based approaches are widely used in design and control of NCS. Such methodologies allow controller synthesis while considering of non-uniform sampling intervals and other network induced behaviour in a unified manner. Emulation based design techniques are used in [13]. Alternatively, a framework for controller design for

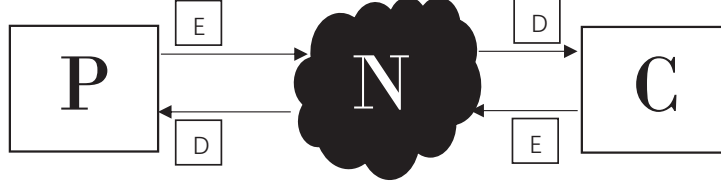


Figure 1: NCS consisting of a plant P, controller C and network N, with encryption-decryption units

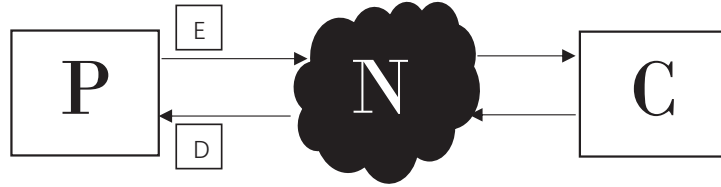


Figure 2: NCS consisting of a plant P, controller C and network N, with semi-homomorphic encryption-decryption units

NCSs based on approximate discrete-time models is proposed in [43]. Similar approaches can also be found in many other works summarised in [14].

Network security and privacy as an important issue of NCS, is not fully discussed in [14]. In the work of [40], the authors categorise different cyber-security attack scenarios into various categories based on the resources the adversary needs. Eavesdropping attack is an important class of those attacks where a malicious attacker tries to monitor the data going through the control loop to extract valuable information about the system. Thus, the integrity of data flowing through the network is compromised. Furthermore, it provides tools for the adversary to potentially launch more complex and harmful attacks such as replay attacks [27]. One possible solution to this problem is using encryption to ensure that information going through the communication channel is protected. As a result, the adversary cannot acquire any information on the system by listening to the communication channels if the encryption is done so that it works properly. Fig. 1 illustrates a typical control loop that uses such encryption-decryption scheme. Due to the prevalence of wireless NCS, data flowing through the network is the most vulnerable information that adversaries can easily access. It can be seen that, by using encryption-decryption techniques, it is difficult for eavesdroppers to access data flowing through the network, however, if the attacker has access to the controller side, the encryption scheme fails to guarantee the security and privacy of the NCS.

Following this motivation, we focus on employing homomorphic encryption schemes for NCS configured in the form of Fig. 2 that allows implementing

controllers using encrypted messages directly, therefore, preventing the curious adversary from obtaining sensitive information about the system. Homomorphic encryption is a form of encryption that allows computation on cipher-texts (encrypted data), generating an encrypted result which, when decrypted, matches the result of operations performed on the plain-texts (unencrypted data). The precise definition of homomorphic encryption will be given in Section 3. An example of such encryption methods is given in [10], where addition and multiplication of two unencrypted integers are implemented via appropriate operations on their corresponding encrypted versions. Semi-homomorphic encryption, on the other hand, only allows either summation or multiplication to be performed on cipher-texts but are easier to implement which is crucial to enable real time computations. In the earlier work by Kogiso and Fujita [20], the authors propose a method to encrypt the controller using RSA [37] and El Gamal [9] encryptions which are encryption schemes semi-homomorphic under multiplications of cipher-texts. Stability and performance guarantees of the closed-loop system using encryptions, however, are not studied thoroughly in [20]. In [8], the authors employ Paillier encryption and provide semi-global practical stability guarantees for linear time-invariant (LTI) systems without disturbances and asymptotic stability is achieved in [19] by introducing a dynamic quantizer. In [26], privacy preserving distributed projected gradient-based algorithms are proposed where both private and public key algorithms are developed, but an affine-gradient assumption is required for public key algorithms. In [3], a private cloud-based quadratic optimization algorithm is studied and the trade-off between communication complexity and privacy guarantees is discussed. Similar ideas are also applied to private distributed averaging [12], [38] and localization problems [2]. However, most of the works mentioned above focus on linear dynamics with the exception of [19] where feedback linearization is applied to achieve linear dynamics. Moreover, robust stabilization problems with modelling uncertainties and disturbances are not studied.

In this paper, we consider the problem of stabilizing a nonlinear NCS using a static controller subject to disturbances using Paillier and RSA cryptosystems which are semi-homomorphic. Paillier cryptosystem is a probabilistic public key cryptography scheme that allows addition of two cipher-texts and multiplication of a cipher-text by a plain-text while RSA encryption allows multiplications of multiple cipher-texts. This allows us to use Paillier encryption for a class of nonlinear control systems with the help of RSA encryption if necessary. In this work, we use a discrete-time model to describe the dynamics of the NCS for simplicity, as the main theme of this work is on the privacy and security of the NCS. The designer follows an emulation based approach to first design a controller for the discrete-time plant without the use of encryption and then based on the performance and stability requirements, the designer chooses the parameters of the encryption scheme. The approach can be generalized to cover systems modelled differently, for instance, using the hybrid modelling framework as shown in [13] and this would be the focus of future work.

To summarize, the main contribution of the paper is that we design privacy preserving static feedback controllers using semi-homomorphic encryption

which robustly stabilize a class of NCSs with disturbances modelled by difference equations. Different ways for implementation of an encryption-based control system in practice are presented. The stability properties are analysed in a unified framework by providing sufficient conditions on the encryption parameters for stabilization of the nonlinear closed-loop systems. Particularly, semi-global practical input-to-state stability (ISS) of the NCS under the proposed encryption schemes are established. Under new sets of assumptions, asymptotic or exponential stability of the aforementioned systems is demonstrated. The stability analysis is Lyapunov based and is different from typically-used methods in quantized control literature [23] and [24]. This is because in addition to measurement quantization, an additional source of quantization, i.e., gain matrix quantization, is also considered. This work extends our previous results [25] to the case where the system is subject to external disturbances. In addition, by imposing a homogeneity assumption on the closed-loop system, we provide less conservative sufficient conditions for the same problem. This also allows the use of dynamic quantizers under additional assumptions to provide stronger stability guarantees. Lastly, we show that, homogeneous systems results recover the linear systems results as a special case and in this manner the results in [8] are recovered.

The rest of the paper is organized as follows. Preliminaries are given in Section 2. Background material about Paillier encryption is presented in Section 3. The NCS model and the problem formulation are presented in Section 4. Controller design for stabilization of the system are given in Section 5. Results for the homogeneous are presented in Section 6 which cover results for linear systems as a special case. We illustrate the results through an example of rigid body control in Section 7. Finally, concluding remarks are given in Section 8.

2 Preliminaries and notations

Let $\mathbb{R} := (-\infty, \infty)$, $\mathbb{R}_{\geq 0} := [0, \infty)$, $\mathbb{Z}_{\geq 0} := \{0, 1, 2, 3, \dots\}$, $\mathbb{Z}_{> 0} := \{1, 2, 3, \dots\}$ and $\mathbb{Z}_n := \{0, 1, 2, 3, \dots, n-1\}$. A function $\alpha : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is of class $\mathcal{K}$ if it is continuous, zero at zero and strictly increasing, and it is of class $\mathcal{K}_{\infty}$ if, in addition, it is unbounded. A continuous function $\beta(s, t) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is of class $\mathcal{KL}$ if for each fixed $t \geq 0$, $\beta(\cdot, t)$ is of class $\mathcal{K}$, and for each fixed $s \geq 0$, $\beta(s, \cdot)$ is non-increasing and satisfies $\lim_{t \rightarrow \infty} \beta(s, t) = 0$. We let Id denote the identity function from $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 0}$, and we use $\gamma_1 \circ \gamma_2$ to denote the composition of two functions γ_1 and γ_2 which are from $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 0}$. The Euclidean norm of a vector $x \in \mathbb{R}^n$ is denoted by $|x| = \sqrt{\sum_{i=1}^n (x_i)^2}$ and its ∞ -norm is denoted by $|x|_{\infty} = \max_{1 \leq i \leq n} |x_i|$. For any function $\phi : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{R}^n$, we denote $\|\phi\| = \sup\{|\phi(k)| : k \in \mathbb{Z}_{\geq 0}\} \leq \infty$. In the case when ϕ is bounded, this is the standard l_{∞} norm. For a matrix $A \in \mathbb{R}^{n \times m}$, $\|A\|_F$ denotes its Frobenius norm and $|A| := \sup_{x \neq 0} \frac{|Ax|}{|x|}$ denotes its induced 2-norm. The scalar a_{ji} denotes the element of A in the j -th row i -th column for $j \in \{1, 2, \dots, n\}$ and $i \in \{1, 2, \dots, m\}$.

We consider a class of systems given by:

$$x^+ = F(x, u), \quad (1)$$

where $x \in \mathbb{R}^{n_x}$ are the states of the system, $F : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \rightarrow \mathbb{R}^{n_x}$ is continuous and inputs $u(\cdot)$ are functions from $\mathbb{Z}_{\geq 0}$ to $\mathbb{R}^{n_u}$. We assume that $F(0, 0) = 0$, so the origin is a fixed point of the system without inputs. We use $\phi(\cdot, x_0, u)$ to denote the trajectory of system (1) with initial state $x(0) = x_0$ and the input signal u . For simplicity, we only consider the time-invariant case, but the results can be easily generalized to time-varying systems.

Definition 1. ([17]) *System (1) is (globally) input-to-state stable if there exist $\beta \in \mathcal{KL}$ and $\sigma \in \mathcal{K}$ such that for each input $u \in l_\infty$ and each $x_0 \in \mathbb{R}^{n_x}$, it holds that:*

$$|\phi(k, x_0, u)| \leq \beta(|x_0|, k) + \sigma(\|u\|), \quad (2)$$

for each $k \in \mathbb{Z}_{\geq 0}$. If it is the case that $u(k) = 0, \forall k \in \mathbb{Z}_{\geq 0}$, and $|\phi(k, x_0)| \leq \beta(|x_0|, k)$, the origin of the system is uniformly globally asymptotically stable (UGAS). The system is uniformly globally exponentially stable (UGES) if the above holds with $\beta(s, k) = Ce^{-\rho k}$ for some $C > 0$ and $\rho > 0$. $\square$

It is worth mentioning that, by causality, the previous definition will not change if (2) is replaced by:

$$|\phi(k, x_0, u)| \leq \beta(|x_0|, k) + \sigma(\|u_{[k-1]}\|), \quad (3)$$

where $u_{[k-1]}$ denotes the truncation of u at $k - 1$.

