Secure and Private Control Using Semi-Homomorphic Encryption ☆,☆☆

Farhad Farokhi[a], Iman Shames[a], Nathan Batterham[a]

[a] *Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, VIC 3010, Australia*

Abstract

Networked control systems with encrypted sensors measurements is considered. Semi-homomorphic encryption, specifically the Paillier encryption, is used so that the controller can perform the required computation on the encrypted data. Conditions on the parameters of the encryption technique are provided that guarantee the stability and the performance of the closed-loop system. The results are subsequently extended Laplacian based distributed systems, such as formation-seeking algorithms. It is shown that the problem of figuring out the state measurements of the neighbouring agents of a compromised agent upon using the proposed algorithm is numerically intractable.

Keywords: Networked control system; Privacy; Security; Semi-homomorphic encryption; Paillier method.

1. Introduction

Recent technological advances in communication engineering have facilitated the design and the deployment of large-scale systems that are remotely monitored and controlled. Modern infrastructures, such as smart grids and intelligent transportation systems, are examples of such systems. The massive size of the collected data and the computational power required for operating these systems have motivated outsourcing estimation and control tasks to third-party platforms, namely, the cloud-computing companies. This allows the system operator to save considerably in terms of the required infrastructure and the budget for expanding the system. Although very desirable, relying on third-party computation is not without its perils. Cyber-security threats and invasion of privacy of the users are just two examples of the sort of problems arising in this context [2–4].

Cyber-security attacks can be decomposed into various categories based on the type and the amount of the resources that the attacker uses to achieve its goal [3]. Eavesdropping is one of the most basic attacks that requires relatively low amount of resources. This attack also serves as a starting point for many more sophisticated attacks [5]. In eavesdropping attacks, the adversary listens to the communication channel between the sensors, the controller, and the actuator to extract valuable information about the model and the controller based on the transmitted data. Encryption is a tool that is widely utilized to combat such attacks. A typical control loop with encryption-decryption units is shown in Figure 1. The sensor and the controller encrypt their signals before transmitting them through the communication network. This technique is good for making eavesdropping attacks difficult over the communication channel, i.e., points A and B in Figure 1. However, the encryption is useless if the cloud-computing platform is compromised, i.e., if the attacker has access to points C, D, and E in Figure 1. Privacy breaches also often happen inside the cloud-computing services, where a third-party service provider or an adversary agent can reconstruct the private data of the participants or the infrastructure. Hence, encryption techniques in the networked systems of the form in Figure 1 are not effective for these privacy breaches. In light of these observations, it is desirable to use encryption techniques, such as semi-homomorphic encryption, that do not require the data to be decrypted before entering the cloud-computing services. Thus, reducing the risks of cyber-security attacks and privacy breaches in points C, D, and E in Figure 1.

In this paper, a networked control loop of the form of Figure 2 is closely studied. Homomorphic encryption is a form of encryption that allows the controller (on the cloud-computing platform) to carry out the necessary computations on encrypted data. Semi-homomorphic encryption are a simpler form of homomorphic encryption that only allow for a category of operations to be performed on the encrypted data. For instance, the Paillier method [6], which is a semi-homomorphic encryption technique, allows summation of plain data to be performed by multiplication of the encrypted ones. On contrary, ElGamal encryption [7] allows the multiplication of plain data using the multiplication of the encrypted data. In contrast, fully-homomorphic encryption schemes, such as Gentry's en-

☆ An early version of this paper was presented at the 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems [1]. Corresponding author F. Farokhi.

☆☆ The work was supported by a McKenzie Fellowship, an early career grant from Melbourne School of Engineering, ARC grant LP130100605, and Defence Science and Technology Group through the Research Agreement MyIP:6288.

Email addresses: ffarokhi@unimelb.edu.au (Farhad Farokhi), ishames@unimelb.edu.au (Iman Shames), n.batterham@student.unimelb.edu.au (Nathan Batterham)

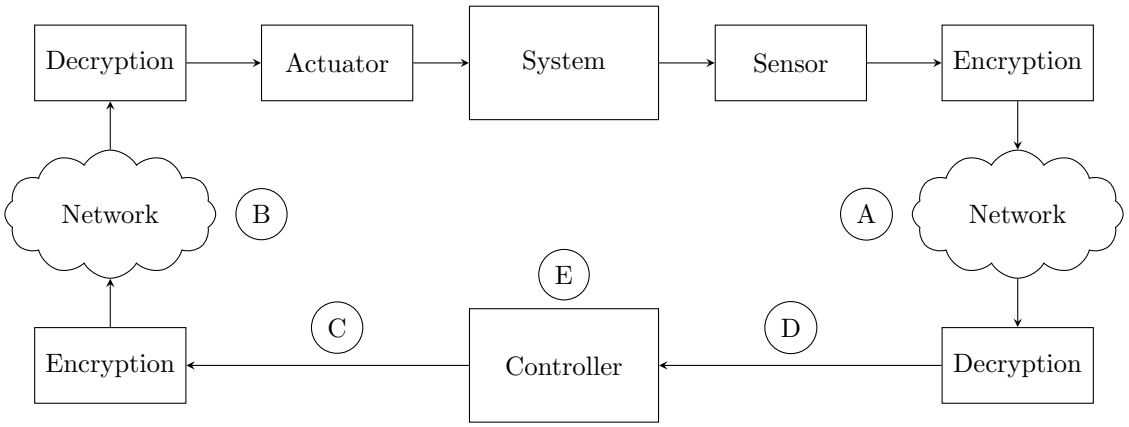

Figure 1: The schematic diagram of a networked control system with encryption-decryption units.

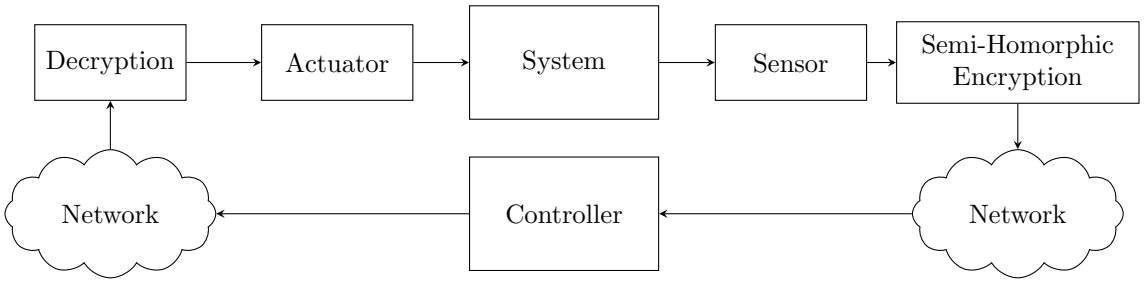

Figure 2: The schematic diagram of a networked control system with semi-homomorphic encryption-decryption units.

cryption [8], allow for both multiplication and summation of plain data through appropriate arithmetic operations on the encrypted data.

In this paper, the Paillier encryption technique is used for secure and private computation of control laws using untrusted cloud-computing platforms. Specifically, the parameters of the Paillier encryption technique are determined so that the stability of the closed-loop system and its closed-loop performance can be guaranteed. The results are subsequently extended Laplacian based distributed systems, such as formation-seeking algorithms. It is shown that the problem of figuring out the state measurements of the neighbouring agents of a compromised agent upon using the proposed algorithm is numerically intractable.

This is not the first time that the semi-homomorphic or homomorphic encryption schemes are utilized when using third-party cloud-computing services; e.g., see [9–13] and the references there-in. However, none of these studies, except [13], have considered these techniques in networked control system. In addition, in [13], only a framework for using semi-homomorphic encryption in networked control systems is developed and practical aspects, such as ensuring stability and maintaining the closed-loop performance of the system, are not studied. Further, these results have not addressed the possibility of using homomorphic encryption in distributed systems for securing the communications from possible adversaries through compromised agents.

