Author/s:
Lin, Y;Farokhi, F;Shames, I;Nesic, D

Title:
Secure Control of Nonlinear Systems Using Semi-Homomorphic Encryption

Date:
2018-01-01

Citation:
Lin, Y., Farokhi, F., Shames, I. & Nesic, D. (2018). Secure Control of Nonlinear Systems Using Semi-Homomorphic Encryption. Proceedings of the 57th IEEE Conference on Decision and Control (CDC), 2018-December, pp.5002-5007. IEEE. https://doi.org/10.1109/CDC.2018.8619569.

Persistent Link:
https://hdl.handle.net/11343/251858

Secure Control of Nonlinear Systems Using Semi-Homomorphic Encryption

Yankai Lin, Farhad Farokhi, Iman Shames, and Dragan Nešić

***Abstract*— A secure nonlinear networked control system (NCS) design using semi-homomorphic encryption, namely, Paillier encryption is studied. Under certain assumptions, control signal computation using encrypted signal directly is allowed by semi-homomorphic encryption. Thus, the security of the NCSs is further enhanced by concealing information on the controller side. However, additional technical difficulties in the design and analysis of NCSs are induced compared to standard NCSs. In this paper, the stabilization of a nonlinear discrete time NCS is considered. More specifically, sufficient conditions on the encryption parameters that guarantee stability of the NCS are provided, and a trade-off between the encryption parameters and the ultimate bound of the state is shown.**

I. INTRODUCTION

Networked control system is an emerging technology that differs from traditional control systems by employing shared communication channels to close the control loop instead of dedicated point-to-point connections to transmit the sensor and actuator data [1]. This offers many benefits including easier installation and maintenance as well as lower cost, weight and less volume. However, the use of shared network also leads to some technical difficulties that have to be carefully dealt with by the designer. A good summary of those issues are given in [21] and [5].

However, network security and privacy as an important issue of NCS, is not discussed in [21]. Cyber-security threats have attracted increased attention from researchers as in the last few years. In the work of [19], the authors decompose different cyber-security attack scenarios into various categories based on the resources the attacker needs. Eavesdropping attack is one important class of those attacks where a malicious attacker tries to monitor the data going through the control loop. Moreover, it enables the attacker to launch more complex attacks such as replay attacks [15]. Fig. 1 illustrates a typical control loop that uses encryption-decryption schemes to deal with this issue. It is able to protect the information flowing through the network. However, if the attacker has access to the information on the controller side, the encryption scheme becomes useless.

Following this motivation, we focus on employing homomorphic encryption schemes for NCS configured in the form of Fig. 2 that enable implementing controllers on encrypted messages directly. Homomorphic encryption is a form of encryption that allows computation on cipher-texts (encrypted data). An example of such encryption methods is given by Gentry [4] which allows both multiplication and summation of plain-text to be performed on cipher-text. Semi-homomorphic encryption, on the other hand, only allows one of them to be performed on cipher-texts. In the earlier work by Kogiso and Fujita [11], the authors propose a method to encrypt the controller using RSA [18] and El Gamal [3] encryptions which are encryption schemes homomorphic under multiplications of cipher-texts. However, in [11] stability and performance guarantees of the closed loop system using encryptions are not studied thoroughly. In [2], the authors provide semi-global practical stability guarantees for linear time-invariant (LTI) systems. However, the nonlinear stabilization problem is not studied. The work [10] studies the design of encrypted control systems using Paillier cryptosystem [17]. In addition to considering the linear case, the author also investigates the stabilization of nonlinear systems using feedback linearization. The possibility of applying Paillier encryption to distributed projected gradient-based algorithms is studied in [14].