3 Background on Paillier encryption

In this section, we formally introduce Paillier encryption and the necessary background knowledge of fixed-point operations that will enable us to apply Paillier encryption to the controller design.

3.1 Fixed-point operations

The main aim of this subsection is to provide the necessary background for signed fixed-point rational numbers represented in base 2 and introduce the mapping to transfer them to integers so that they can be encrypted via the method of Paillier. For non-negative integers $n \geq m$ with $n + m > 0$, denote the set of signed rational numbers in base 2 as $\mathbb{Q}(n, m)$. Precisely: $\mathbb{Q}(n, m) = \{b \in \mathbb{Q} : b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} b_i 2^{i-m-1}, b_i \in \{0, 1\}, \forall i \in 1, \dots, n\}$. It can be verified that this set contains all rational numbers between -2^{n-m-1} and $2^{n-m-1} - 2^{-m}$ separated from each other by the resolution of 2^{-m} . For a digital processor to use these rational numbers, it is desirable to transform these numbers to integers. To do so, we define the mapping: $f_{n,m}(b) : \mathbb{Q}(n, m) \rightarrow \mathbb{Z}_{2^n} = (2^m b) \bmod 2^n$. Moreover, the inverse mapping is defined as $\chi_{n,m}^{-1}(a) :$

$\mathbb{Z}_{2^n} \rightarrow \mathbb{Q}(n, m) = (a - 2^n \mathbb{I}_{a \geq 2^{n-1}})/2^m$, where $\mathbb{I}_p$ is the characteristic function that is 1 if the statement p is true and is 0 otherwise. Using these functions, we state some results that enable us to perform certain operations. The complete proof of these results can be found in [8].

Proposition 1. *The following statements are true:*

- i). $\chi_{n,m}^{-1}(\chi_{n,m}(b)) = b, \forall b \in \mathbb{Q}(n, m);$
- ii). $\chi_{n,m}(\chi_{n,m}^{-1}(a)) = a, \forall a \in \mathbb{Z}_{2^n}.$ □

This proposition shows that every operation performed on the set of signed fixed-point rational numbers can be transformed into an operation performed on the set of integers modulo 2^n and vice versa. The next proposition provides more detailed relationships between these operations. Whenever appropriate, a succinct notation with respect to m and n is used, e.g., $\chi_{n,m}$ and $\chi_{n,m}^{-1}$ are written as χ and χ^{-1} . The following operations on $\mathbb{Z}_{2^n}$ are defined:

Definition 2. *For $a, a^* \in \mathbb{Z}_{2^n}$:*

- i). $a \oplus^n a^* := (a + a^*) \bmod 2^n;$
- ii). $a \otimes^n a^* := aa^* \bmod 2^n.$ □

Finally, the following result is particularly useful for cases where fractional bits exist.

Proposition 2. *The following statement is true for all $b, b^* \in \mathbb{Q}(n, m)$ such that $bb^* \in \mathbb{Q}(n, m)$:*

$$\chi_{n+2m,0}(2^{2m}bb^*) = \chi_{n+2m,0}(2^mb)^{n+2m} \otimes \chi_{n+2m,0}(2^mb). \quad \square$$

3.2 Paillier encryption

In this subsection, we introduce the steps and properties of Paillier encryption. The security guarantees of the Paillier encryption rely on a standard cryptographic assumption named Decisional Composite Residuosity (DCR) [32]. The steps to implement a Paillier encryption scheme are given in Algorithm 1.

In Paillier encryption, N is the public key which is shared with all parties and is used for encryption. The pair (λ, μ) is the private key which is accessible only for entity that needs to decrypt the message. It is shown in [32] that:

$$D(E(t; r)) = t, \forall r \in \mathbb{Z}_N^*, \forall t \in \mathbb{Z}_N. \quad (4)$$

This gives the invertible relationship between cipher-texts and plain-texts.

Remark 1. *It can be seen that carrying out the aforementioned encryption scheme and conducting computation on encrypted data involves quantization of the signals and calculation using large integers. Moreover, truncating extra digits is not allowed. This is due to the fact for two cipher-texts $E(a)$ and $E(b)$, a sufficiently small $|E(a) - E(b)|$ in general does not imply a small $|a - b|$. This also reveals that the proposed encryption scheme prevents eavesdropping attacks at the cost of losing information of plain-texts available to the designer.* □

Algorithm 1 Paillier encryption

Key generation:

- 1: Select large prime numbers p and q randomly and independently of each other such that $\gcd(pq, (1-p)(1-q)) = 1$, where $\gcd(a, b)$ refers to the greatest common divisor of a and b
- 2: Compute public key $N = pq$
- 3: Calculate private key $\lambda = \text{lcm}(p-1, q-1)$ and $\mu = \lambda^{-1} \bmod N$, where $\text{lcm}(a, b)$ refers to the least common multiple of a and b

Encryption:

- 1: Select random $r \in \mathbb{Z}_N^* := \{x \in \mathbb{Z}_N \mid \gcd(x, N) = 1\}$
- 2: Construct the cipher-text of a message $t \in \mathbb{Z}_N$ as $E(t; r) = (N + 1)^{tr^N} \bmod N^2$

Decryption:

- 1: For any cipher-text $c \in \mathbb{Z}_{N^2}$, the plain-text is given by $D(c) = L(c^\lambda \bmod N^2) \mu \bmod N$, where $L(x) = (x-1)/N$
-

Before stating results of homomorphic properties of Paillier encryption, we first state the following definition:

Definition 3. *A homomorphic encryption scheme is a public-key encryption scheme for which $D(E(a) \otimes E(b)) = a \oplus b$, where $\otimes, \oplus$ are some group operations on the cipher-text and plain-text space respectively.* $\square$

If, for instance, $\oplus$ represents addition then the encryption scheme is additive homomorphic. The following proposition shows that under certain conditions Paillier encryption is additive homomorphic.

Proposition 3. *The following relationships of encrypted data hold:*

- i). $\forall r, r^* \in \mathbb{Z}_N^*$ and $\forall t, t^* \in \mathbb{Z}_N$ such that $t+t^* \in \mathbb{Z}_N$, $E(t; r)E(t^*; r^*) \bmod N^2 = E(t+t^*; rr^*)$;
- ii). $\forall r \in \mathbb{Z}_N^*$ and $\forall t, t^* \in \mathbb{Z}_N$ such that $tt^* \in \mathbb{Z}_N$, $E(t; r)^{t^*} \bmod N^2 = E(tt^*; r^{t^*})$. $\square$

These two results show that it is possible to do some calculations directly on the cipher-texts and then decrypt. However, since it is impossible to check the sign of a cipher-text, it is more difficult to implement multiplication. The following proposition shows that implementing multiplication of an integer and a cipher-text is possible using the operator defined in Definition 2.

Proposition 4. *Assume that $N > 2^n$ and $a \overset{n}{\otimes} a^* \in \mathbb{Z}_{2^n}$. Then, for any $r \in \mathbb{Z}_N^*$ and $a, a^* \in \mathbb{Z}_{2^n}$, we have $D(E(a; r)^{a^*} \bmod N^2) \bmod 2^n = a \overset{n}{\otimes} a^*$. $\square$*

Remark 2. *A necessary condition required in Proposition 4 is that the outcome of multiplication does not overflow, namely, it remains in $\mathbb{Z}_{2^n}$. Note also that,*

multiplication can only be done between two fixed-point rational numbers with given integer and fractional bits, thus, only a subset of real control gains are available for use depending on the number of bits. Since checking overflows using only cipher-texts is impossible, the designer must carefully choose the relevant parameters to ensure that all algebraic computations are closed with respect to the chosen set of fixed point rational numbers, otherwise the decrypted signals may not be the same as the original signal. $\square$

In view of Remark 2 and Proposition 2, to be able to implement the controller, the gain matrix must be restricted to the set $\mathbb{Q}(n_1, m_1)^{n_u \times n_y}$ for some appropriately chosen non-negative integers $n_1 \geq m_1$ and $n_1 + m_1 > 0$. The output from the sensor also needs to be quantized i.e. it has to be projected to the set $\mathbb{Q}(n_2, m_2)^{n_y}$ for non-negative integers $n_2 \geq m_2$ and $n_2 + m_2 > 0$.

To simplify the notations of multiplication of matrices of encrypted elements, the following matrix product is defined:

Definition 4. For a matrix $A \in \mathbb{R}^{n \times m}$, a column vector $v \in \mathbb{R}^m$ and a positive integer N , the matrix product $c = A \overset{N^2}{*} v$ is defined as:

$$c_j = \left(\prod_{i=1}^j v_i^{A_{ji}} \right) \text{mod } N^2, \quad (5)$$

for $j \in \{1, 2, \dots, n\}$. $\square$

With this background knowledge, we present the architecture of the NCS in the next section.

4 NCS architecture and problem statement

In this section we propose the mathematical model of the NCS considered in this paper and three different implementations of the NCS that can be described and analysed in a unified manner: static output feedback control, combination of basis functions, and two-server based state feedback control. We show that they fit in our general framework for stability analysis.

The plant of the NCS is given by the discrete-time system:

$$x^+ = f(x, u, w) \quad (6)$$

where $x \in \mathbb{R}^{n_x}$ is the state of the system, $u \in \mathbb{R}^{n_u}$ is the control input and $w \in \mathbb{R}^{n_w}$ is a vector representing unknown disturbances and modelling uncertainties of the plant considered respectively. The mapping $f : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_w} \rightarrow \mathbb{R}^{n_x}$ is in general nonlinear. In addition, $f(0, 0, 0) = 0$ so that the origin is a fixed point of the system when disturbance does not exist. Since only addition and multiplication (of cipher-texts and plain-texts) can be done using encrypted data, the following static feedback controller is considered in this paper:

$$u = Kg(x), \quad (7)$$

where $K \in \mathbb{R}^{n_u \times n_y}$ is the gain matrix to be designed and $g(x) : \mathbb{R}^{n_x} \rightarrow \mathbb{R}^{n_y}$ is in general a continuous nonlinear function and $g(0) = 0$.

Remark 3. *The structure of the controller may be restrictive, as dynamic controllers like PID controllers, for instance, typically seen in the industry, are not included. There are some non-trivial challenges in dealing with dynamic or observer based controllers that are beyond the scope of this paper and they will be left for future work. We refer interested readers to recent works [7] and [12] on this issue by requiring certain operations to take place over integers only and [28] which uses reset controllers.* $\square$

By substituting (7) in (6), we arrive at the following expression of the closed-loop system:

$$x^+ = f(x, Kg(x), w). \quad (8)$$

The main objective of this study is to implement the controller of the form (7) using Paillier encryptions to achieve some desired closed-loop stability properties that will be specified later.