The rest of the paper is organized as follows. First, background materials on fixed-point arithmetic and semi-homomorphic encryptions are presented in Section 2. The control strategy is discussed in Section 3. The results are generalized to Laplacian based distributed systems in Section 4. Numerical examples are provided in Section 5 and the paper is concluded in Section 6.

2. Background materials

2.1. Fixed-point arithmetic

The objects of interest, in this paper, are signed fixed-point rational numbers in base 2, such as

$$\pm \underbrace{c_{n-1}c_{n-2}\cdots c_{m+1}}_{\text{integer bits}} . \underbrace{c_m c_{m-1}\cdots c_1}_{\text{fractional bits}}$$

for given integers $n, m \in \mathbb{N}$ such that $m \leq n$. The set of all such numbers can be denoted by

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

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 2^{-m}. Although conceptually useful, these fixed-point

rationals need to be transformed into integers so that a digital processor can use them. To do so, define the mapping $f_{n,m} : \mathbb{Q}(n,m) \to \mathbb{Z}_{2^n}$ such that $f_{n,m}(b) = 2^m b \bmod 2^n$ for all $b \in \mathbb{Q}(n,m)$. The notation $\mathbb{Z}_q$ denotes the set of integers modulo q for all $q \in \mathbb{N}$. Moreover, define the inverse mapping $f^{-1}_{n,m} : \mathbb{Z}_{2^n} \to \mathbb{Q}(n,m)$ such that $f^{-1}_{n,m}(a) = (a - 2^n \mathbb{1}_{a \geq 2^{n-1}})/2^m$ for all $a \in \mathbb{Z}_{2^n}$, where $\mathbb{1}_p$ is a characteristic function that is equal to one if the statement p holds true and equal to zero otherwise.

Proposition 1. *The following two statements are valid:*

1. $f^{-1}_{n,m}(f_{n,m}(b)) = b$ *for all* $b \in \mathbb{Q}(n,m)$;
2. $f_{n,m}(f^{-1}_{n,m}(a)) = a$ *for all* $a \in \mathbb{Z}_{2^n}$.

Proof. See Appendix A. □

This proposition shows that $\mathbb{Q}(n,m)$ is isomorph to $\mathbb{Z}_{2^n}$ and thus every operation in the set of signed fixed-point rationals $\mathbb{Q}(n,m)$ can be translated into an operation in the set of integers modulo 2^n and *vice versa*. This relationship is explored in detail in the following proposition. Noting that n and m are clear from the context, with slight abuse of notation, in this proposition, f and f^{-1} are used instead of $f_{n,m}$ and $f^{-1}_{n,m}$, respectively.

Proposition 2. *The following identities hold:*

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

Proof. See Appendix B. □

For the ease of the presentation of the operations in $\mathbb{Z}_{2^n}$, the following operators for all $a, a' \in \mathbb{Z}_{2^n}$ are defined:

$$a \overset{n}{\oplus} a' = (a + a') \bmod 2^n,$$
$$a \overset{n}{\ominus} a' = (2^n + a - a') \bmod 2^n,$$
$$a \underset{m}{\overset{n}{\otimes}} a' = ((a - 2^n \mathbb{1}_{a \geq 2^{n-1}})(a' - 2^n \mathbb{1}_{a' \geq 2^{n-1}})/2^m) \bmod 2^n.$$

The following properties can be proved for these new operators.

Corollary 1. *The following identities hold:*

1. *For all* $b, b' \in \mathbb{Q}(n,m)$ *such that* $b + b' \in \mathbb{Q}(n,m)$, $f_{n,m}(b+b') = f_{n,m}(b) \overset{n}{\oplus} f_{n,m}(b')$;
2. *For all* $b \in \mathbb{Q}(n,m)$ *such that* $-b \in \mathbb{Q}(n,m)$, $f_{n,m}(-b) = 0 \overset{n}{\ominus} f_{n,m}(b)$;
3. *For all* $b, b' \in \mathbb{Q}(n,m)$ *such that* $b - b' \in \mathbb{Q}(n,m)$, $f_{n,m}(b-b') = f_{n,m}(b) \overset{n}{\ominus} f_{n,m}(b')$;
4. *For all* $b, b' \in \mathbb{Q}(n,m)$ *such that* $bb' \in \mathbb{Q}(n,m)$, $f_{n,m}(bb') = f_{n,m}(b) \underset{m}{\overset{n}{\otimes}} f_{n,m}(b')$.

Proof. The proof directly follows from the application of Proposition 2. □

The multiplication is more difficult to implement in comparison to the summation as the sign of the operands (i.e., the numbers on which the operators act) needs to be checked. This creates difficulties in the subsequent sections (as the sign of encrypted numbers cannot be checked). Interestingly, this difficulty is caused by the existence of the fractional bits. The following properties of the multiplication are used in the subsequent sections to overcome the difficulty of implementing it.

Proposition 3. *The following properties are valid:*

1. $a \underset{0}{\overset{n}{\otimes}} a' = aa' \bmod 2^n$;
2. $a \underset{m}{\overset{n}{\otimes}} a' = (aa'/2^m) \bmod 2^n$ *if* $2^m | a'$ *and* $a' < 2^{n-1}$.

Proof. See Appendix C. □

Note that if a is divisible by 2^m then $f^{-1}_{n,m}(a)$ is an integer. Therefore, the complexity of the implantation can be reduced by ensuring that one of the numbers is positive and that its fixed-point representation is integer. Finally, the following useful property can be used for cases where $m \neq 0$.

Proposition 4. *For all* $b, b' \in \mathbb{Q}(n,m)$ *such that* $bb' \in \mathbb{Q}(n,m)$,

$$f_{n+2m,0}(2^{2m} bb') = f_{n+2m,0}(2^m b) \underset{0}{\overset{n+2m}{\otimes}} f_{n+2m,0}(2^m b).$$

Proof. See Appendix D. □

The result of Proposition 4 is particularly useful as the implementation of the operation $\underset{0}{\overset{n+2m}{\otimes}}$ does not require comparisons (see Proposition 3) in contrast to implementation of $\underset{m}{\overset{n}{\otimes}}$.

2.2. Semi-homomorphic encryption

In this subsection, a simple semi-homomorphic encryption scheme, namely, the Paillier encryption technique, is introduced. This technique relies on Decisional Composite

Residuosity Assumption[1] [6]. The encryption scheme is as follows:

- 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 $\lambda = \operatorname{lcm}(p-1, q-1)$ and $\mu = \lambda^{-1} \bmod N$, where $\operatorname{lcm}(a, b)$ refers to 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 ciphertext of a message $t \in \mathbb{Z}_N$ as $E(t; r) = (N+1)^t r^N \bmod N^2$.
- Decryption:
  - For any ciphertext $c \in \mathbb{Z}_{N^2}$, the plain text is given by $D(c) = L(c^\lambda \bmod N^2)\mu \bmod N$, where $L(x) = (x-1)/N$.

In the Paillier encryption scheme, N is the public key (i.e., it is shared with all the parties and is used for encryption) and the pair (λ, μ) is the private key (i.e., only the entity that needs to decrypt the data has access to it). Following [6], an important (and obvious) property of the this system is that

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

This shows that there is an invertible relationship between the encrypted texts and the plain text. The following important properties can be proved to establish that the Paillier is a semi-homomorphic encryption scheme.

Proposition 5. *The following identities hold:*

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

Proof. See Appendix E. □

These two properties provide an opportunity to perform calculations on the encrypted data. However, noting that it is impossible to check the sign of an encrypted number, multiplication is not easy to implement. The following result identifies a few cases in which the multiplication is implementable.