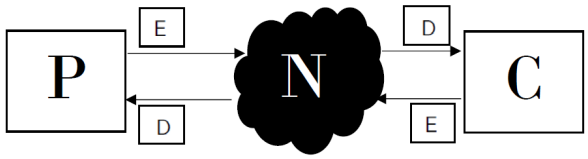

Fig. 1. NCS consisting of a plant P, controller C and network N, with encryption-decryption units

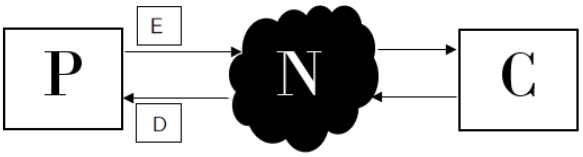

Fig. 2. NCS consisting of a plant P, controller C and network N, with semi-homomorphic encryption-decryption units

In this paper, we consider the problem of stabilizing a nonlinear NCS using Paillier encryption which allows (i) addition of two encrypted values and (ii) multiplication of an encrypted value by a plain-text value. These operations can be easily generalized to the case involving multiplications between a plain-text matrix and a vector of cipher-texts. In this work, we use a discrete-time model to describe the dynamics of the NCS for simplicity, as the main aim of this

*This work was supported under the Australian Research Council under the Discovery Project DP170104099.

The authors are with the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, 3010, Victoria, Australia. yankail@student.unimelb.edu.au, farhad.farokhi@unimelb.edu.au, iman.shames@unimelb.edu.au, dnesic@unimelb.edu.au.

work is to ensure the security and privacy for the NCS. A more detailed analysis of NCS using a discrete-time model can be found in [20]. The designer first designs a controller for the discrete-time plant without the use of encryption and then based on stability requirements, the designer chooses the parameters of the encryption scheme.

To summarize, the main contribution of the paper is that we give a framework of using Paillier encryption to design controllers which stabilize a class of nonlinear NCSs while preserving security and privacy of data flowing through the network. Sufficient conditions on the encryption parameters for stabilization of the nonlinear closed loop systems without overflow and underflow are provided. Moreover, by imposing a stronger assumption on the closed loop system, namely, linearity, we provide less conservative sufficient conditions for the same problem. Lastly, it also covers linear NCSs as a special case where the results in [2] can be recovered.

The rest of the paper is organized as follows. Preliminaries are given in Section II. Background material about Paillier encryption is presented in Section III. The NCS model and the problem formulation are presented in Section IV. Controller design for stabilization of the system are given in Section V and a numerical example is presented in Section VI. Conclusions are given in Section VII.

II. Preliminaries and notations

Let $\mathbb{R}$ be the set of real numbers, $\mathbb{R}_{\geq 0} := [0, \infty)$, $\mathbb{Z}_{\geq 0} := \{0, 1, 2, 3, ...\}$, $\mathbb{Z}_{>0} := \{1, 2, 3, ...\}$ and $\mathbb{Z}_n := \{0, 1, 2, 3, ...n-1\}$. We use (x, y) to denote $[x^T, y^T]^T \in \mathbb{R}^{n+m}$ for $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^m$. A function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ 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 $\beta(s, t) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ 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 decreasing to zero. 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 the ∞-norm of it is denoted by $|x|_\infty = \max_{1 \leq i \leq n} |x_i|$. For any function $\phi : \mathbb{Z}_{\geq 0} \to \mathbb{R}^n$, 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. The scalar a_{ji} denotes the element of A in the j-th row i-th column for $j \in \{1, 2, ..., n\}$ and $i \in \{1, 2, ..., m\}$. For a real, square and symmetric matrix P the largest and the smallest eigenvalue of P are denoted by $\lambda_{max}(P)$ and $\lambda_{min}(P)$ respectively.