In view of Remark 1, we make the following standing assumption throughout the paper:

Assumption 1. *The control computation (7) is error free.* $\square$

Following the discussion in Remark 1, errors in cipher-texts may possibly result in unpredictable errors in the corresponding plain-texts. This issue should be addressed by properly designing the communication networks to ensure high quality transmission, via parity code, for instance. If such an error occurs, it can be regarded as a disturbance signal with short durations acting on the system. Provided that the duration is not long enough, one would expect the desired properties of the closed-loop system to be preserved. For simplicity of the stability analysis, we make the above assumption to eliminate the effect of such errors.

As mentioned in the previous part of the paper, Paillier encryption can only be applied to non-negative integers. As a result, for a real valued signal, we first truncate it to fixed-point rational numbers and then lift it to non-negative integers via χ defined in Section 3, so that it can be encrypted. Meanwhile, we must also ensure that overflow and underflow do not occur in algorithmic operations by choosing the public key length sufficiently large. We follow an emulation based approach where the designer first designs a gain matrix $K \in \mathbb{R}^{n_u \times n_y}$ that globally stabilizes the system (8) and then adjusts the gain matrix to get $\bar{K} \in \mathbb{R}^{n_u \times n_y}$ that have fixed-point rational elements only. To do so, we introduce non-negative integers m_1 , n_1 , m_2 and n_2 and perform the following operations on K and $g(x)$:

$$\bar{K} = \arg \min_{T \in \mathbb{Q}(n_1, m_1)^{n_u \times n_y}} \|T - K\|_F, \quad (9)$$

$$\bar{g}(x) = \arg \min_{z \in \mathbb{Q}(n_2, m_2)^{n_y}} |z - g(x)|. \quad (10)$$

Thus, with some abuse of notations, the closed-loop system using encrypted signals can be written in the following form:

$$x^+ = f(x, \chi_2(\mathbf{D}(\chi_1(\bar{K}) \overset{N^2}{*} \mathbf{E}(\chi_1(\bar{g}(x))))), w), \quad (11)$$

where the operators $\mathbf{E}$ and $\mathbf{D}$ here work element wise. The function χ_1 converts fixed-point rational numbers to integers while χ_2 does the opposite and the operation $\overset{N^2}{*}$ is defined in Definition 4.

The following assumption is important to characterize the errors induced by the truncation/quantization process defined by $e_1 = \|\bar{K} - K\|_F$ and $e_2 = |\bar{g}(x) - g(x)|$ and the compact set $\mathbb{B}_\Delta = \{x \in \mathbb{R}^{n_x} : |x| \leq \Delta\}$ the system is supposed to operate in.

Assumption 2. For any $\epsilon_1, \epsilon_2, \bar{\Delta} > 0$, there exist n_1, m_1, n_2 and m_2 sufficiently large, such that $e_1 \leq \epsilon_1$, $e_2 \leq \epsilon_2$, $\bar{K} \in \mathbb{Q}(n_1, m_1)^{n_u \times n_y}$ and $\bar{g}(x) \in \mathbb{Q}(n_2, m_2)^{n_y}, \forall x \in \mathbb{B}_\Delta$. $\square$

In the following, three examples that satisfy the above assumption are given.

4.1 Static output feedback

This is the simplest structure that fits the model (6) and (7), where the function $g(x)$ represents the output function and a proportional type controller is used to stabilize the plant. If $g(x) = x$ then it becomes the standard state feedback controller. In this situation, the truncation process takes place on the signal $g(x)$ directly.

Then we have the following lemmas:

Lemma 1. For any $\epsilon_1, \epsilon_2 > 0$, if m_1, m_2, n_u and n_y are such that $m_1 \geq -\log_2(\epsilon_1/\sqrt{n_u n_y}) - 1$ and $m_2 \geq -\log_2(\epsilon_2/\sqrt{n_u n_y}) - 1$, then $e_1 \leq \epsilon_1$ and $e_2 \leq \epsilon_2$. $\square$

Proof. It can be verified that $2^{-m_1+1} \leq \epsilon_1/\sqrt{n_u n_y}$. Thus, we have:

$$e_1 = \sqrt{\sum_{i=1, j=1}^{n_u, n_y} (K_{ij} - \bar{K}_{ij})^2} \leq \sqrt{\sum_{i=1}^{n_u n_y} 2^{-2m_1-2}} \leq \epsilon_1.$$

By following similar steps one can also show that $e_2 \leq \epsilon_2$ holds under the given assumption. $\square$

Lemma 2. For any $\bar{\Delta} > 0$, if m_1, m_2, n_1, n_2, n_u and n_y are such that $n_1 \geq m_1 + 1 + \log_2(\max_{i,j} |K_{ij}|)$ and $n_2 \geq m_2 + 1 + \log_2(\max_{0 \leq |x| \leq \bar{\Delta}} |g(x)|_\infty)$, then $\bar{K} \in \mathbb{Q}(n_1, m_1)^{n_u \times n_y}$ and $\bar{g}(x) \in \mathbb{Q}(n_2, m_2)^{n_y}, \forall x \in \mathbb{B}_{\bar{\Delta}}$. $\square$

Proof. It can be proved by noting that $2^{n_1-m_1-1} \geq \max_{i,j} |K_{ij}|$ and $2^{n_2-m_2-1} \geq \max_{0 \leq |x| \leq \bar{\Delta}} |g(x)|_\infty$. $\square$

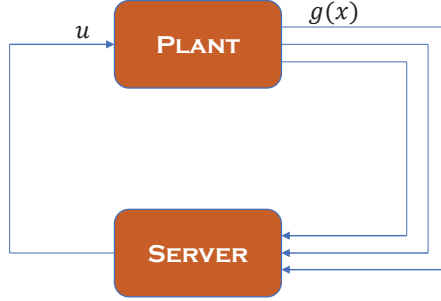


Figure 3: NCS loop with multiple channels

4.2 Combination of basis functions

In this subsection, we consider the structure shown in Fig. 3. At the plant side, we have sensors capable of performing operations directly to generate functions which we call basis functions. One typical example for this situation is optimization algorithms over the cloud where the agent (plant) sends gradient information rather than the state x over the network. Another example is where multiple elementary functions are used as basis functions to approximate a desired nonlinear function that may be hard to realize due to computational constraints. This is common in engineering designs, for instance, when the principles of reinforcement learning are applied to adaptive and optimal control problems [22, 15]. A set of linearly independent smooth basis functions are normally used to approximate the cost function and the control policy in policy iteration of an optimal control problem. Problems in distributed averaging can also be put in this form where the basis functions are the states of the agents and the linear combination depends on the choice of the weights over the connection graph. A particular interesting problem in this set up is the potential information leakage between nodes/plants after decryption. This happens when the control input is decrypted at one particular node. If the plant knows the control law, it can infer the state of another node based on its own state information. Detailed discussion of this issue is presented in a recent paper [38]. The proposed encryption-based control law, however, can still be captured by (7).

It is not hard to see that Lemma 1 and Lemma 2 also hold in this setting.

4.3 Two-server structure with state measurement only

The most general case considered in this paper is shown in Fig. 4. At the plant side sensors are only capable of providing state measurements x , but not able to perform any computations. Since under Paillier encryption the most we can do is addition and multiplication, we introduce two independent non-colluding servers that make use of the continuity of $g(x)$ and another multiplicative homomorphic

cryptosystem to realize the controller (7). In this set up, we use a polynomial function $\tilde{g}(x)$ to approximate the function $g(x)$ and then apply RSA encryption to perform polynomial calculations¹. The sensor at the plant side first encrypts the state measurement x using RSA encryption to Server 1, and Server 1 calculates powers of x using cipher-texts directly and then returns it to the plant side. Then Paillier encryption is applied to extract $\tilde{g}(x)$ as an approximation of $g(x)$ in the same way as done in Section 4.1 and operations in cipher-texts are executed by Server 2. For $x = [x_1 \ x_2 \ \dots \ x_{n_x}]^T \in \mathbb{R}^{n_x}$, let $a = [a_1 \ a_2 \ \dots \ a_n]^T$ be an n_x -tuple of non-negative integers and define $x^a := x_1^{a_1} \cdot x_2^{a_2} \cdots x_{n_x}^{a_{n_x}}$. From the Weierstrass approximation theorem [35], for any $\bar{\Delta}, \varepsilon_1 > 0$, there exists $M > 0$ such that $\sum_{i=1}^{n_x} a_i \leq M$ for all a and:

$$|\tilde{g}(x) - g(x)| \leq \varepsilon_1, \ \forall x \in \mathbb{B}_{\bar{\Delta}}, \quad (12)$$

where each element of $\tilde{g}(x)$ is given by the sum over a finite number of n_x -tuples: $\sum_a c_a x^a$ where c_a are real coefficients that will be embedded in the matrix K .

In addition to the use of polynomial basis function as a way of approximation, polynomial feedback is also used in other situations due to the development in sum of squares (SOS) programs [34]. Since then, there have been many results in the literature on controller synthesis for nonlinear systems based on SOS approaches. See, for example [36], [16], [44], [6] and [4] on the applications of polynomial feedback controllers for different problems.

In order to apply RSA encryption, the state measurement x has to go through the same truncation-lifting process to get a fixed-point rational number $\tilde{x}$. Due to uniform continuity of $\tilde{g}(x)$ over $\mathbb{B}_{\bar{\Delta}}$, for any $\varepsilon_2 > 0$, $|\tilde{g}(x) - \tilde{g}(\tilde{x})| \leq \varepsilon_2$ can be satisfied if the truncation error $|x - \tilde{x}|$ is small enough. If it is the case that $\varepsilon_1 + \varepsilon_2 \leq \epsilon_2$, it can be verified that Assumption 2 is satisfied since the argument regarding ϵ_1 in Lemma 1 and Lemma 2 still hold in this setting. This two-server architecture covers the case of feedback linearization discussed in [19].

5 Main result

In this section, we state the main result of this work providing sufficient conditions on the parameters including m_1 , n_1 , m_2 and n_2 to guarantee certain stability properties. We also show that large m_1 and m_2 lead to better closed-loop performance but requires more computational resources, similarly large n_2 results in a larger region of attraction of the origin.

5.1 Robust stabilization

In this part we will show that if the controller (7) renders the closed-loop system (8) ISS with respect to w , then the controller described by Algorithm 2

¹El Gamal encryption is also multiplicative homomorphic however RSA encryption also works on $\mathbb{Z}_N$ while El Gamal encryption works only on a subset of $\mathbb{Z}_N$ [20], for simplicity we consider RSA encryption here only, but the analysis can be extended to cover the case where El Gamal encryption is used.