[1]Decisional Composite Residuosity Assumption refers to that given integers $N \in \mathbb{Z}$ and $x \in \mathbb{Z}_{N^2}$, it is "hard" to decide whether there exists $y \in \mathbb{Z}_{N^2}$ such that $x \equiv y^N \bmod N$. This is equivalent to that the decryption without access to the private key is computationally impossible unless P=NP.

Proposition 6. *Assume that $N > 2^n$. For all $r \in \mathbb{Z}_N^*$ and $a, a' \in \mathbb{Z}_{2^n}$, the following statements are valid:*

1. *$D((E(a; r)^{a'} \bmod N^2)^\theta \bmod N^2) \bmod 2^n = a \overset{n}{\underset{m}{\otimes}} a'$ with $\theta = 2^{-m} \bmod N$, if $a \overset{n}{\underset{m}{\otimes}} a' \in \mathbb{Z}_{2^n}$, $a, a' < 2^{n-1}$, and $\gcd(2^m, N) = 1$;*
2. *$D(E(a; r)^{a'/2^m} \bmod N^2) \bmod 2^n = a \overset{n}{\underset{m}{\otimes}} a'$ if $a \overset{n}{\underset{m}{\otimes}} a' \in \mathbb{Z}_{2^n}$, $2^m | a'$, and $a' < 2^{n-1}$;*
3. *$D(E(a; r)^{a'} \bmod N^2) \bmod 2^n = a \overset{n}{\underset{0}{\otimes}} a'$ if $a \overset{n}{\underset{0}{\otimes}} a' \in \mathbb{Z}_{2^n}$.*

Proof. See Appendix F.

Proposition 6 requires that the outcome of the multiplication does not overflow (i.e., it does not become large than Z_{2^n}). Since checking overflows are not possible when working with the encrypted data, it is up to the designer to select a large enough set of fixed point rationals so that the outcome of all the algebraic computations stays inside the same set.

With these background material in hand, the control architecture is presented in the next section.

3. Control architecture

Consider the discrete-time linear time-invariant dynamical system of the form

$$x[k+1] = Ax[k] + Bu[k],\ x[0] = x_0, \tag{1a}$$
$$y[k] = Cx[k], \tag{1b}$$

where $x[k] \in \mathbb{R}^{p_x}$ denotes the state, $u[k] \in \mathbb{R}^{p_u}$ denotes the control input, and $y[k] \in \mathbb{R}^{p_y}$ denotes the outputs measured by the sensors. The controller takes the form of

$$u[k] = Ky[k]. \tag{2}$$

Throughout this paper, the following assumption is made.

Assumption 1. *There exists $\bar{K} \in \mathbb{R}^{p_u \times p_y}$ such that $A + B\bar{K}C$ is Schur, i.e., all the eigenvalues of $A + B\bar{K}C$ are inside the unit circle in the complex plane.*

Conditions for checking the validity of this assumption as a function of the model matrices and their sparsity patterns are given in [14, 15]. To be able to implement the control law in (2) on digital computers, one needs to restrict the control gain to be in the set $\mathbb{Q}(n_1, m_1)^{p_u \times p_y}$ for some appropriately selected parameters $n_1, m_1 \in \mathbb{N}$. The existence of such quantized control gains is ensured by that the eigenvalues of a matrix are continuous functions of the entries of the matrix [16, p. 88-89]. In fact, the continuity shows that, for any $\bar{K} \in \mathbb{R}^{p_u \times p_y}$ such that $A + B\bar{K}C$ is Schur, there exists $\epsilon(\bar{K}) > 0$ such that $A + BKC$ is Schur if $\|K - \bar{K}\|_F \leq \epsilon(\bar{K})$. The following results can be proved.

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

Require: n_1, m_1, n_2, m_2, $\bar{K}$, $y[k]$, p, q
Ensure: $u[k]$
Set $n = p_y + n_1 + n_2$ and $m = m_1 + m_2$
\# Control designer
Compute $K \in \arg\min_{K' \in \mathbb{Q}(n_1,m_1)^{p_u \times p_y}} \|K' - \bar{K}\|_F$
Transmit $\Gamma_{ji} = f_{n+2m,0}(2^m K_{ji})$ to the controller
\# Sensors
for $i = 1, \ldots, p_y$ **do**
  Construct $\tilde{y}_i[k]$ by projecting $y_i[k]$ in $\mathbb{Q}(n_2, m_2)$
  Transmit $z_i = E(f_{n+2m,0}(2^m \tilde{y}_i[k]); r)$ to the controller
end for
\# Controller
for $j = 1, \ldots, p_u$ **do**
  Set $\ell_j[k] = z_1^{\Gamma_{j1}} \bmod N^2$
  for $i = 2, \ldots, p_y$ **do**
    Compute $\ell_j[k] = (\ell_j[k](z_i^{\Gamma_{ji}} \bmod N^2)) \bmod N^2$
  end for
  Transmit $\ell_j[k]$ to the actuators
end for
\# Actuators
for $j = 1, \ldots, p_u$ **do**
  Implement $u_j[k] = D(\ell_j[k]) \bmod 2^{n+2m}/2^{2m}$
end for

Proposition 7. *Let $\bar{K} \in \mathbb{R}^{p_u \times p_y}$ such that $A + B\bar{K}C$ is Schur. Let $K \in \arg\min_{K' \in \mathbb{Q}(n_1,m_1)^{p_u \times p_y}} \|K' - \bar{K}\|_F$ for $m_1 \geq \lceil -\log_2(\epsilon(\bar{K})/\sqrt{p_u p_y}) \rceil$ and $n_1 \geq \lceil m_1 + 1 + \log_2(\max_{i,j} |\bar{K}_{ij}|) \rceil$. Then, $A + BKC$ is Schur.*

Proof. See Appendix G. □

In addition to quantizing the controller parameters, the output of the system needs to be also quantized. Let $\tilde{y}[k]$ denoted the quantized version of the output $y[k]$, that is,

$$\tilde{y}[k] = \min_{z \in \mathbb{Q}(n_2,m_2)^{p_y}} \|z - y[k]\|_2,$$

for appropriately selected $n_2, m_2 \in \mathbb{N}$. To be able to properly quantize the output, it should be proved that it stays bounded.

Proposition 8. *Assume that $A + BKC$ is Schur. There exists $M(x_0) > 0$ such that $y[k] \in [-M(x_0), M(x_0)]^{p_y}$ for the system (1) with controller $u[k] = K\tilde{y}[k]$ if $n_2 \geq \lceil m_2 + 1 + \log_2(M(x_0)) \rceil$.*

Proof. See Appendix H. □

The control designer, the sensors, the controller (which is implemented on the cloud), and the actuators can follow Algorithm 1 to ensure the private and secure implementation of the static control law in (2).

Theorem 1. *Let $\bar{K} \in \mathbb{R}^{p_u \times p_y}$ be such that $A + B\bar{K}C$ is Schur. Assume*

$$N > 2^{p_y + n_1 + n_2}, \tag{3a}$$
$$m_1 \geq \lceil -\log_2(\epsilon(\bar{K})/\sqrt{p_u p_y}) \rceil, \tag{3b}$$
$$n_1 \geq \lceil m_1 + 1 + \log_2(\max_{i,j} |\bar{K}_{ij}|) \rceil, \tag{3c}$$
$$n_2 > \lceil m_2 + 1 + \log_2(M(x_0)) \rceil. \tag{3d}$$

Then $\lim_{k \to \infty} \operatorname{dist}(x[k], \mathcal{B}(2^{-m_2}\xi)) = 0$, where $\xi > 0$ is a constant[2], if the controller is calculated by Algorithm 1.