III. Backgroud materials of Paillier encryption

A. Fixed-point operations

The main aim of this part is to give some basic results about signed fixed-point rational numbers in base 2 and introduce the function to transfer them to integers so that they can be Paillier encrypted. Most of the material here can also be found in [2]. 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: $\mathbb{Q}(n, m) = \{b \in \mathbb{Q} : b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} b_i 2^{i-m-1}, b_i \in \{0, 1\}, \forall i \in 1, ..., n\}$. 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: $\chi_{n,m}(b) : \mathbb{Q}(n, m) \to \mathbb{Z}_{2^n} = 2^m b \mod 2^n$. Moreover, the inverse mapping is defined as $\chi_{n,m}^{-1}(a) : \mathbb{Z}_{2^n} \to \mathbb{Q}(n, m) = (a - 2^n \mathbb{I}_{a \geq 2^{n-1}})/2^m$, 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 without proofs.

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 demonstrates that $\mathbb{Q}(n, m)$ is isomorph to $\mathbb{Z}_{2^n}$, consequently, 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. 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 1: For a, $a^* \in \mathbb{Z}_{2^n}$:

i). $a \overset{n}{\oplus} a^* = (a + a^*) \mod 2^n$;

ii). $a \overset{n}{\otimes} a^* = a a^* \mod 2^n$. ■

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

Proposition 2: For all $b, b^* \in \mathbb{Q}(n, m)$ such that $bb^* \in \mathbb{Q}(n, m)$:

$$\chi_{n+2m,2m}(bb^*) = \chi_{n+2m,m}(b) \overset{n+2m}{\otimes} \chi_{n+2m,m}(b^*).$$

■

B. 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) [16]. The steps to do Paillier encryption scheme are given below:

- Key generation:
  - 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;
  - Compute public key $N = pq$;
  - Calculate private key $\lambda = \text{lcm}(p-1, q-1)$ and $\mu = \lambda^{-1} \mod N$, where $\text{lcm}(a, b)$ refers to the least common multiple of a and b.
- Encryption:
  - Select random $r \in \mathbb{Z}_N^* := \{x \in \mathbb{Z}_N | \gcd(x, N) = 1\}$;
  - Construct the cipher-text of a message $t \in \mathbb{Z}_N$ as $\mathsf{E}(t; r) = (N+1)^t r^N \mod N^2$.
- Decryption:

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

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 [16] that:

$$\mathsf{D}(\mathsf{E}(t;r)) = t, \forall r \in \mathbb{Z}_N^*, \forall t \in \mathbb{Z}_N. \tag{1}$$

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 may not be allowed. This is due to the fact for two cipher-texts $\mathsf{E}(a)$ and $\mathsf{E}(b)$, a sufficiently small $|\mathsf{E}(a) - \mathsf{E}(b)|$ in general does not imply a small $|a-b|$. ■

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 $t + t^* \in \mathbb{Z}_N$, $\mathsf{E}(t;r)\mathsf{E}(t^*;r^*) \bmod N^2 = \mathsf{E}(t+t^*, rr^*)$;

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

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 1.

Proposition 4: Assume that $N > 2^n$. $\forall r \in \mathbb{Z}_N^*$ and $a, a^* \in \mathbb{Z}_{2^n}$, $\mathsf{D}(\mathsf{E}(a;r)^{a^*} \bmod N^2) \bmod 2^n = a \overset{n}{\otimes} a^*$ if: $a \overset{n}{\otimes} a^* \in \mathbb{Z}_{2^n}$. ■

Remark 2: A necessary condition required in Proposition 4 is that the outcome of multiplication does overflow which means it stays 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 are 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. ■

IV. NCS ARCHITECTURE AND PROBLEM STATEMENT

The considered NCS architecture is depicted in Fig. 2, where Paillier encryption is used to allow computing control inputs directly using encrypted data. The plant of the NCS is given by the discrete-time system:

$$x^+ = f(x,u) \tag{2}$$

where $x \in \mathbb{R}^{n_x}$ is the state of the system and $u \in \mathbb{R}^{n_u}$ is the control input of the plant considered respectively. The mapping $f : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \to \mathbb{R}^{n_x}$ is in general nonlinear. Moreover, $f(0,0) = 0$ 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 proportional controller is considered in this paper:

$$u = Kg(x), \tag{3}$$

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

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. However, it is still possible to cover some cases where static state feedback controller is used to control the system. Moreover, it also covers the case when the designer wants to use $g(x)$ to approximate a desired function that can not be easily realised due to hardware constraints. ■