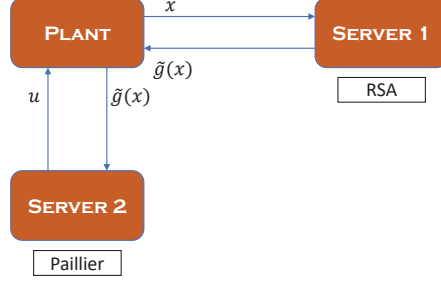


Figure 4: NCS loop with two servers

also inherits a robustness property weaker than ISS. In particular, if (8) is ISS with respect to w , the state remains bounded for any bounded w , however, the controller in Algorithm 2 only gives bounded state when the l_∞ norm of the disturbance is bounded by a known constant. Moreover, it will be shown that the more computational resources we have, the larger the upper bound of the disturbance can be made.

To state the main result, we make the following assumptions:

Assumption 3. *There exists an ISS Lyapunov function $V : \mathbb{R}^{n_x} \rightarrow \mathbb{R}_{\geq 0}$ for system (8), such that the following inequalities hold for any $C > 0$ and some $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{K}_\infty, \gamma \in \mathcal{K}$:*

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|), \quad (13)$$

$$V(f(x, Kg(x), w)) - V(x) \leq -\alpha_3(|x|) + \gamma(|w|), \quad (14)$$

for any $x \in \mathbb{R}^{n_x}$,

$$|V(x_1) - V(x_2)| \leq L_v |x_1 - x_2|, \quad (15)$$

for any $\max\{|x_1|, |x_2|\} \leq C$, where L_v is the Lipschitz constant of V that may depend on C . $\square$

If a globally Lipschitz V can be found, then L_v is independent of C .

Assumption 4. *The function f is continuous on $\mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_w}$. Moreover, for every compact set $S \subset \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_w}$, there exists $L_f > 0$ such that $|f(x, u_1, w) - f(x, u_2, w)| \leq L_f |u_1 - u_2|$, for all (x, u_1, w) and $(x, u_2, w) \in S$. $\square$*

Remark 4. *Assumption 3 is a necessary and sufficient condition for the closed-loop system (8) to be ISS with respect to w if f is continuous, as shown by Theorem 1 of [17]. Besides, in [17], the existence of a smooth ISS Lyapunov function is also proved and the ISS-gain function $\sigma(s)$ in Definition 1 is given by $\alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ (Id + \rho) \circ \gamma(s)$, where ρ is any $\mathcal{K}_\infty$ function such that $Id - \rho \in \mathcal{K}_\infty$. This is a stronger property than the Lipschitzness assumed in Assumption 3. However, such a Lyapunov function may be very hard to find*

since it typically requires the solution of the corresponding difference equation whereas finding a non-smooth but Lipschitz Lyapunov function may be easier. In fact, a continuous Lyapunov function implies certain robustness of the closed-loop system which is discussed in detail in [18]. If the above conditions only hold locally or a compact set rather than the origin is to be stabilized, one can obtain a similar result using the same approach. $\square$

The control designer can follow the steps given by Algorithm 1 to implement the control law using the uniform quantizations in (9) and (10), which is the main factor that may adversely impact the control performance. As mentioned in the introduction part, this is slightly different from the scenario considered in the quantized control literature [23] and [24]. Namely, the above papers only consider quantized measurement or quantized input. However, in our case, in addition to measurement quantization, the gain matrix K also needs to be quantized. This is the reason why we take a different approach compared to [23] and [24].

In the presence of disturbances, we have the following result for the closed-loop system (11) using the controller described in Algorithm 2:

Algorithm 2 Secure and private implementation of the static controller with encrypted measurements

Require: $n_1, m_1, n_2, m_2, \bar{K}, \bar{g}(x), p, q$

Ensure: u

- 1: Set $n \leftarrow n_y + n_1 + n_2 - 1$, $m \leftarrow m_1 + m_2$ and $\bar{y} \leftarrow \bar{g}(x)$
 - 2: # Control Designer
 - 3: Construct $\Gamma_{ji} \leftarrow \chi_{n+2m,0}(2^m \bar{K}_{ji})$
 - 4: # Sensors
 - 5: **for** $i = 1, \dots, n_y$ **do**
 - 6: Transmit $z_i \leftarrow E(\chi_{n+2m,0}(2^m \bar{y}_i); r)$ to the controller
 - 7: **end for**
 - 8: # Controller
 - 9: Construct $l = \Gamma \overset{N^2}{*} z$
 - 10: Transmit l_j to the actuators
 - 11: # Actuators
 - 12: **for** $j = 1, \dots, n_u$ **do**
 - 13: Implement $u_j \leftarrow D(l_j) \bmod 2^{n+2m} / 2^{2m}$
 - 14: **end for**
-

Theorem 1. Suppose there exists $K \in \mathbb{R}^{n_u \times n_y}$ such that Assumptions 1-4 hold. Then, there exists $\beta \in \mathcal{KL}$ such that for any $\delta, \Delta > 0$, disturbances upper bounded by the constant $\Delta_w > 0$ and design parameters $0 < \mu_1 < 1$ and $0 < \mu_2 < 1$, one can choose $N > 2^{n_y+n_1+n_2-1}$, $\epsilon_1 = \frac{(1-\mu_1)\alpha_3(\delta_x)}{M_1 L_V L_f}$, $\epsilon_2 = \frac{\mu_1(1-\mu_2)\alpha_3(\delta_x)}{L_V L_f |K|}$ and $\bar{\Delta} = \max\{\Delta, \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\eta + \gamma(\Delta_w)), \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \mu_1^{-1} \mu_2^{-1} \rho^{-1}(\gamma(\Delta_w))\}$ to guarantee that any solution $\phi(\cdot, x, w)$ to (11) satisfies:

$$|\phi(k, x_0, w)| \leq \beta(|x_0|, k) + \sigma(\|w\|) + \delta, \quad (16)$$

for any $|x_0| \leq \Delta$, where:

- δ_x is chosen to satisfy $\delta = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\frac{M_2(1-\mu_1)\alpha_3(\delta_x)}{M_1} + \mu_1(1 - \mu_2)\alpha_3(\delta_x))$,
- ρ is any $\mathcal{K}_\infty$ function such that $Id - \rho \in \mathcal{K}_\infty$,
- $\sigma(s) = \max\{\sigma_1, \sigma_2\}$ with $\sigma_1(s) = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \mu_1^{-1} \mu_2^{-1}(Id + \rho) \circ \gamma(s)$,
 $\sigma_2(s) = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ (Id + \rho) \circ \gamma(2s)$.

The functions $\alpha_1, \alpha_2, \alpha_3$ come from Assumption 3, $M_1 = \max_{\delta_x \leq |x| \leq \Delta} |g(x)|$, $M_2 = \max_{0 \leq |x| \leq \delta_x} |g(x)|$. $\square$

Proof. The proof is given in the Appendix. $\square$

Remark 5. Assumption 2 requires the two errors to be small and can be met by selecting the design parameters appropriately based on Lemma 1 and Lemma 2 and the discussion in Section 4.3. $\square$

The above theorem shows that the closed-loop system exhibits semi-global input-to-state practical stability namely, the upper bound of the disturbance can be arbitrary, the norm of the initial state can be from an arbitrarily large set and δ can be chosen arbitrarily small. This is very similar to the regional input-to-state practical stability discussed in [21], and the bound on the disturbance is used to establish the existence of robustly positively invariant set as shown in Definition 2.1 of [21]. One can follow the conditions listed in Theorem 1 to select large enough integers such that Assumption 2 holds to implement Algorithm 1. The tuning parameters μ_1 and μ_2 characterize the approximation errors of the gain matrix and measurement respectively, larger (smaller) values lead to more (less) accurate approximations.

Remark 6. In order to break the Paillier encryption scheme, the potential attacker needs to figure out the z_i and l_j in Algorithm 1. However, this is numerically intractable under Decisional Composite Residuosity assumption if the key length is chosen to be large enough. See [32] and [26] for more details on semantic security analysis of the Paillier encryption scheme. However, RSA encryption is not semantically secure. Consequently, if polynomial feedback is used, Server 1 in Fig. 4.3 must operate in a secure way. Alternatively, El Gamal encryption can be used to perform multiplications. $\square$

Remark 7. There is a trade-off between the performance of the system and the required resources. Large m and N are required to ensure a large domain of attraction and a small neighbourhood around the origin to which the state converges to, when the system is disturbance free. In addition, when the system is subject to disturbances, larger m leads to larger μ_1 and μ_2 , therefore, smaller ISS gain function from w to x and smaller δ . This further results in a positively larger bound on the disturbance while still guaranteeing boundedness of the closed-loop trajectory of (11). On the other hand, larger n and N improves the bound of disturbances by ensuring a larger Δ . However, this also increases the

computational cost of the encryption and decryption algorithm. Note that each multiplication in Algorithm 1 costs $\mathcal{O}(N^2)$ operations and each exponentiation costs $\mathcal{O}(N^3)$ operations. If n_u and n_y are independent of N , the overall computational complexity scales with $\mathcal{O}(N^3)$. Moreover, instead of sending packets of length $\mathcal{O}(n)$, in Algorithm 1, the communication involves sending packets of length $\mathcal{O}(N)$, and N grows exponentially as n increases. This exponential growth of computational and communication burden may induce delays that may not be ignored in the modelling of the system and requires high data rate. This can be interpreted as the cost of achieving security and privacy of the NCS. $\square$

5.2 Disturbance free case

In this case $w \equiv 0$, and the closed-loop NCS (8) can be written as:

$$x^+ = f(x, Kg(x), 0). \quad (17)$$

Like the previous case, the control designer also follows the steps given by Algorithm 1 to implement the control law. For simplicity, we use the symbols $\tilde{E}$ and $\tilde{D}$ to include the fixed-point rational number and integer conversions done in Algorithm 2 and the corresponding closed-loop system is given by:

$$x^+ = f(x, \tilde{D}(\bar{K} \overset{N^2}{*} \tilde{E}(\bar{g}(x))), 0). \quad (18)$$

The following result is the special case of Theorem 1 when $w \equiv 0$ and the main result of [25].