Proof. See Appendix I. □

Remark 1. (Stability and Performance). *Theorem 1 proves that the closed-loop system is practically stable (rather than asymptomatic stability). This is due to the effect of the quantization. This theorem further relates the performance of the system to m_2, the resolution of the quantization of the output measurements $y[k]$. By increasing this resolution, the performance can be improved arbitrarily.*

Remark 2. (Computational Complexity and Communication Overhead). *The computation cost of the encryption and decryption algorithms scale[3] as $\mathcal{O}(N^3)$ because the most burdensome computation in both cases is calculating exponential operations. Each multiplication is Algorithm 1 costs $\mathcal{O}(N^2)$ operations and each exponentiation costs $\mathcal{O}(N^3)$ operations. Therefore, assuming that $p_u, p_y = \mathcal{O}(1)$, i.e., constants independent of N, the overall computational complexity of Algorithm 1 scales as $\mathcal{O}(N^3)$. In addition, note that instead of sending packets of the size n, the communication involves transmitting packets of the length $\mathcal{O}(N)$. Finally, recall that N itself scales exponentially with n, i.e., $N = \mathcal{O}(2^n)$. This exponential increase in the computational complexity and communication overhead can be interpreted as the cost of privacy and security in networked control systems.*

Remark 3 (Privacy and Security). *The problem of breaking the Paillier's encryption and thus, in the setup of Algorithm 1, figuring out the state measurements $y[k]$ from all z_i and ℓ_j is numerically intractable under Decisional Composite Residuosity Assumption if the key length is selected large enough. In fact, it can be proved that any probabilistic polynomial-time adversary (i.e., an adversary with extremely high, yet reasonable, computational ability; see [17, p. 187] for a proper definition) can only infer the correct $\tilde{y}_i[k]$ from all the communicated messages (i.e., z_i and ℓ_i) with probability 2^{-n_2} plus a negligible function[4]*

[2] $\xi = (c_1 + c_2)(1/\lambda_{\min}(Q) + 1/\lambda_{\min}(P))$ where P, Q, c_1, and c_2 are defined in the proof of Proposition 8.

[3] We say $f_1(N)$ scales as $\mathcal{O}(f_2(N))$ if $\lim_{N \to \infty} f_1(N)/f_2(N) = c < \infty$.

[4] A function $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is called negligible if, for any $c \in \mathbb{N}$, there exists $n_c \in \mathbb{N}$ such that $f(n) \leq 1/n^c$ for all $n \geq n_c$ [18].

Algorithm 2 Secure and private implementation of the static controller with encrypted control parameters.

Require: n_1, m_1, n_2, m_2, $\bar{K}$, $y[k]$, p, q
Ensure: $u[k]$
1: Set $n = p_y + n_1 + n_2$ and $m = m_1 + m_2$
2: # Control designer
3: Compute $K \in \arg\min_{K' \in \mathbb{Q}(n,m)^{p_u \times p_y}} \|K' - \bar{K}\|_F$
4: Transmit $\Gamma_{ji} = E(f_{n+2m,0}(2^m K_{ji}); r)$ to the controller
5: # Sensors
6: **for** $i = 1, \ldots, p_y$ **do**
7: Construct $\tilde{y}_i[k]$ by projecting $y_i[k]$ in $\mathbb{Q}(n, m)$
8: Transmit $\bar{y}_i[k] = f_{n+2m,0}(2^m \tilde{y}_i[k])$ to the controller
9: **end for**
10: # Controller
11: **for** $j = 1, \ldots, p_u$ **do**
12: Set $\ell_j[k] = \Gamma_{j1}^{\bar{y}_1[k]} \bmod N^2$
13: **for** $i = 2, \ldots, p_y$ **do**
14: Compute $\ell_j[k] = (\ell_j[k](\Gamma_{ji}^{\bar{y}_i[k]} \bmod N^2)) \bmod N^2$
15: **end for**
16: Transmit $\ell_j[k]$ to the actuators
17: **end for**
18: # Actuators
19: **for** $j = 1, \ldots, p_u$ **do**
20: Implement $u_j[k] = D(\ell_j[k]) \bmod 2^{n+2m}/2^{2m}$
21: **end for**

of the key length. This is a direct consequence of the semantic security, also known as Indistinguishability under Chosen Plaintext Attack (IND-CPA), in [6]. Therefore, the probability that an adversary can infer the measurements (from all the encrypted communications and computations) is equal to 2^{-n_2} for large enough key lengths. Note that 2^{-n_2} is equal to the probability of guessing a measurement without the basis of any observations. Therefore, the adversary cannot gain anything from having access to the encrypted measurements.

Contrary to the previously-described scenario, it could be of interest to encrypt the controller parameters instead of the output measurements. This could be because of that the controller is a trade secret and needs to be kept privately while outsourcing the computational aspects to the cloud services. Algorithm 2 describes the procedure that the sensors, the controller (on the cloud), and the actuators must follow to ensure the controller parameters are protected.

Theorem 2. *Let $\bar{K} \in \mathbb{R}^{p_u \times p_y}$ be such that $A + B\bar{K}C$ is Schur. Assume that the conditions in* (3) *hold. Then $\lim_{k\to\infty} \operatorname{dist}(x[k], \mathcal{B}(2^{-m_2}\xi)) = 0$, where $\xi > 0$ is a constant, if the controller is calculated by Algorithm 2.*

Proof. The proof is similar to the that of Theorem 1. □

4. Laplacian based distributed systems

Consider a network comprised of J nodes. The interconnection of these nodes can be captured by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $i \in \mathcal{V} = \{1, \ldots, J\}$ and $\mathcal{E}$ being the vertex set and the set of directed edges, respectively, where the directed edge $(i, j) \in \mathcal{E}$ if the dynamics of node j depends on node i. We call a graph $\mathcal{G}$ *strongly connected* if it is possible to reach any $i \in \mathcal{V}$ starting from any $j \in \mathcal{V}$ by traversing edges in their direction(s). We have the following standing assumption.

Assumption 2. *The graph $\mathcal{G}$ is strongly connected.*

The dynamics of each node $\mathcal{V}$ of a vast majority of such networks (see, e.g., [19–22]) is of the following form

$$x_i[k+1] = A_i x_i[k] + \tau\,(v_i[k] + u_i[k]) \tag{4}$$

$$v_i[k] = -\sum_{j \in \mathcal{N}_i} v_{ji}[k] \tag{5}$$

$$v_{ji}[k] = w_{ji}[k]\,(x_j[k] - x_i[k]) \tag{6}$$

where $x_i[k] \in \mathbb{R}^{p_{xi}}$ denotes the state of system i, $u[k] \in \mathbb{R}^{p_{ui}}$ denotes the control input of node i, $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\}$, $w_{ji}[k] \in (0, w_{\max}]$, $\forall i, j \in \mathcal{V}$ and $k \geq 0$ with $w_{\max}$ being a bounded positive real number, and τ is some appropriately selected sampling time.