By substituting (3) to (2), we arrive at the following expression of the closed loop system:

$$x^+ = f(x, Kg(x)). \tag{4}$$

The main objective of this study is to develop a framework to implement the controller of the form (4) with Paillier encryptions that guarantees certain stability properties. In view of Remark 1, we make the following standing assumption throughout the paper:

Assumption 1: The control computation (3) and the digital data transmitted through the network are error free. ■

The above assumption enables us to properly design the matrix K to make controller (3) equivalent to the control law calculated using encrypted signals based on Proposition 2 as shown in Theorem 1 later.

V. STABILITY RESULT

A. The nonlinear case

In view of Remark 2, to be able to implement (3), 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 $n_2 + m_2 > 0$.

For the closed loop system:

$$x^+ = f(x, Kg(x)), \tag{5}$$

we follow an emulation like approach that the designer first design a gain matrix $K \in \mathbb{R}^{n_u \times n_y}$ that globally stabilize the system (4) and then adjust the gain matrix to get $\bar{K} \in \mathbb{R}^{n_u \times n_y}$ that can be used to multiply encrypted numbers based on the resources available. To state the main result, we make the following assumptions:

Assumption 2: There exists a Lyapunov function $V : \mathbb{R}^{n_x} \to \mathbb{R}_{\geq 0}$ that is Lipschitz continuous on every compact set of $\mathbb{R}^{n_x}$ with the Lipschitz constant L_v for system (5), such that the following inequalities hold for α_1, α_2 and $\alpha_3 \in \mathcal{K}_\infty$:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|), \tag{6}$$

$$V(f(x, Kg(x))) - V(x) \leq -\alpha_3(|x|), \tag{7}$$

for any $x \in \mathbb{R}^{n_x}$. ■

Assumption 3: The function f is continuous on $\mathbb{R}^{n_x} \times \mathbb{R}^{n_u}$. Moreover, for every compact set $S \subset \mathbb{R}^{n_x} \times \mathbb{R}^{n_u}$, there exists $L_f > 0$ such that $|f(x, u_1) - f(x, u_2)| \leq L_f|u_1 - u_2|$, for all (x, u_1) and $(x, u_2) \in S$. ■

Assumption 4: The function $g(x)$ is continuous on $\mathbb{R}^{n_x}$ and $g(0) = 0$. ■

Remark 4: If the origin of the closed loop system (5) is uniformly globally asymptotically stable (UGAS), then by Theorem 1 of [7], a smooth Lyapunov function that satisfies Assumption 2 is guaranteed to exist. 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 [8]. If the controller can only locally stabilize the origin or stabilize a compact set containing the origin, one can obtain a similar result using the same approach. ■

Now we are ready to state our first main result. The control designer, the sensors, the controller and the actuators can follow the steps given by Algorithm 1 to implement the control law. The corresponding closed loop system is given by:

$$x^+ = f(x, \bar{K}\bar{g}(x)). \tag{8}$$

We use $\phi(k, x_0)$ to denote the solution of (8) at time k (assuming the initial time instant is 0) starting at x_0.