Corollary 1. *Suppose there exists $K \in \mathbb{R}^{n_u \times n_y}$ such that Assumptions 1-4 hold with $w = 0$. Then, there exists $\beta \in \mathcal{KL}$ such that for any $\delta, \Delta > 0$ and design parameters $0 < \mu_1 < 1$ and $0 < \mu_2 < 1$, one can choose $N > 2^{n_y+n_1+n_2-1}$, $\epsilon_1 = \frac{(1-\mu_1)\alpha_3(\delta_x)}{M_1 L_V L_f}$, $\epsilon_2 = \frac{\mu_1(1-\mu_2)\alpha_3(\delta_x)}{L_V L_f |K|}$ and $\bar{\Delta} = \Delta$ to guarantee that any solution $\phi(\cdot, x, w)$ to (18) satisfies:*

$$|\phi(k, x_0)| \leq \beta(|x_0|, k) + \delta, \quad (19)$$

for any $|x_0| \leq \Delta$, where

- δ_x is chosen to satisfy $\delta = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\frac{M_2(1-\mu_1)\alpha_3(\delta_x)}{M_1}) + \mu_1(1 - \mu_2)\alpha_3(\delta_x)$,
- ρ is any $\mathcal{K}_\infty$ function such that $Id - \rho \in \mathcal{K}_\infty$.

The functions $\alpha_1, \alpha_2, \alpha_3$ come from Assumption 3, $M_1 = \max_{\delta_x \leq |x| \leq \bar{\Delta}} |g(x)|$, $M_2 = \max_{0 \leq |x| \leq \delta_x} |g(x)|$. $\square$

Proof. The proof is a special case of the proof of Theorem 1 and is omitted. $\square$

This result shows semi-global practical stability of the closed-loop system (17) which means that for any set of initial conditions of the form $\{x_0 \in \mathbb{R}^{n_x} : |x_0| \leq \Delta\}$ where $\Delta > 0$ can be arbitrarily large and for any arbitrarily small δ , one can select large enough integers according to Assumption 2 and Corollary 1 to implement Algorithm 1 and ensure that (19) holds.

5.3 Security enhancement

In this subsection, we provide a brief analysis on the resilience of the proposed encryption based control strategy against replay attacks. Replay attack [27] refers to the situation where an attacker wishes to disrupt the operation of a control system in steady state without being detected. The attacker will hijack the sensors, observe and record their readings for a certain amount of time and repeat them afterwards while carrying out the attack. In [27], the authors propose a watermarking based scheme for discrete-time LTI systems controlled by an infinite horizon Linear Quadratic Gaussian (LQG) controller. The idea is to add a zero mean Gaussian noise to the original input from LQG design. As a result, even when the system is operated in steady state, the control input at different time instances will be different with probability one. This makes it hard for the attacker to remain stealthy at the cost of losing some performance in the LQG sense. Recall the detailed steps of Paillier encryption given in Section 3.2, for an appropriately chosen N based on Theorem 1, at each time instance a random $r \in \mathbb{Z}_N^*$ must be selected and this randomness is useful in replay attack detection as shown in the following proposition. For notational convenience, a replay attack in which the number of consecutive recordings and repeats is no more than M is called an M -step replay attack. In particular, we restrict our attention to replay attacks that only record and replay the data without any other attempts to remain stealthy. Similarly, an M -step detector refers to the detector that collect and keep the received (encrypted) measurements for M consecutive steps. The defender is using the following criterion to perform replay attack detection:

1. The M -step detector collects M consecutive measurements, when a new measurement arrives the oldest one is discarded.
2. The detector records the number of repeated measurements in the M collected ones. If a sequence of measurements with length more than 1 is repeated, an alarm is triggered to indicate the presence of the replay attack.

Proposition 5. *Given the public key N , assume at each time instance, r is drawn from elements of $\mathbb{Z}_N^*$ with equal probability independently from other time instances. Then an M_a -step replay attack can be detected by an M_d -step detector with a false alarm rate no larger than $\frac{1}{(N-3)}$ if $M_d > M_a + 1$. $\square$*

Proof. By the definition of $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$, it can be seen that 1, p and q are the only 3 elements in $\mathbb{Z}_N$ that are not in $\mathbb{Z}_N^*$. As a result, r is drawn from elements of $\mathbb{Z}_N^*$ with equal probability $P = \frac{1}{N-3}$. It is shown by Lemma 3 in [32] that the integer-valued encryption function $E(t; r)$ from $\mathbb{Z}_N \times \mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$ is bijective. As a result, for the same unencrypted measurement $t \in \mathbb{Z}_N$, the corresponding cipher-text will be different if r is chosen differently and each possible cipher-text is generated with the same probability $P = \frac{1}{N-3}$. Moreover, the fact that $M_d > M_a + 1$ allows the detector to collect at least 2 consecutive repeated measurements replayed by the attacker together with the measurements collected

by the attacker to launch the attack. Due to independent selection at each time instance, if the system is at steady state and there is no disturbance, the probability of receiving a sequence of repeated measurements of length M without a replay attack is given by $\frac{1}{(N-3)^M}$ which makes the worst case false alarm rate $\frac{1}{(N-3)}$ (corresponding to the case of 2 consecutive identical measurements). If this is not the case the probability can only be smaller than $\frac{1}{(N-3)}$. To see this, for $t_1 \neq t_2 \in \mathbb{Z}_N$, if there exist $r_1 \neq r_2 \in \mathbb{Z}_N^*$ such that $E(t_1; r_1) = E(t_2; r_2)$, $E(t_1; r_1) = E(t_2; r_2)$ can only happen with probability $\frac{1}{(N-3)}$ since the cardinality of $\mathbb{Z}_N^*$ remains the same. If for $t_1 \neq t_2 \in \mathbb{Z}_N$, there exist no $r_1 \neq r_2 \in \mathbb{Z}_N^*$ such that $E(t_1; r_1) = E(t_2; r_2)$, the false alarm rate becomes 0. Thus the proof is complete. $\square$

Remark 8. *In fact, the requirement of selecting r from $\mathbb{Z}_{N^2}^*$ with equal probability is not necessary. However, if this is the case, the false alarm rate will be given by P_{max} , where P_{max} denotes the largest probability of one particular element getting selected which is no smaller than $\frac{1}{N-3}$. In other words, the selection rule in Proposition 5 gives the detector with the smallest upper bound of the false alarm rate estimate, provided that the detector has more memory than the attacker according to $M_d > M_a + 1$. Moreover, it is also possible to relax the condition $M_d > M_a + 1$ to $M_d > M_a$ by checking whether there is any element appearing more than once. But this will result in a false alarm rate that grows to 1 as M_a increases. In applications N is often chosen to be very large, the probability of receiving repeated measurements is extremely low. Thus, it is possible to detect potential replay attacks by checking the consistency of the encrypted measurements received with very low false alarm rate. However, the result above is stated for replay attacks that record and replay only. If the attacker is more intelligent and has access to the public key N the attacker can encrypt 0 and multiply it by the recorded data (equivalent to adding 0 to the plain-text in view of Proposition 3) to generate a different random cipher-text and remain stealthy. In this case, encryption may not give this resilience for free and other results [27] should be used to prevent these more intelligent replay attacks.* $\square$

For other attacks that require data injection to be stealthy, it is shown in [40] that, it is necessary to properly design the attack policy. However, this can not be done without breaking the Paillier encryption scheme which makes our proposed scheme resilient against these type of attacks.

6 Homogeneous control systems

In this section, we show that if more information about the system dynamics is available to the designer, the results in Theorem 1 and Corollary 1 can be improved and made less conservative. Namely, we show that if the controller can render the closed-loop system homogeneous with degree zero, the expressions

for n_1 , n_2 , m_1 and m_2 will be simplified. If in addition, the quantizers have infinite ranges, then global practical stability can be established.

Consider the following autonomous discrete-time nonlinear system:

$$x^+ = G(x), \quad (20)$$

where $G : \mathbb{R}^{n_x} \rightarrow \mathbb{R}^{n_x}$ is the jump map that satisfies $G(0) = 0$. A homogeneous system is defined as follows:

Definition 5. *System (20) is homogeneous (with degree zero) if given any real number $\lambda > 0$, we have $G(\lambda x) = \lambda G(x)$ for all $x \in \mathbb{R}^{n_x}$.* $\square$

Remark 9. *The definition of homogeneity considered in this paper is a simplified version compared to the work [42], where the authors consider a much more generalised version of dilations and cover Definition 5 as a special case. Based on the homogeneity assumption and regularity on the jump map function of the difference inclusion, the existence of a Lyapunov function that has certain nice properties are guaranteed and local stability is proved to imply global stability.* $\square$

The following lemma states equivalent properties for homogeneous systems:

Lemma 3. *Assume G is continuous on $\mathbb{R}^{n_x}$ and the system (20) is homogeneous (of degree zero) in the sense of Definition 5 and the origin of (20) is (uniformly) locally asymptotically stable, then:*

- i). *The origin of (20) is (uniformly) globally exponentially stable.*
- ii). *There exists a continuous function $V : \mathbb{R}^{n_x} \rightarrow \mathbb{R}_{\geq 0}$ that is smooth on $\mathbb{R}^{n_x} \setminus \{0\}$ and positive constants c_1 , c_2 , c_3 and L such that:*

$$c_1|x| \leq V(x) \leq c_2|x|, \quad (21)$$

$$V(G(x)) - V(x) \leq -c_3|x|, \quad (22)$$

$$|V(x+v) - V(x)| \leq L|v|, \quad (23)$$

$$\forall x, v \text{ such that } x \neq 0 \text{ and } x+v \neq 0. \quad \square$$

Proof. This is a special case of Theorem 1 of [31] and is thus omitted. $\square$

By imposing another assumption on the closed-loop system (8), it is possible to state stability results when the closed-loop system is affected by disturbances:

Assumption 5. *The function f is continuous and satisfies $|f(x, u_1, w_1) - f(x, u_2, w_2)| \leq L_f|u_1 - u_2| + L_w|w_1 - w_2|$ globally on $\mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_w}$.* $\square$

Theorem 2. *If Assumption 2 and Assumption 5 hold. And suppose there exists $K \in \mathbb{R}^{n_u \times n_u}$ such that Assumption 4 holds globally for the closed-loop system (17) and $|g(x)|$ is upper bounded by $\kappa|x|$ for some $\kappa > 0$. Moreover, if the controller (7) renders the disturbance free closed-loop system (17) homogeneous and asymptotically stabilises the origin of (17), then for any δ , $\Delta > 0$,*

disturbances upper bounded by the constant $\Delta_w > 0$ and design parameters $0 < \mu_1 < 1$ and $0 < \mu_2 < 1$, one can choose $N > 2^{n_y+n_1+n_2-1}$, $\epsilon_1 = \frac{c_3(1-\mu_1)}{\kappa LL_f}$, $\epsilon_2 = \frac{\mu_1(1-\mu_2)c_3\delta_x}{LL_f|K|}$ and $\bar{\Delta} = \max\left\{\Delta, \frac{c_2(\eta+LL_w\Delta_w)}{c_1c_3\rho}, \frac{c_2LL_w\Delta_w}{c_1c_3\mu_1\mu_2\rho}\right\}$ to guarantee that any solution $\phi(\cdot, x, w)$ to (11) satisfies:

$$|\phi(k, x_0, w)| \leq \frac{c_2}{c_1}|x_0|\left(1 - \frac{\mu_1\mu_2c_3}{c_2}\right)^k + \sigma||w|| + \delta, \quad (24)$$

for any $|x_0| \leq \Delta$, where δ_x is chosen to satisfy $\delta = \frac{c_2\mu_1(1-\mu_2)\delta_x}{c_1\rho}$, ρ is any constant such that $0 < \rho < 1$ and $\sigma = \frac{c_2LL_w}{c_1c_3\mu_1\mu_2}$. The positive constants c_1, c_2 and c_3 come from Lemma 3. $\square$