Remark 4. *Assumption 2 is sufficient for the guaranteeing the convergence of the systems whose dynamics are of the type described by* (4)-(6). *This assumption is presented for the sake of simplicity of the exposition and can be relaxed to include the cases where the network is time-varying. However, this will have no impact on the discussion presented next.*

Note that while i in principle does not require the states of all its neighbours explicitly to evaluate (5), in practice these values are revealed, i.e., only the difference of the states is required to evaluate the control law rather than absolute state measurements. This poses a security risk due to the fact that if node i is compromised by an adversary, the states of all its neighbours are revealed to the adversary as well. In what follows, a mechanism to remedy this security vulnerability is described. First, we assume that each $j \in \mathcal{N}_i$ has access to N_i, i.e. the public key of node i. At each time step k, i transmits $E_i(\bar{x}_i^-[k]; r_{ij}[k])$ to $j \in \mathcal{N}_i$ where $\bar{x}_i^-[k] = f_{n+2m,0}(-2^m \tilde{x}_i[k])$, $\tilde{x}_i[k]$ is the projection of $x_i[k]$ onto $\mathbb{Q}(n, m)$, and random $r_{ij}[k] \in \mathbb{Z}_{N_i}^\star$. Agent j in turn picks a random $w_{ji}[k] \in (0, w_{\max}]$ and computes $\tilde{w}_{ji}[k]$, i.e. the projection of $w_{ji}[k]$ onto $\mathbb{Q}(n, m)$. It then transmits $e_{ij}[k]^{\bar{w}_{ji}[k]} \bmod N_i^2$ back to i, where

$$e_{ij}[k] = E_i(\bar{x}_i^-[k]; r_{ij}[k]) E_i(\bar{x}_j^+[k]; \rho_{ji}[k]) \bmod N_i^2, \tag{7}$$

with random $\rho_{ji}[k] \in \mathbb{Z}_{N_i}^\star$, $\bar{x}_j^+[k] = f_{n+2m,0}(2^m \tilde{x}_j[k])$, $\bar{w}_{ji}[k] = f_{n+2m,0}(2^m \tilde{w}_{ji}[k])$, and $\tilde{x}_j[k]$ being the projection of $x_j[k]$ onto $\mathbb{Q}(n, m)$. Agent i decrypts this message

and obtains $v_{ji}[k]$ after dividing the decrypted value by 2^{2m} without explicitly knowing $\bar{x}_j^+$ (or in fact $x_j[k]$). In summary, the secure implementation of (4)-(6) is as the following:

$$x_i[k+1] = A_i x_i[k] + \tau\left(v_i[k] + u_i[k]\right) \tag{8}$$

$$v_i[k] = -\sum_{j\in\mathcal{N}_i} v_{ji}[k] \tag{9}$$

$$v_{ji}[k] = D_i(e_{ij}[k]^{\bar{w}_{ji}[k]} \bmod N_i^2)/2^{2m},\ \forall j \in \mathcal{N}_i, \tag{10}$$

where $D_i(c) = L_i(c^{\lambda_i} \bmod N_i^2)\mu_i \bmod N_i$, $L_i(d) = (d-1)/N_i$, and (λ_i, μ_i) are the private keys of node i, and $e_{ij}[k]$ is given in (7). In this new setup, if node i is compromised only a scaled difference between the state of i and its neighbours is immediately revealed to the adversary. We conclude this section by stating a few results for the case where node i is compromised by an adversary. Consequently, we assume that the adversarial node knows (λ_i, μ_i), $x_i[k]$, and $v_{ji}[k]$. Note that is due to the fact that the adversary is able to carry out the decryption step of (10). For the ease of exposition in what follows we make the following standing assumption.

Assumption 3. *The states $x_j[k]$, $j \in \{1,\dots,J\}$ are scalar.*

The adversary node then needs to find all the solutions to the following equation to be able to estimate the projection of $x_j[k]$ onto $\mathbb{Q}(n,m)$;

$$w(x - \tilde{x}_i[k]) = v_{ji}[k]. \tag{11}$$

where $w, x \in \mathbb{Q}(n,m)$. From [23] we know that (11) is NP-complete and the complexity bound[5] for finding all its solutions is equal to $\Theta\left(2^{2n}\right)$. However, one can make a stronger statement regarding the complexity of finding at least one pair (x,w) that satisfies (11). To this aim, one needs to cast (11) as integer linear equations.

Before continuing any further we define the following sets:

$$\Omega_{ji}^+ = \{(\varphi,\vartheta)|\varphi - \alpha_i^+\vartheta = \beta_{ji}, \varphi \in \mathbb{Z}_{2^{2n-1}-2^n}, \vartheta \in \mathbb{Z}_{2^{n-1}-1}\} \tag{12}$$

where $\alpha_i^+ = (\tilde{x}_i[k] + 2^{n-m})2^m$, $\beta_{ji} = 2^{2m}v_{ji}[k]$, and

$$\Omega_{ji}^- = \{(\varphi,\vartheta)|\varphi + \alpha_i^+\vartheta = -\beta_{ji}, \varphi \in \mathbb{Z}_{2^{2n-1}-2^n}, \vartheta \in \mathbb{Z}_{2^{n-1}-1}\} \tag{13}$$

where $\alpha_i^- = (\tilde{x}_i[k] - 2^{n-m})2^m$. Moreover, define χ_{ji} as the set of all solution pairs (x,w) of (11) with $x, w \in \mathbb{Q}(n,m)$. We have the following result.

[5]For positive functions $x(n)$ and $y(n)$ of integer number n we write $x(n) = \Theta(y(n))$ if there exist $c, c' > 0$ such that large enough n, $cy(n) \le x(n) \le c'y(n)$. For more details on $\Theta(\cdot)$ the reader may consult [23, Chapter 8].

Proposition 9. *The following statements are true.*

1. *For any $(x,w) \in \chi_{ji}$ there is a unique $(\varphi,\vartheta) \in \Omega_{ji}^+$ such that $\varphi = w(x + 2^{n-m})2^{2m}$ and $\vartheta = 2^m w$. Similarly for any $(\varphi,\vartheta) \in \Omega_{ji}^+$ there exists a unique $(x,w) \in \chi_{ji}$ such that $w = 2^{-m}\vartheta$ and $x = 2^{-m}\vartheta^{-1}\varphi - 2^{n-m}$.*
2. *For any $(x,w) \in \chi_{ji}$ there is a unique $(\varphi,\vartheta) \in \Omega_{ji}^-$ such that $\varphi = -w(x - 2^{n-m})2^{2m}$ and $\vartheta = 2^m w$. Similarly for any $(\varphi,\vartheta) \in \Omega_{ji}^+$ there exists a unique $(x,w) \in \chi_{ji}$ such that $w = 2^{-m}\vartheta$ and $x = -2^{-m}\vartheta^{-1}\varphi + 2^{n-m}$.*
3. *$|\chi_{ji}| = |\Omega_{ji}^+| = |\Omega_{ji}^-|$ where $|\cdot|$ denotes the cardinality of its argument.*

Proof. See Appendix J.

The following proposition introduces potentially smaller subsets of Ω_{ji}^+ and Ω_{ji}^- that contain at least one of the solutions to (12) or (13).

Proposition 10. *The following statements are true.*

1. *If $\Omega_{ji}^+ \neq \emptyset$ then there exists at least one pair $(\varphi,\vartheta) \in \Omega_{ji}^+$ such that $(\varphi,\vartheta) \in \Phi_{ji}^+$ where*

$$\Phi_{ji}^+ = \{(\varphi,\vartheta)|\varphi - \alpha_i^+\vartheta = \beta_{ji}, \varphi \in \mathbb{Z}_{\min(2^{2n-1}-2^n,\gamma_{ji}^+)}, \vartheta \in \mathbb{Z}_{\min(2^{n-1}-1,\gamma_{ji}^+)}\}, \tag{14}$$

$\gamma_{ji}^+ = 2\eta_{i+}^5(1 + |\beta_{ji}|)$, and $\eta_{i+} = \max(1, |\alpha_i^+|)$.

2. *If $\Omega_{ji}^- \neq \emptyset$ then there exists at least one pair $(\varphi,\vartheta) \in \Omega_{ji}^-$ such that $(\varphi,\vartheta) \in \Phi_{ji}^-$ where*

$$\Phi_{ji}^- = \{(\varphi,\vartheta)|\varphi + \alpha_i^-\vartheta = -\beta_{ji}, \varphi \in \mathbb{Z}_{\min(2^{2n-1}-2^n,\gamma_{ji}^-)}, \vartheta \in \mathbb{Z}_{\min(2^{n-1}-1,\gamma_{ji}^-)}\}, \tag{15}$$

$\gamma_{ji}^- = 2\eta_{i-}^5(1 + |\beta_{ji}|)$, and $\eta_{i-} = \max(1, |\alpha_i^-|)$.