Algorithm 1 Secure and private implementation of the static controller with encrypted measurements

Require: n_1, m_1, n_2, m_2, K, $g(x)$, p, q
Ensure: u

Set $n \leftarrow n_y + n_1 + n_2 - 1$, $m \leftarrow m_1 + m_2$ and $y = g(x)$
\# Control Designer
Compute $\bar{K} \leftarrow \arg\min_{A \in \mathbb{Q}(n_1, m_1)^{n_u \times n_y}} ||A - K||_F$
Construct $\Gamma_{ji} \leftarrow \chi_{n+2m,m}(\bar{K}_{ji})$
\# Sensors
for $i = 1, ..., n_y$ **do**
  Construct $\bar{y} \leftarrow \arg\min_{z \in \mathbb{Q}(n_2, m_2)^{n_y}} |z - y|$
  Transmit $z_i \leftarrow \mathsf{E}(\chi_{n+2m,m}(\bar{y}_i); r)$ to the controller
end for
\# Controller
for $j = 1, ..., n_u$ **do**
  Set $l_j \leftarrow z_1^{\Gamma_{j1}} \bmod N^2$
  for $i = 2, ..., n_y$ **do**
    Compute $l_j \leftarrow (l_j(z_i^{\Gamma_{ji}} \bmod N^2)) \bmod N^2$
  end for
  Transmit l_j to the actuators
end for
\# Actuators
for $j = 1, ..., n_u$ **do**
  Implement $u_j \leftarrow \mathsf{D}(l_j) \bmod 2^{n+2m}/2^{2m}$
end for

In Algorithm 1, the main factor that may deteriorate the control performance is due to the uniform quantizers in step 3 and 7. This is slightly different with the scenario considered in the quantized control literature [12] and [13]. 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 [12] and [13].

Theorem 1: Suppose there exists $K \in \mathbb{R}^{n_u \times n_y}$ such that Assumption 2 holds, and Assumption 3 and Assumption 4 hold for the closed loop system (5). Then, there exists $\beta \in \mathcal{KL}$ such that for any $0 < \delta < \Delta$ and $x_0 \in \{z \in \mathbb{R}^{n_x} : |z| \leq \Delta\}$ one can choose integers n_1, m_1, n_2, m_2 and N large enough so that:

i). $N > 2^{n_y + n_1 + n_2 - 1}$,
ii). $m_1 \geq -\log_2(\epsilon_1/\sqrt{n_u n_y}) - 1$,
iii). $n_1 \geq m_1 + 1 + \log_2(\max_{i,j}|K_{ij}|)$,
iv). $m_2 \geq -\log_2(\epsilon_2/\sqrt{n_y}) - 1$,
v). $n_2 \geq m_2 + 1 + \log_2(\max_{0 \leq |x| \leq \Delta}|g(x)|_\infty)$,

to guarantee that any solution $\phi(\cdot, x)$ to (8) satisfies:

$$|\phi(k, x_0)| \leq \max\{\beta(|x_0|, k), \delta\}, \tag{9}$$

where

$$\epsilon_1 = \tfrac{(1-\mu_1)\alpha_3(\delta_x)}{M_1 L_V L_f},$$
$$\epsilon_2 = \tfrac{\mu_1(1-\mu_2)\alpha_3(\delta_x)}{L_V L_f |\bar{K}|},$$

with $\delta = \alpha_1^{-1} \circ \alpha_2 \circ \alpha_3^{-1} \circ \rho^{-1}(\frac{M_2(1-\mu_1)\alpha_3(\delta_x)}{M_1} + \mu_1(1 - \mu_2)\alpha_3(\delta_x))$, 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 2, $M_1 = \max_{\delta_x \leq |x| \leq \Delta}|g(x)|$, $M_2 = \max_{0 \leq |x| \leq \delta_x}|g(x)|$, $0 < \mu_1 < 1$ and $0 < \mu_2 < 1$ are constants chosen by the designer.

■

This theorem shows 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 follow the conditions listed in Theorem 1 to select large enough integers to implement Algorithm 1 and ensure that (9) holds. The constants μ_1 and μ_2 characterise the quantization error of the gain matrix and measurement respectively, larger (smaller) values lead to finer (coarser) quantizers which will determine the ultimate bound of the state.