Proof. The proof can be found in the Appendix. $\square$

The results in the previous two propositions show that if the controller renders the closed-loop homogeneous and $g(x)$ is linearly bounded, then for any gain matrix K , there exists $\bar{K}$ sufficiently close to K such that the desired stability properties of the quantization free system are preserved under gain matrix quantization. This also covers the result in [8] and [25] as a special case. where a static state feedback controller is used to control a discrete-time LTI system. An immediate conclusion is that if all of the assumptions mentioned in Theorem 2 hold and the quantizer of the function $g(x)$ has infinite range, then system (18) can be globally practically stabilised. Even if this is not the case, the choice of n_1 and m_1 will no longer depend on δ . Moreover, using the Lipschitzness of the Lyapunov function, it is possible to show that the closed-loop system is ISS with respect to actuator errors. Thus, this problem reduces to the discrete-time counterpart of the cases shown in [23] and [24]. However, what is slightly different from the problem setting in [23] and [24] is that, in [23] and [24] it is required that saturation can be detected from quantized measurements. However, as discussed in Remark 2, it is impossible to satisfy the saturation detection assumption in [23] and [24]. As a result, in order to use dynamic quantizer to achieve ISS (UGAS) of the closed-loop system when there are (no) disturbances, it is required that, prior to the encryption of the state measurements, saturation of the quantizer can be detected and zoom-out² is triggered if saturation is detected. Such implementation is proposed in [1], where the rule to update the zoom variable is done in a closed-loop fashion: the information of the measurement is used to ensure that saturation is avoided before transmission. Since the technical details of dynamic quantization overlap a lot with the continuous version presented in [24] and [1], we choose not to present them in this work and refer the interested readers to [24] and [1].

7 An Illustrative example

In this part, we consider the following example of attitude control of a rigid body using three inputs from [36]. The complete attitude dynamics are given

²See [23] for an explanation of zoom-out.

by:

$$\begin{aligned}\dot{\omega} &= J^{-1}S(\omega)J\omega + J^{-1}u \\ \dot{\psi} &= H(\psi)w\end{aligned}\tag{25}$$

with $\omega \in \mathbb{R}^3$ the angular velocity vector in a body-fixed frame, $\psi \in \mathbb{R}^3$ the Rodrigues parameter vector and $u \in \mathbb{R}^3$ the control input. The positive definite inertia matrix J is equal to $\text{diag}(4, 2, 1)$ in this example while $S(\omega)$ and $H(\psi)$ are given by:

$$S(\omega) = \begin{bmatrix} 0 & \omega_3 & -\omega_2 \\ -\omega_3 & 0 & \omega_1 \\ \omega_2 & -\omega_1 & 0 \end{bmatrix}$$

$$H(\psi) = \frac{1}{2}(I - S(\psi) + \psi\psi^T),$$

where I denotes the 3×3 identity matrix. And the designed controller in [36] is given by:

$$\begin{aligned}u_1(\omega, \psi) &= -0.49\psi_1^3 - 0.86\omega_1^3 - 1.2\omega_1\psi_1^2 - 1.5\omega_1\psi_2^2 \\ &\quad - 1.1\omega_1\psi_3^2 + 0.37\omega_1^2\psi_1 - 2.6\omega_1 - 0.77\psi_1 \\ &\quad + 0.035\omega_2\psi_1\psi_2 \\ u_2(\omega, \psi) &= -0.28\psi_2^3 - 0.29\omega_2^3 - 0.27\omega_2\psi_1^2 + 0.17\omega_2^2\psi_2 \\ &\quad - 0.37\psi_1^2\psi_2 - 0.69\omega_2\psi_2^2 - 1.1\omega_2\psi_3^2 \\ &\quad - 0.45\psi_2\psi_3^2 - 1.1\omega_1^2\omega_2 - 0.44\omega_1\psi_1\psi_2 \\ &\quad - 0.46\psi_2 - 1.1\omega_2 + 0.24\omega_1\omega_2\psi_1 \\ u_3(\omega, \psi) &= -0.14\psi_3^3 - 0.18\omega_3^3 - 0.44\omega_1^2\omega_3 - 0.34\omega_2^2\omega_3 \\ &\quad - 0.55\omega_3\psi_2^2 + 0.11\omega_1^2\psi_3 + 0.052\omega_3^2\psi_3 \\ &\quad - 0.18\psi_1^2\psi_3 - 0.039\psi_2^2\psi_3 - 0.2\omega_2^2\psi_3 \\ &\quad - 0.38\omega_3\psi_3^2 + 0.4\omega_2\omega_3\psi_2 + 0.37\omega_1\omega_3\psi_1 \\ &\quad + 0.43\omega_2\psi_2\psi_3 - 0.69\omega_3 - 0.35\psi_3.\end{aligned}$$

This controller fits into our framework and we study stability properties of the Euler discretization to the continuous time system with a sampling period $T = 0.01\text{s}$. However, the controller is designed in [36] using density functions which do not necessarily guarantee UGAS of the closed-loop system. By using SOSTOOLS [33], we obtain the following Lyapunov function that guarantees that the closed-loop system is UGAS: $V(\omega, \psi) = 4.117\omega_1^2 - 1.569 \times 10^{-11}\omega_1\omega_2 + 9.63 \times 10^{-12}\omega_1\omega_3 + 2.031\omega_1\psi_1 - 3.877 \times 10^{-12}\omega_1\psi_2 + 8.338 \times 10^{-13}\omega_1\psi_3 + 3.678\omega_2^2 - 3.274 \times 10^{-12}\omega_2\omega_3 - 6.11 \times 10^{-12}\omega_2\psi_1 + 2.323\omega_2\psi_2 + 2.051 \times 10^{-12}\omega_2\psi_3 + 3.284\omega_3^2 + 8.196 \times 10^{-12}\omega_3\psi_1 + 9.284 \times 10^{-12}\omega_3\psi_2 + 1.709\omega_3\psi_3 + 1.4\psi_1^2 - 4.147 \times 10^{-12}\psi_1\psi_2 + 3.635 \times 10^{-12}\psi_1\psi_3 + 2.118\psi_2^2 + 1.065 \times 10^{-11}\psi_2\psi_3 + 1.669\psi_3^2$. Therefore, semi-global practical asymptotic stability of the Euler discretized model can be concluded due to Theorem 2 in [39]. This is enough to apply our results

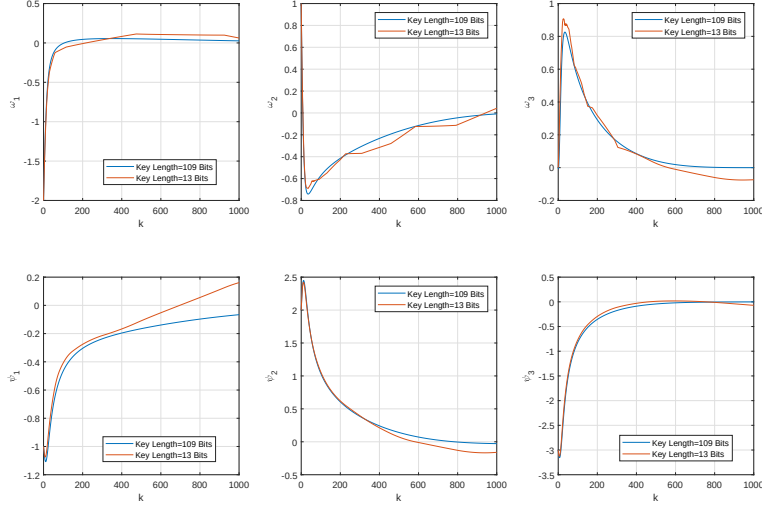


Figure 5: Trajectory of the controlled rigid body

on discrete-time systems since the polynomial structure of the closed-loop dynamics ensure that Assumption 3 and 4 are always satisfied over compact sets. While this is the case, stability of the Euler discretized model in general does not imply stability of the exact discrete time model and we refer readers to [29] and [30] for more details. Additionally, it should be noted that the practical stability in this example are contributed by both the sampling time T and the encryption.

In this example, we set $n_1 - m_1 - 1 = 1$ and $m_1 = 40$. The precision levels of the quantizers used for state measurement is 2^{-60} ($m_2 = 60$). The initial state is fixed at $[\omega \ \psi]^T = [-2 \ 1 \ 0 \ -1 \ 2 \ -3]^T$ and $n_y = 6$ leading to $n_2 - m_2 - 1 = 2$, which gives the key length of at least 109 bits. Following the steps in Algorithm 2, we simulate the behaviour of the closed-loop system with encrypted measurements. Additionally, a trajectory with key length being 13 bits is also generated for comparison. It is worth mentioning that a key length of 13 is often too short for practical use of Paillier encryption since it does not take too long for the attacker to break the encryption. It is used here just for illustrative purposes. The total computational times for systems using encryption with different key lengths are shown below in Table 1. The computation is done with Python programming language on Windows 10 over a laptop with Intel(R) i7-7500 CPU at 2.70GHz and 16GB of RAM. This also justifies the choice of $T = 0.01s$. However, the data shown in Table 1 indicate that a key length of 600 bits may not be suitable for real-time computations. For readers interested in real-time computations, we refer to [41] where FPGA-

based systems are used to get 1ms delays for key length of 512 bits and 10ms for key length of 1024 bits . From Fig. 5, it can be seen that the trajectory of the closed-loop system using encrypted control signals of a 109-bit key length is almost identical to the plot in [36] showing that increasing the key length does help recover the behaviour of the emulated controller. However, longer key lengths require longer computation times, which further require longer sampling periods to ensure that the necessary computations can be finished on time, this may lead to further issues since a large sampling period may result in the loss of stability of the original sampled-data model.