Proof. The proof is a consequence of applying Theorem 13.4 of [23] to (12) and (13).

Remark 5. *Note that there is no guarantees that the feasible solution pairs that belong to Φ_{ji}^+ and Φ_{ji}^- correspond to the real values of $\tilde{x}_j[k]$ and $\tilde{w}_{ji}[k]$. But in the absence of any other known bounds on the solution of the integer linear programs of the type described above, in what follows, we limit our discussion to these solutions.*

In the absence of any other information (and if P $\neq$ NP), the computational complexity of finding the solutions promised in Proposition 10 is equal to $\gamma_{ji} = \Theta\left(\min\left(\psi_{ji}^+, \psi_{ji}^-, 2^{2n}\right)\right)$ where

$$\psi_{ji}^+ = \min(2^{n-1} - 1, \gamma_{ji}^+)\min(2^{2n-1} - 2^n, \gamma_{ji}^+),$$

and

$$\psi_{ji}^{-} = \min(2^{n-1}-1, \gamma_{ji}^{-}) \min(2^{2n-1}-2^{n}, \gamma_{ji}^{-}).$$

However, in the case where $\tilde{x}_i[k] \gg -2^{n-m-1}$, $\gamma_{ji} = \Theta\left(\min\left(\left(\gamma_{ji}^{-}\right)^2, 2^{2n}\right)\right)$ or if $\tilde{x}_i[k] \ll 2^{n-m-1} - 2^{-m}$ then $\gamma_{ji} = \Theta\left(\min\left(\left(\gamma_{ji}^{+}\right)^2, 2^{2n}\right)\right)$. These observations lead to the following result.

Proposition 11. *If node i is hacked by an adversary, then the computational complexity of the problem of finding one pair of feasible solutions of (11) is equal to $\Theta\left(\min\left(4(1+|\beta_{ji}|)^2, 2^{2n}\right)\right)$ if $\tilde{x}_i[k] = -2^{n-m-1}$ or $\tilde{x}_i[k] = 2^{n-m-1} - 2^{-m}$.*

Proof. Let $\tilde{x}_i[k] = -2^{n-m-1}$ (as the case where $\tilde{x}_i[k] = 2^{n-m-1} - 2^{-m}$ is identical). Then $\alpha_i^{+} = 0$, $\psi_{ji}^{+} = 2(1+|\beta_{ji}|)$, and consequently from Proposition 10 $\gamma_{ji} = \Theta\left(\min\left(4(1+|\beta_{ji}|)^2, 2^{2n}\right)\right)$.

Proposition 11 states the relative ease of finding at least one pair of feasible solutions of (11) if the hacked node has a state close to the boundaries of $\mathbb{Q}(m,n)$. From a control design perspective then it is necessary to ensure that n is chosen in such a way that $\tilde{x}_i[k]$ does not take any value close to the extrema of $\mathbb{Q}(n,m)$, i.e. -2^{n-m} or $2^{n-m}-2^{-m}$. For instance if n is selected in a way that $|\tilde{x}_i[k]| \leq \kappa$ for $\kappa \in \mathbb{Q}(n,m)$ and $k \geq 0$ then with similar arguments to those in the proof of Proposition 11 it can be seen that the smallest computational complexity of finding a pair of solutions of (11) becomes $\gamma_{ji} = \Theta\left(\min\left(\psi_{ji}^{+}, 2^{2n}\right)\right)$, where $\gamma_{ji}^{+} = 2\left(2^{m}(2^{n-m-1}-\kappa)\right)^5(1+|\beta_{ji}|))$. Selecting n in a way that $\kappa \ll 2^{n-m-1}$ renders the computational complexity of finding one pair of feasible solutions equal to that of finding all the solutions of (11), i.e. $\gamma_{ji} = \Theta\left(2^{2n}\right)$.

5. Experiment and numerical example

In this section, first, the application of Algorithm 1 to navigate a differential wheeled robot to a desired destination is demonstrated. The robot is a low-cost platform named GoPiGo developed by Dexter Industries. The computations are done locally on a Raspberry Pi 2 that is connected to the robot. The position of the centre of mass of the robot is measured using an OptiTrak camera system; see Figure 3. The speed references for each of the wheels are provided such that the robot travels with desired linear and angular velocities. Particularly, one can apply appropriate inputs to the wheels to choose between two modes of operations; (1) turn on the spot, (2) move on a direct line along the robot's heading direction, see [24, Chapter 13] for more information on the equations of motion for a differential wheeled robot. Let $x = [x_1, x_2]^\top$ and $\theta \in [-\pi, \pi]$ denote the position and the heading of the vehicle, respectively and τ is the sampling time. In this experiment sampling time is set to be equal to $0.1s$.

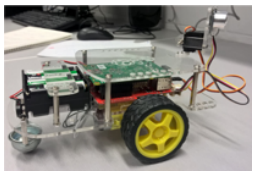

Figure 3: The experimental setup.

Moreover, v and ω are the linear and the angular velocities of the vehicle such that $|v| \leq v_{\max}$ and $|\omega| \leq \omega_{\max}$ with $v_{\max}$ and $\omega_{\max}$ being the maximum values for the linear and angular speeds. The desired destination is assumed to be $x_d = [0.9, 0.9]^\top$ and is provided by an external controller. It is assumed that x and x_d need to be encrypted with p and q being random prime numbers in $[2^{63}, 2^{64}]$. Moreover, $n = 10$ and $m = 5$. For security purposes, the reference planner and the sensor encrypt their messages and the external controller calculates and transmits $\Delta[k] = E(f_{n+2m,0}(2^m K(\tilde{x}_d - \tilde{x}[k])); r)$ (based on the encrypted data using Algorithm 1) to the robot at each step k where K is a random integer unknown to the robot. It is ensured that $\omega_{\max} \geq 2\pi/\tau$ and $v_{\max} \geq K(x_d - x[0])$. Under the aforementioned modes of operation where for the first half of the sampling time the robot turns on the spot and for the second half it travels along its heading, and in the light of this assumption the dynamics of the robot can be written as

$$x[k+1] = x[k] + \frac{\tau}{2}\nu[k] \tag{16}$$

$$\theta[k+1] = \theta[k] + \frac{\tau}{2}\omega_d[k] \tag{17}$$

where $\nu[k] = D(\Delta[k])$ and $\omega_d[k]$ is the smallest signed angle between $\theta[k]$ and $\theta_d[k] = \tan_2^{-1}(\nu[k])$ with $\tan_2^{-1}(\cdot)$ being the two argument inverse tangent of its vector argument. The trajectory of the centre of mass of the robot is depicted in Figure 4. A video of the experiment can also be accessed on YouTube[6]. Table 1 shows the computational time required for encryption, computing the control law (using the encrypted measurements), and decrypting the control signal for various key lengths (in bits). As expected the computational time increases with the key length; however, it is possible to perform all the required tasks if the key length is smaller than or equal 256 bits within 0.1 sec sampling time. For larger key lengths, sampling time should be increased, e.g., the sampling time should be increased to 0.25 sec if the key length is 512 bits.