Remark 5: There is a trade-off between the performance of the system and the required resources. In order to achieve a large domain of attraction and a small neighbourhood around the origin to which the state is converging to, the designer needs to choose a large enough N and m. However, this also increases the computational cost of Algorithm 1. 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 as $\mathcal{O}(N^3)$. 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. Striking a balance optimally between these quantities is relevant in practice. However, it is far from trivial since the system involves several nonlinearities and many parameters. The investigation of this problem is beyond the scope of this work and is left for future research. ■

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 DCR assumption if the key length is chosen to be large enough. Detailed discussions on this problem can be found in [16]. ■

B. The linear case

In this section, we show that if more information about the system dynamics is available to the designer, the results in Theorem 1 can be improved and made less conservative. Namely, we show that if the plant is a linear time-invariant and is controlled by a static state feedback controller, the expressions for n_1, n_2, m_1 and m_2 will be simplified. It recovers the result in [2] as a special case but using a different but equivalent formulation. If in addition, the quantizers have infinite ranges, then global practical stability can be established.

Remark 7: In fact, for linear systems it is possible to state similar results based on the continuity of eigenvalues as in [2] and discrete time input-to-state stability (ISS) [6] based results using quadratic Lyapunov functions as discussed for the continuous case in [12] and [13]. This is due to the fact that asymptotic stability for linear systems is equivalent to ISS with respect to measurement noises which is one of the main assumptions in [12] and [13]. Here, we present it in a different but equivalent way to make it consistent with Theorem 1 for linear systems. ■

Suppose the plant is described by the following linear difference equation:

$$x^+ = Ax + Bu, \tag{10}$$

controlled by:

$$u = Kx. \tag{11}$$

where $x \in \mathbb{R}^{n_x}$ is the state of the system, $u \in \mathbb{R}^{n_u}$ is the input and we have $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_u}$ $K \in \mathbb{R}^{n_u \times n_x}$. And the closed loop system corresponding to Algorithm 1 is given by:

$$x^+ = Ax + B\bar{K}\bar{x}, \tag{12}$$

The following assumption is made on the controller:

Assumption 5: $A+BK$ is Schur, that is, all eigenvalues of the matrix $A+BK$ are inside the unit circle in the complex plane. ■

It is well-known, see [9] for example, that if Assumption 5 is satisfied, there exist positive definite matrices P and Q that satisfy the discrete-time Lyapunov equation:

$$\tilde{A}^T P \tilde{A} - P = -Q, \tag{13}$$

where $\tilde{A} = A + BK$. Then it can be easily seen that Assumption 2 are satisfied with $\alpha_1(s) = \lambda_{min}(P)s^2$, $\alpha_2(s) = \lambda_{max}(P)s^2$, $\alpha_3(s) = \lambda_{min}(Q)s^2$ and $L_v = 2|P||x|$. Assumption 3 is met with $L_f = |B|$. This leads to the following corollary:

Corollary 1: Suppose there exists $K \in \mathbb{R}^{n_u \times n_y}$ such that Assumption 5 holds. Then, for any $0 < \delta < \Delta$ and $x_0 \in \{z \in \mathbb{R}^{n_x} : |z| \leq \Delta\}$ one can choose integers n_1, m_1, n_2, m_2 and N large enough so that:

i). $N > 2^{n_y+n_1+n_2-1}$,
ii). $m_1 \geq -\log_2(\epsilon_1/\sqrt{n_u n_y})$,
iii). $n_1 \geq m_1 + 1 + \log_2(\max_{i,j}|K_{ij}|)$,
iv). $m_2 \geq -\log_2(\epsilon_2/\sqrt{n_y})$,
v). $n_2 \geq m_2 + 1 + \log_2(|x_0|_\infty)$,

to guarantee that any solution $\phi(\cdot, x)$ to (12) satisfies:

$$|\phi(k, x_0)| \leq \max\{\frac{\lambda_{max}(P)}{\lambda_{min}(P)}|x_0|(1 - \frac{\mu_1\mu_2\lambda_{min}(Q)}{\lambda_{max}(P)})^k, \delta\}, \tag{14}$$