Table 1:

Key Lengths and Computation Times	
Key Length (bits)	Computation Time (ms)
10	0.207
120	6.096
240	31.398
480	268.411
600	633.732

8 Conclusions and future work

We have investigated the problem of using Paillier encryption to ensure the security and privacy of a NCS consisting of a discrete-time static controller and a discrete-time plant connected via a network. Assuming that the corresponding closed-loop system satisfies a robust asymptotic stability property when no encryption is used, we have provided sufficient conditions on the encryption parameters to guarantee a given ultimate bound and region of attraction of the state. Additionally, we have shown that if the disturbance is bounded by a sufficiently small number, it is possible to robustly stabilize the plant. Moreover, by imposing homogeneity assumptions on the closed-loop system, we have provided sufficient conditions to ensure that under gain matrix quantization it is possible to fully inherit the stability properties of the emulated controller enabling the use of dynamic quantizers to achieve ISS (UGAS) when there are (no) disturbances. The results have been applied to linear time-invariant systems to recover the main result in [8].

Future work will focus on applying these results to NCSs modelled by hybrid systems [11] and to look at the ways of implementing dynamic controllers.

References

- [1] M. Abdelrahim, V. S. Dolk, and W. P. M. H. Heemels. Input-to-state stabilizing event-triggered control for linear systems with output quantiza-

- tion. In *Proceedings of the 55th IEEE Conference on Decision and Control*, pages 483–488, 2016.
- [2] A. Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. Srivastava. Proloc: resilient localization with private observers using partial homomorphic encryption: demo abstract. In *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, pages 41–52, 2017.
 - [3] A. B. Alexandru, K. Gatsis, Y. Shoukry, S. A. Seshia, P. Tabuada, and G. J. Pappas. Cloud-based quadratic optimization with partially homomorphic encryption. *arXiv preprint arXiv:1809.02267*, 2018.
 - [4] J. Anderson and A. Papachristodoulou. Advances in computational lyapunov analysis using sum-of-squares programming. *Discrete and Continuous Dynamical Systems Series B*, 20(8):2361–2381, 2015.
 - [5] P. Antsaklis and J. Baillieul. Special issue on technology of networked control systems. *Proceedings of the IEEE*, 95(1):5–8, 2007.
 - [6] Z. Chen and J. Huang. Global robust stabilization of cascaded polynomial systems. *Systems & Control Letters*, 47(5):445–453, 2002.
 - [7] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim. Need for controllers having integer coefficients in homomorphically encrypted dynamic system. In *Proceedings of the 57th IEEE Conference on Decision and Control*, pages 5020–5025, 2018.
 - [8] F. Farokhi, I. Shames, and N. Batterham. Secure and private control using semi-homomorphic encryption. *Control Engineering Practice*, 67:13–20, 2017.
 - [9] T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO '84*, 196:10–18, 1984.
 - [10] C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.
 - [11] R. Goebel, R. G. Sanfelice, and A. R. Teel. *Hybrid Dynamical systems: Modelling, Stability and Robustness*. Princeton University Press, 2012.
 - [12] C. N. Hadjicostis. Privacy preserving distributed average consensus via homomorphic encryption. In *Proceedings of the 57th IEEE Conference on Decision and Control*, pages 1258–1263, 2018.
 - [13] W. P. M. H. Heemels, A. R. Teel, N. van de Wouw, and D. Nešić. Networked control systems with communication constraints: Tradeoffs between transmission intervals, delays and performance. *IEEE Transactions on Automatic Control*, 55(8):1781–1796, 2010.

- [14] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, 95(1):138–162, 2007.
- [15] Y. Jiang and Z. P. Jiang. Robust adaptive dynamic programming and feedback stabilization of nonlinear systems. *IEEE Transactions on Neural Networks and Learning Systems*, 25(5):882–893, 2014.
- [16] Y. Jiang and Z. P. Jiang. Global adaptive dynamic programming for continuous-time nonlinear systems. *IEEE Transactions on Automatic Control*, 60(11):2917–2929, 2015.
- [17] Z. P. Jiang and Y. Wang. Input-to-state stability for discrete-time nonlinear systems. *Automatica*, 37(6):857–869, 2001.
- [18] C. M. Kellett and A. R. Teel. On the robustness of $\mathcal{KL}$ -stability for difference inclusions: smooth discrete-time lyapunov functions. *SIAM Journal on Control and Optimization*, 44(3):777–800, 2005.
- [19] M. Kishida. Encrypted control system with quantiser. *IET Control Theory & Applications*, 13(1):146–151, 2019.
- [20] K. Kosigo and T. Fujita. Cyber-security enhancement of networked control systems using homomorphic encryption. In *Proceedings of the 54th IEEE Conference on Decision and Control*, pages 6836–6843, 2015.
- [21] M. Lazar, D. Muñoz de la Peña, W. P. M. H. Heemels, and T. Alamo. On input-to-state stability of min–max nonlinear model predictive control. *Systems & Control Letters*, 57(1):39–48, 2008.
- [22] F. L. Lewis, D. Vrabie, and K. G. Vamvoudakis. Reinforcement learning and feedback control: Using natural decision methods to design optimal adaptive controllers. *IEEE Control Systems Magazine*, 32(6):76–105, 2012.
- [23] D. Liberzon. Hybrid feedback stabilization of systems with quantized signals. *Automatica*, 39(9):1543–1554, 2003.
- [24] D. Liberzon and D. Nešić. Input-to-state stabilization of linear systems with quantized state measurements. *IEEE Transactions on Automatic Control*, 52(5):767–781, 2007.
- [25] Y. Lin, F. Farokhi, I. Shames, and D. Nešić. Secure control of nonlinear systems using semi-homomorphic encryption. In *Proceedings of the 57th IEEE Conference on Decision and Control*, pages 5002–5007, 2018.
- [26] Y. Lu and M. Zhu. Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 96:314–325, 2018.
- [27] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Proceedings of the 47th annual Allerton conference on communication, control, and computing*, pages 911–918, 2009.

- [28] C. Murguia, F. Farokhi, and I. Shames. Secure and private implementation of dynamic controllers using semi-homomorphic encryption. *arXiv preprint arXiv:1812.04168*, 2018.
- [29] D. Nešić and A. R. Teel. A framework for stabilisation of nonlinear sampled-data systems based on their approximate discrete-time models. *IEEE Transactions on Automatic Control*, 49(7):1103–1122, 2004.
- [30] D. Nešić, A. R. Teel, and P. V. Kokotović. Sufficient conditions for stabilization of sampled-data nonlinear systems via discrete-time approximations. *Systems & Control Letters*, 38(4–5):259–270, 1999.
- [31] D. Nešić, A. R. Teel, G. Valmorbida, and L. Zaccarian. Finite-gain $\mathcal{L}_p$ stability for hybrid dynamical systems. *Automatica*, 49(8):2384–2396, 2013.
- [32] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'99)*, pages 223–238, 1999.
- [33] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. A. Parrilo. SOSTOOLS: Sum of squares optimization toolbox for MATLAB. 2013. Available from <http://www.eng.ox.ac.uk/control/sostools>, <http://www.cds.caltech.edu/sostools> and <http://www.mit.edu/~parrilo/sostools>.
- [34] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, 2000.
- [35] M. J. D. Powell. *Approximation Theory and Methods*. Cambridge University Press, Cambridge, U.K., 1981.
- [36] S. Prajna, P. A. Parrilo, and A. Rantzer. Nonlinear control synthesis by convex optimization. *IEEE Transactions on Automatic Control*, 49(2):310–314, 2004.
- [37] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM*, 21(2):120–126, 1978.
- [38] M. Ruan, H. Gao, and Y. Wang. Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, to appear.
- [39] A. R. Teel. Lyapunov methods in nonsmooth optimization, part I: Quasi-Newton algorithms for Lipschitz, regular functions. In *Proceedings of the 39th IEEE Conference on Decision and Control*, pages 112–117, 2000.

- [40] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, 2015.
- [41] J. Tran, F. Farokhi, M. Cantoni, and I. Shames. Implementing homomorphic encryption based secure feedback control. *Control Engineering Practice*, 97:104350, 2020.
- [42] S. E. Tuna and A. R. Teel. Discrete-time homogeneous Lyapunov functions for homogeneous difference inclusions. *In Proceedings of the 43rd IEEE Conference on Decision and Control*, pages 1606–1610, 2004.
- [43] N. van de Wouw, D. Nešić, and W. P. M. H. Heemels. A discrete-time framework for stability analysis of nonlinear networked control systems. *Automatica*, 48(6):1144–1153, 2012.
- [44] J. Xu, L. Xie, and Y. Wang. Simultaneous stabilization and robust control of polynomial nonlinear systems using sos techniques. *IEEE Transactions on Automatic Control*, 54(8):1892–1897, 2009.

A Proof of Theorem 1

Proof. First, note that step 9 of Algorithm 1 represents the standard multiplication between matrices on encrypted numbers. Since each addition may lead to at most one more integer bit, for an n_y dimensional vector $\bar{g}(x)$, $n_y - 1$ additions are required. Thus the condition $N > 2^{n_y + n_1 + n_2 - 1}$ ensures that all encrypted data can be decrypted to get the desired control inputs without overflow and underflow. For simplicity, we will use the following equivalent dynamics $f(x, \bar{K}\bar{g}(x), w)$ to represent the closed-loop system.

We represent $f(x, \bar{K}g(x), w)$ and $f(x, Kg(x), w)$ by f_1 and f respectively for simplicity. Similarly we write $f(x, \bar{K}\bar{g}(x), w)$ as f_2 . We prove the theorem by 2 steps. First, we show that under certain conditions the closed-loop system with gain matrix quantization (f_1) is ISS in a proper sense, then based on this result, we derive sufficient conditions to allow extra quantization of the measurement signal (f_2) without losing ISS.