Next, we consider the case where $J = 10$ mobile agents over a connected graph with dynamics

$$x_i[k+1] = x_i[k] + \tau v_i[k]$$

$$v_i[k] = -\sum_{j \in \mathcal{N}_i} v_{ji}[k]$$

[6] https://youtu.be/7M17R5bcv4o

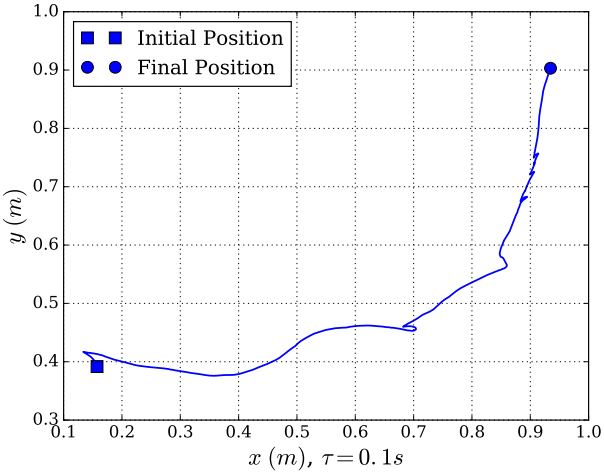

Figure 4: The trajectory of the centre of mass of the robot. The experiment is assumed to be complete when $\|x[k] - x_d\| \leq 0.05$.

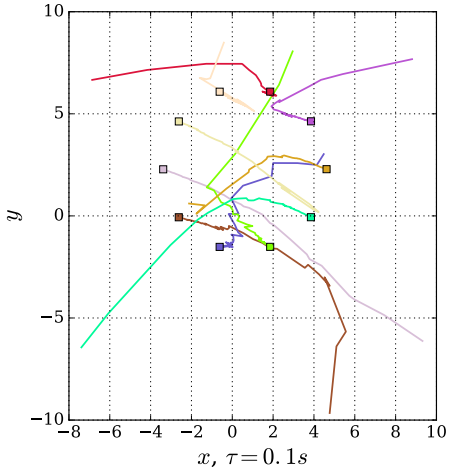

Figure 5: The trajectories of the agents converging to a formation shape under semi-homomorphic encryption information passing.

Table 1: The computational time of various parts of the algorithm.

Key length (bits)	64	128	256	512
Encryption (ms)	0.897	2.877	15.568	103.333
Controller (ms)	0.951	2.934	15.800	108.921
Decryption (ms)	0.318	0.976	5.408	36.537

where $v_{ji}[k]$ is obtained from decrypting the encrypted version of $w_{ji}[k]\,(x_j[k] - x_i[k] + u_j - u_i)$ similar to the mechanism outlined in Section 4 where u_i, $i \in \{1, \ldots, J\}$ determine the shape of the formation that the agents acquire. Each agent i does not have access to $x_j[k]$ and u_j, $j \in \mathcal{N}_i$ in this simulation. In this simulation, similar to the previous case, the private keys are selected from $[2^{63}, 2^{64}]$, $n = 10$, $m = 5$, $\tau = 0.1$, and $w_{\max} = 3$. The trajectories of the agents are depicted in Figure 5.

6. Conclusions

In this paper, networked control systems with encrypted sensors measurements were considered. The sensors use the Paillier encryption, which is a semi-homomorphic encryption, so that the controller can perform the required computation on the encrypted data. The parameters of the encryption technique were constructed to guarantee the stability of the closed-loop system and to ensure certain bounds on the closed-loop performance. This provides strong privacy and security guarantees for the closed-loop system at the cost of extra computations (thus increasing the consumption of resources, such as energy and time). Future research questions may include implementing dynamic feedback controllers and taking advantage of hardware acceleration for faster computation of the components of Algorithm 1 and Algorithm 2. One of the difficulties of the dynamic controller is that the number of the fractional bits in the state of the dynamic controller, which is encrypted, grows larger with time (due to presence of multiplications of rational numbers). Therefore, the encrypted implementation of the dynamic controller can only run for a short planning horizon. Computationally friendly methods should be developed to address this difficulty.

References

[1] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," in *Proceedings of the 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys)*, 2016.

[2] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," *IEEE Control Systems*, vol. 35, no. 1, pp. 66–81, 2015.

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

[4] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *Smart Grid, IEEE Transactions on*, vol. 6, no. 1, pp. 486–495, 2015.

[5] 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.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings* (J. Stern, ed.), pp. 223–238, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, STOC '09, pp. 169–178, 2009.

[9] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the 44th annual ACM Symposium on Theory of Computing*, pp. 1219–1234, 2012.

[10] M. Brenner, J. Wiebelitz, G. Von Voigt, and M. Smith, "Secret program execution in the cloud applying homomorphic encryption," in *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference*, pp. 114–119, 2011.
[11] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, no. 1, pp. 69–73, 2012.
[12] F. Kerschbaum, "Outsourced private set intersection using homomorphic encryption," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 85–86, 2012.
[13] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Proceedings of the 54th Annual Conference on Decision and Control*, pp. 6836–6843, 2015.
[14] S.-H. Wang and E. J. Davison, "On the stabilization of decentralized control systems," *Automatic Control, IEEE Transactions on*, vol. 18, no. 5, pp. 473–478, 1973.
[15] B. D. Anderson and D. J. Clements, "Algebraic characterization of fixed modes in decentralized control," *Automatica*, vol. 17, no. 5, pp. 703–712, 1981.
[16] D. Serre, *Matrices: Theory and Applications*. Graduate Texts in Mathematics, Springer New York, 2010.
[17] O. Goldreich, *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.
[18] R. Ostrovsky and E. W. Skeith, "Private searching on streaming data," *Journal of Cryptology*, vol. 20, no. 4, pp. 397–430, 2007.
[19] J. A. Fax and R. M. Murray, "Information flow and cooperative control of vehicle formations," *IEEE transactions on automatic control*, vol. 49, no. 9, pp. 1465–1476, 2004.
[20] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on automatic control*, vol. 48, no. 6, pp. 988–1001, 2003.
[21] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," *Systems & Control Letters*, vol. 53, no. 1, pp. 65–78, 2004.
[22] W. Ren and R. Beard, "Decentralized scheme for spacecraft formation flying via the virtual structure approach," *Journal of Guidance, Control, and Dynamics*, vol. 27, no. 1, pp. 73–82, 2004.
[23] C. H. Papadimitriou and K. Steiglitz, *Combinatorial optimization: algorithms and complexity*. Dover Publications, 1998.
[24] S. M. LaValle, *Planning algorithms*. Cambridge university press, 2006.
[25] J. P. Hespanha, *Linear Systems Theory*. Princeton University Press, 2009.

Appendix A. Proof of Proposition 1

Since the proofs of parts (1) and (2) are very similar, the proof of part (1) is only presented. First, note that

$$\begin{aligned} &f_{n,m}^{-1}(f_{n,m}(b)) \\ &\quad = f_{n,m}^{-1}(2^m b \bmod 2^n) \\ &\quad = f_{n,m}^{-1}\bigg(\Big(-b_n 2^{n-1} + \sum_{i=1}^{n-1} 2^{i-1} b_i\Big) \bmod 2^n\bigg), \end{aligned}$$

where $b_i \in \{0,1\}$ for all $i \in \{1,\dots,n\}$ are selected so that $b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} 2^{i-m-1} b_i$. For $b \geq 0$, the expression for $f_{n,m}^{-1}(f_{n,m}(b))$ can be further simplified to

$$\begin{aligned} f_{n,m}^{-1}(f_{n,m}(b)) &= f_{n,m}^{-1}\bigg(\Big(\sum_{i=1}^{n-1} 2^{i-1} b_i\Big) \bmod 2^n\bigg) \\ &= \Big(\sum_{i=1}^{n-1} 2^{i-1} b_i\Big)/2^m \\ &= b. \end{aligned}$$

A similar argument leads to that $f^{-1}(f(b)) = b$ if $b < 0$.