where:

$$\epsilon_1 = \frac{\lambda_{min}(Q)(1-\mu_1)}{2|P||B|},$$
$$\epsilon_2 = \frac{\mu_1(1-\mu_2)\lambda_{min}(Q)\delta_x}{2|P||B||\bar{K}|},$$

with $\delta = \sqrt{\frac{\rho^{-1}(\mu_1(1-\mu_2)\lambda_{min}(Q)\delta_x)\lambda_{max}(P)}{\lambda_{min}(Q)\lambda_{min}(P)}}$, ρ is any $\mathcal{K}_\infty$ function such that $Id - \rho \in \mathcal{K}_\infty$. The positive constants $0 < \mu_1 < 1$ and $0 < \mu_2 < 1$ are constants chosen by the designer. ■

The previous corollary shows that for linear systems with a static state feedback controller 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. An immediate conclusion is that if all of the assumptions mentioned in Corollary 1 hold and the quantizer of the function $g(x)$ has infinite range, then system (8) 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.

VI. Illustrative Example

In this section, we apply the results of the previous sections to a nonlinear system example. For simplicity, the following first order nonlinear system is considered:

$$x^+ = -1.73\sqrt{|x|} + 0.5x + u, \tag{15}$$

where $x \in \mathbb{R}$ is the state of the system and $u \in \mathbb{R}$ is the input of the system. We design a static state feedback control law $u = 1.73\sqrt{|x|}$ to asymptotically stabilize the origin of (15).

Following the steps in Algorithm 1, we simulate the behaviour of the closed loop system with encrypted measurements with different key lengths to compare the performance and computation time to finish the whole encryption-decryption processes when different key lengths are used. In order to apply our main results, one first needs to verify that the Assumptions made in Section V are satisfied. It can be noticed that Assumption 2 is satisfied by $V(x) = x^2$, $\alpha_1(s) = \alpha_2(s) = s^2$ and $\alpha_3(s) = 0.75s^2$. And Assumption

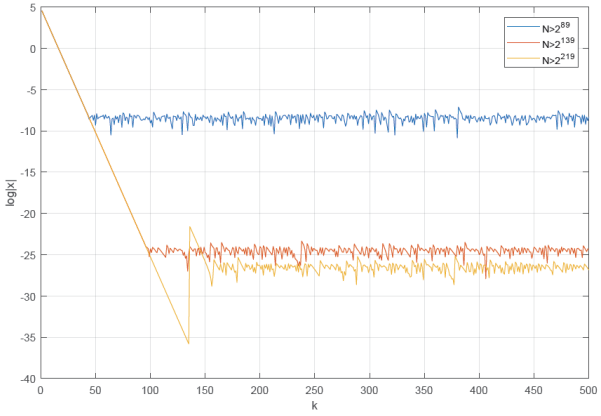

Fig. 3. Trajectories of the state with different key lengths

3 holds with $L_f = 1$. The total computational times for systems using encryption with different key lengths are shown below in TABLE I. 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. Due to space limitations, only the first 3 corresponding trajectories of TABLE I are shown in Fig. 3 in base 10 logarithmic scale.

TABLE I

KEY LENGTHS AND COMPUTATION TIMES

Key Length (bits)	89	139	219	512	640
Computation Time (ms)	3.51	10.13	35.92	317.13	745.36