Then for the same Lyapunov function given in Assumption 3, we have for all $x \in \mathbb{R}^{n_x}$:

$$\begin{aligned} V(f_1) - V(x) &= V(f_1) - V(f) + V(f) - V(x) \\ &\leq V(f_1) - V(f) - \alpha_3(|x|) + \gamma(|w|). \end{aligned} \tag{26}$$

For any $\Delta_x = \bar{\Delta} > 0$, on the ball of radius Δ_x , $\mathbb{B}_{\Delta_x} = \{x \in \mathbb{R}^{n_x} : |x| \leq \Delta_x\}$, there exists a positive constant L_V such that $|V(x) - V(y)| \leq L_V|x - y|$, for all $x, y \in \mathbb{B}_{\Delta_x}$. Thus (26) implies that for all $x \in \mathbb{B}_{\Delta_x}$:

$$\begin{aligned} V(f_1) - V(x) &\leq V(f_1) - V(f) - \alpha_3(|x|) + \gamma(|w|) \\ &\leq |V(f_1) - V(f)| - \alpha_3(|x|) + \gamma(|w|) \\ &\leq L_V|f_1 - f| - \alpha_3(|x|) + \gamma(|w|) \\ &\leq L_V L_f e_1 |g(x)| - \alpha_3(|x|) + \gamma(|w|). \end{aligned} \tag{27}$$

where the second step follows from the fact that a continuous mapping maps a compact set to another compact set, thus the existence of the Lipschitz constant L_V can be guaranteed. Since $g(x)$ is continuous on $\mathbb{R}^{n_x}$, for any $\delta_x \leq |x| \leq \Delta_x$, $|g(x)|$ attains its maximum $M_1 > 0$. Thus we have if $e_1 \leq \epsilon_1 = \frac{(1-\mu_1)\alpha_3(\delta_x)}{M_1 L_V L_f}$ with $0 < \mu_1 < 1$, then $V(f_1) - V(x) \leq -\mu_1 \alpha_3(|x|) + \gamma(|w|)$.

For all $\delta_x \leq |x| \leq \Delta_x$ the following holds:

$$\begin{aligned} V(f_2) - V(x) &= V(f_2) - V(f_1) + V(f_1) - V(x) \\ &\leq V(f_2) - V(f_1) - \mu_1 \alpha_3(|x|) + \gamma(|w|) \\ &\leq L_V |f_2 - f_1| - \mu_1 \alpha_3(|x|) + \gamma(|w|) \\ &\leq L_V L_f |\bar{K}| e_2 - \mu_1 \alpha_3(|x|) + \gamma(|w|). \end{aligned} \quad (28)$$

Thus, if $e_2 \leq \epsilon_2 = \frac{\mu_1(1-\mu_2)\alpha_3(\delta_x)}{L_V L_f |\bar{K}|}$ with $0 < \mu_2 < 1$, we have $V(f(x, \bar{K}\bar{g}(x), w)) - V(x) \leq -\mu_1 \mu_2 \alpha_3(|x|) + \gamma(|w|)$. In contrast to the continuous time case, this condition is insufficient for concluding that the discrete-time closed-loop system is semi-globally practically ISS as discussed in Section III of [29]. For the region $\mathbb{B}_{\delta_x} = \{x \in \mathbb{R}^{n_x} : |x| \leq \delta_x\}$, (28) does not hold in general, instead, from (27), we have for all $x \in \mathbb{B}_{\delta_x}$:

$$\begin{aligned} V(f_2) - V(x) &\leq V(f_2) - V(f_1) + V(f_1) - V(x) \\ &\leq L_V L_f (e_1 |g(x)| + e_2 |\bar{K}|) - \alpha_3(|x|) + \gamma(|w|) \\ &\leq L_V L_f (\epsilon_1 |g(x)| + \epsilon_2 |\bar{K}|) - \alpha_3(|x|) + \gamma(|w|) \\ &\leq -\alpha_3(|x|) + \gamma(|w|) + \eta. \end{aligned} \quad (29)$$

where $\eta = \frac{M_2(1-\mu_1)\alpha_3(\delta_x)}{M_1} + \mu_1(1-\mu_2)\alpha_3(\delta_x)$, $M_2 = \max_{x \in \mathbb{B}_{\delta_x}} |g(x)|$. By Lemma 3.5 in [17], the set $\{x \in \mathbb{R}^{n_x} : V(x) \leq b_1\}$ where $b_1 = \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\eta + \gamma(|w|))$ and ρ is any $\mathcal{K}_\infty$ function such that $Id - \rho \in \mathcal{K}_\infty$, is forward invariant. Define $b_{1max} = \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\eta + \gamma(\Delta_w))$. Since the upper bound of the disturbance satisfies $\alpha_1^{-1}(b_{1max}) < \Delta_x$, the state cannot escape away from the set $\mathbb{B}_{\Delta_x}$ from the set $\mathbb{B}_{\delta_x}$ even in the presence of disturbances. As a result, following similar arguments, the set $\{x \in \mathbb{R}^{n_x} : V(x) \leq b_2\}$ is also forward invariant, where $b_2 = \alpha_2 \circ \alpha_3^{-1} \circ \mu_1^{-1} \mu_2^{-1} \rho^{-1}(\gamma(|w|))$. Define $b_{2max} = \alpha_2 \circ \alpha_3^{-1} \circ \mu_1^{-1} \mu_2^{-1} \rho^{-1}(\gamma(\Delta_w))$. Since we have $\alpha_1^{-1}(b_{2max}) < \Delta_x$, the set $\mathbb{B}_{\Delta_x}$ is forward invariant. Then follow similar arguments in Section 3.5 in [17], we deduce that there exists $\beta \in \mathcal{KL}$ such that $\phi(k, x_0, w)$, the solution of (11) starting at x_0 with $|x_0| \leq \Delta_x$ at time k satisfies:

$$|\phi(k, x_0, w)| \leq \beta(|x_0|, k) + \sigma(|w|) + \delta, \quad (30)$$

where $\delta = \alpha_1^{-1}((\frac{M_2(1-\mu_1)}{M_1} + \mu_1(1-\mu_2))\alpha_3(\delta_x) + \alpha_2(\delta_x))$ and $\sigma(s) = \max\{\sigma_1, \sigma_2\}$ where $\sigma_1(s) = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \mu_1^{-1} \mu_2^{-1} (Id + \rho) \circ \gamma(s)$, $\sigma_2(s) = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ (Id + \rho) \circ \gamma(2s)$. $\square$

B Proof of Theorem 2

Proof. We only present a sketch of the proof since it overlaps a lot with the proof of Theorem 1. Based on stated assumptions and Lemma 3, (21), (22) and (23) are guaranteed to hold.

Thus, by Lemma 3, for all $x \in \mathbb{R}^{n_x}$ we have:

$$\begin{aligned} V(f) - V(x) &= V(f) - V(f(x, Kg(x), 0)) \\ &\quad + V(f(x, Kg(x), 0)) - V(x) \\ &\leq -c_3|x| + LL_w|w|. \end{aligned} \quad (31)$$

$$\begin{aligned} V(f_1) - V(x) &= V(f_1) - V(f) + V(f) - V(x) \\ &\leq V(f_1) - V(f) - c_3|x| + LL_w|w| \\ &\leq |V(f_1) - V(f)| - c_3|x| + LL_w|w| \\ &\leq L|f_1 - f| - c_3|x| + LL_w|w| \\ &\leq LL_f e_1 \kappa |x| - c_3|x| + LL_w|w|. \end{aligned} \quad (32)$$

Then we have if $e_1 \leq \epsilon_1 = \frac{c_3(1-\mu_1)}{LL_f \kappa}$, where, $0 < \mu_1 < 1$, it holds true that $V(f_1) - V(x) \leq -\mu_1 c_3|x| + LL_w|w|$ for all $x \in \mathbb{R}^{n_x}$.

Since the following holds:

$$\begin{aligned} V(f_2) - V(x) &= V(f_2) - V(f_1) + V(f_1) - V(x) \\ &\leq V(f_2) - V(f_1) - \mu_1 c_3|x| + LL_w|w| \\ &\leq L|f_2 - f_1| - \mu_1 c_3|x| + LL_w|w| \\ &\leq LL_f |\bar{K}| e_2 - \mu_1 c_3|x| + LL_w|w|. \end{aligned} \quad (33)$$

Thus, for any $0 < \delta_x < \Delta_x < \infty$, if $e_2 \leq \epsilon_2 = \frac{\mu_1(1-\mu_2)c_3\delta_x}{LL_f|\bar{K}|}$, with $0 < \mu_2 < 1$ we have $V(f(x, \bar{K}\bar{g}(x), w)) - V(x) \leq -\mu_1\mu_2 c_3|x| + LL_w|w| \leq -\frac{\mu_1\mu_2 c_3}{c_2}V(x) + LL_w|w|$. For the region $\mathbb{B}_{\delta_x} = \{x \in \mathbb{R}^{n_x} : |x| \leq \delta_x\}$, we have:

$$\begin{aligned} V(f_2) - V(x) &\leq V(f_2) - V(f_1) + V(f_1) - V(x) \\ &\leq \mu_1(1 - \mu_2)c_3\delta_x - \mu_1 c_3|x| + LL_w|w| \\ &\leq -\mu_1 c_3|x| + LL_w|w| + \eta \\ &\leq -\frac{\mu_1 c_3}{c_2}V(x) + LL_w|w| + \eta, \end{aligned} \quad (34)$$

where $\eta = \mu_1(1 - \mu_2)c_3\delta_x$. By Lemma 3.5 in [17], the set $\{x \in \mathbb{R}^{n_x} : V(x) \leq b_1\}$ where $b_1 = \frac{c_2(\eta + LL_w||w||)}{c_3\rho}$ and ρ is any constant such that $0 < \rho < 1$, is forward invariant. Define $b_{1max} = \frac{c_2(\eta + LL_w\Delta_w)}{c_3\rho}$. Since the upper bound of the disturbance satisfies $\frac{b_{1max}}{c_1} < \Delta_x$, the state cannot escape away from the set $\mathbb{B}_{\Delta_x}$ from the set $\mathbb{B}_{\delta_x}$ even in the presence of disturbances. Following similar arguments, the set $\{x \in \mathbb{R}^{n_x} : V(x) \leq b_2\}$ is also forward invariant, where

$b_2 = \frac{c_2 L L_w ||w||}{c_3 \mu_1 \mu_2 \rho}$. Define $b_{2max} = \frac{c_2 L L_w \Delta_w}{c_3 \mu_1 \mu_2 \rho}$. Since we have $\frac{b_{2max}}{c_1} < \Delta_x$, the set $\mathbb{B}_{\Delta_x}$ is forward invariant. Then $\phi(k, x_0)$ with $|x_0| \leq \Delta_x$ satisfies:

$$|\phi(k, x_0)| \leq \frac{c_2}{c_1} |x_0| \left(1 - \frac{\mu_1 \mu_2 c_3}{c_2}\right)^k + \sigma ||w|| + \delta, \quad (35)$$

where $\delta = \frac{c_2 \eta}{c_1 c_3 \rho}$, $\sigma = \max\{\sigma_1, \sigma_2\}$, $\sigma_1 = \frac{c_2 L L_w}{c_1 c_3 \mu_1 \mu_2}$ and $\sigma_2 = \frac{c_2 L L_w}{c_1 c_3 \mu_1}$. Since we have $0 < \mu_2 < 1$, $\sigma = \sigma_1 = \frac{c_2 L L_w}{c_1 c_3 \mu_1 \mu_2}$. $\square$