It is clear that the control gain 1.73 $(n_1 - m_1 - 1 = 1)$ can not be finitely represented in base 2, therefore, it can not be implemented directly and must be quantized following the steps shown in Algorithm 1. So, the precision level for the gain also has an impact on the ultimate bound of the state, as shown in Fig. 3. The coarsest levels required for quantization from top to bottom are 2^{-30} $(m_1 = 30)$ for the gain and 2^{-40} $(m_2 = 40)$ for the state measurement, 2^{-80} $(m_1 = 80)$ for the gain and 2^{-40} $(m_2 = 40)$ for the state measurement and 2^{-80} $(m_2 = 80)$ for the gain and 2^{-120} $(m_2 = 120)$ for the state measurement, respectively. Obviously, longer key length in general leads to smaller ultimate bound for the state. In this example, $n_y = 1$. The initial state is fixed at $x = 35000$ $(n_2 - m_2 - 1 = 16)$ in this particular example, which leads to the 3 different key lengths being 89, 139 and 219 bits. If one needs to deal with much larger initial states, even longer key lengths may be needed according to Theorem 1 for general nonlinear systems.

VII. CONCLUSION AND FUTURE WORK

We have investigated a scenario in which a discrete-time static controller and a discrete-time plant are connected via a network. And to ensure the security and privacy of the NCS, Paillier encryption is used to encrypt the state measurement. 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. The results have been applied to linear time-invariant systems to recover the main result in [2].

Future work will focus on considering the effect of disturbances on the closed loop systems, investigation of the possibilities to achieve global asymptotic stability by dynamic quantization, see [12] and [13] for instance. Moreover, it is also of interest to apply these results to NCSs modelled by hybrid systems and to look at the ways of implementing dynamic controllers.

REFERENCES

[1] P. Antsaklis and J. Baillieul. Special issue on technology of networked control systems. *Proceedings of the IEEE*, vo. 95, no. 1, pp. 5-8, 2007.
[2] F. Farokhi, I. Shames and N. Batterham, Secure and private cloudbased control using semi-homomorphic encryption, *Control Engineering Practice*, vol. 67, pp. 13-20, 2017.
[3] T.E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *In Proceedings of CRYPTO 84*, vol. 196, pp. 10-18, 1984.
[4] C. Gentry, *A fully homomorphic encryption schemes*, Ph.D. Thesis, Stanford University, 2009.
[5] J.P. Hespanha, P. Naghshtabrizi, and Y. Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138-162, 2007.
[6] Z.P. Jiang and Y. Wang, Input-to-state stability for discrete-time nonlinear systems, *Automatica*, vol. 37, pp. 857-869, 2001.
[7] Z.P. Jiang and Y. Wang, A converse Lyapunov theorem for discrete-time systems with disturbances, *Systems & Control Letters*, vol. 45, no. 1, pp. 49-58, 2002.
[8] 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*, vol. 44, no. 3, pp. 777-800, 2005.
[9] H.K. Khalil. *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.
[10] M. Kishida. Encrypted Control System with Quantizer. https://arxiv.org/abs/1807.06717.
[11] 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*, pp. 6836-6843, 2015.
[12] D. Liberzon. Hybrid feedback stabilization of systems with quantized signals, *Automatica*, vol. 39, pp. 1543-1554, 2003.
[13] D. Liberzon and D. Nešić. Input-to-state stabilization of linear systems with quantized state measurements, *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 767-781, 2007.
[14] Y. Lu and M. Zhu. Privacy preserving distributed optimization using homomorphic encryption, *Automatica*, vol. 96, pp. 314-325, 2018.
[15] Y. Mo and B. Sinopoli. Secure Control Against Replay Attacks, *In Proceedings of the 47th annual Allerton conference on communication, control, and computing*, pp. 911-918, 2009.
[16] 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)*, pp. 223-238, 1999.
[17] P. Paillier. Composite-residuosity based cryptography-an overview. *Cryptobytes*, vol. 5, no. 1, pp. 20-26, 2002.
[18] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.
[19] A. Teixeira, I. Shames, H. Sandberg, and K.H. Johansson, A secure control framework for resource-limited adversaries, *Automatica*, vol. 51, pp. 135-148, 2015.
[20] 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*, vol. 48, pp. 1144-1153, 2012.
[21] L. Zhang, H. Gao and O. Kaynak, Network-Induced Constraints in Networked Control Systems-A Survey, *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 403-416, 2013.