Appendix B. Proof of Proposition 2

Note that

$$\begin{aligned} (f(b)+f(b')) \bmod 2^n &= (2^m b \bmod 2^n + 2^m b' \bmod 2^n) \bmod 2^n \\ &= 2^m (b+b') \bmod 2^n \\ &= f(b+b'). \end{aligned}$$

For any $b \in \mathbb{Q}(n,m)$, there exists $(b_i)_{i=1}^n \in \{0,1\}^n$ such that $b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} 2^{i-m-1} b_i$. Therefore,

$$\begin{aligned} f(-b) &= (-2^m b) \bmod 2^n \\ &= \begin{cases} \Big(-\sum_{i=1}^{n-1} 2^{i-1} b_i\Big) \bmod 2^n, & b \geq 0, \\ \Big(2^{n-1} - \sum_{i=1}^{n-1} 2^{i-1} b_i\Big) \bmod 2^n, & b < 0, \end{cases} \\ &= \begin{cases} 2^n - \sum_{i=1}^{n-1} 2^{i-1} b_i, & b \geq 0, \\ 2^{n-1} - \sum_{i=1}^{n-1} 2^{i-1} b_i, & b < 0, \end{cases} \\ &= \begin{cases} 2^n - a, & b \geq 0, \\ 2^n - \Big(2^{n-1} + \sum_{i=1}^{n-1} 2^{i-1} b_i\Big), & b < 0, \end{cases} \\ &= 2^n - a, \end{aligned}$$

where $a = f(b)$. For the product operation, the proof needs to be separated into multiple cases:

- Case 1 ($b, b' \geq 0$): Let $a, a' \in \mathbb{Z}_{2^n}$ and $b, b' \in \mathbb{Q}(n,m)$ be such that $a = f(b)$ and $a' = f(b')$. In this case, it can be proved that

$$\begin{aligned} f(bb') &= f(f^{-1}(a) f^{-1}(a')) \\ &= f((a - 2^n \mathbb{1}_{a \geq 2^{n-1}})(a' - 2^n \mathbb{1}_{a' \geq 2^{n-1}})/2^{2m}) \\ &= f(aa'/2^{2m}) \\ &= (aa'/2^m) \bmod 2^n. \end{aligned}$$

- Case 2 ($b \geq 0$ and $b' < 0$): Note that

$$\begin{aligned} f(bb') &= f((a - 2^n \mathbb{1}_{a \geq 2^{n-1}})(a' - 2^n \mathbb{1}_{a' \geq 2^{n-1}})/2^{2m}) \\ &= f(a(a' - 2^n)/2^{2m}) \\ &= (a(a' - 2^n)/2^m) \bmod 2^n. \end{aligned}$$

- Case 3 ($b, b' < 0$): It can be shown that

$$\begin{aligned} f(bb') &= f((a-2^n\mathbb{1}_{a\geq 2^{n-1}})(a'-2^n\mathbb{1}_{a'\geq 2^{n-1}})/2^{2m}) \\ &= f((a-2^n)(a'-2^n)/2^{2m}) \\ &= ((a-2^n)(a'-2^n)/2^m) \bmod 2^n. \end{aligned}$$

This concludes the proof.

Appendix C. Proof of Proposition 3

The proof of part (1) directly follows from the application of Proposition 2. For part (2), the following two cases may occur:

- Case 1 ($a < 2^{n-1}$): In this case, by definition, $a \overset{n}{\underset{m}{\otimes}} a' = (aa'/2^m) \bmod 2^n$.
- Case 2 ($a \geq 2^{n-1}$): Note that

$$\begin{aligned} a \overset{n}{\underset{m}{\otimes}} a' &= ((a-2^n)a'/2^m) \bmod 2^n \\ &= (aa'/2^m - 2^n(a'/2^m)) \bmod 2^n \\ &= (aa'/2^m) \bmod 2^n, \end{aligned}$$

where the last equality follows from that $a'/2^m \in \mathbb{Z}$.

This concludes the proof.

Appendix D. Proof of Proposition 4

First, construct $\bar{b} = 2^m b$ and $\bar{b}' = 2^m b'$. Since $b, b' \in \mathbb{Q}(n,m)$, it can be deduced that $\bar{b}, \bar{b}' \in \mathbb{Q}(n+m,0) \subseteq \mathbb{Q}(n+2m,0)$. Let $a = f_{n,m}(b)$, $a' = f_{n,m}(b')$, $\bar{a} = f_{n+2m,0}(\bar{b})$, and $\bar{a}' = f_{n+2m,0}(\bar{b}')$. Now, Corollary 1 can be used to show that $f_{n+2m,0}(\bar{b}\bar{b}') = \bar{a} \overset{n+2m}{\underset{0}{\otimes}} \bar{a}'$ since $\bar{b}\bar{b}' \in \mathbb{Q}(n+2m,0)$ following the observation that $\bar{b}\bar{b}' = 2^{2m} bb'$ with $bb' \in \mathbb{Q}(n,m)$. Therefore, $f_{n,m}(bb') = f_{n,m}(\bar{b}\bar{b}'/2^{2m}) = f_{n,m}(f^{-1}_{n+m,0}(\bar{a} \overset{n}{\underset{0}{\otimes}} \bar{a}')/2^{2m})$.

Appendix E. Proof of Proposition 5

Notice that

$$\begin{aligned} &E(t;r)E(t';r') \bmod N^2 \\ &\qquad = (N+1)^{t+t'}(rr')^N \bmod N^2 \\ &\qquad = E(t+t'; rr'),\ \forall r, r' \in \mathbb{Z}_N^*, \forall t, t' \in \mathbb{Z}_N, \end{aligned}$$

and

$$\begin{aligned} E(t;r)^{t'} \bmod N^2 &= (N+1)^{t't} r^{t'N} \bmod N^2 \\ &= E(t't; r^{t'}),\ \forall r \in \mathbb{Z}_N^*, \forall t, t' \in \mathbb{Z}_N. \end{aligned}$$

This concludes the proof.

Appendix F. Proof of Proposition 6

The proof of part (1) follows from

$$\begin{aligned} (E(a;r)^{a'} \bmod N^2)^\theta \bmod N^2 &= E((aa') \bmod N; r^{a'})^\theta \bmod N^2 \\ &= E((aa'\theta) \bmod N; r^{a'\theta}) \\ &= E((aa'/2^m) \bmod N; r^{a'\theta}) \\ &= E(aa'/2^m; r^{a'\theta}) \\ &= E(a \overset{n}{\underset{m}{\otimes}} a'; r^{a'\theta}). \end{aligned}$$

The proof of the rest of the parts follows from the application Propositions 5 and 3.

Appendix G. Proof of Proposition 7

If n_1 and m_1 are selected such that $2^{n_1-m_1-1} > \max_{i,j} |\bar{K}_{ij}|$ and $2^{-m_1} \leq \epsilon(\bar{K})/\sqrt{p_u p_y}$, then

$$\begin{aligned} \|K - \bar{K}\|_F &= \sqrt{\sum_{i,j} (K_{ij} - \bar{K}_{ij})_2^2} \\ &\leq \sqrt{\sum_{i,j} 2^{-2m_1}} \\ &\leq \sqrt{\sum_{i,j} \epsilon(\bar{K})^2/(p_u p_y)} \\ &= \epsilon(\bar{K}). \end{aligned}$$

This concludes the proof.

Appendix H. Proof of Proposition 8

The stability of the closed-loop system implies that there exists a Lyapunov function of the form $x^\top P x$ with positive-definite P for which $(A+BKC)^\top P(A+BKC) - P = -Q < 0$ [25, p. 71]. Let $e[k] = y[k] - \tilde{y}[k]$. Assume that $|e_i[k]| \leq 2^{-m_2}$ for all k. First, we prove that $\mathcal{X} := \{x \in \mathbb{R}^{p_x} \,|\, x^\top P x \leq \zeta\}$ for an appropriately selected ζ is an invariant set. To do so, notice that

$$\begin{aligned} &x[k+1]^\top P x[k+1] - x[k]^\top P x[k] \\ &\quad = x[k]^\top ((A+BKC)^\top P(A+BKC) - P) x[k] \\ &\qquad + 2x[k]^\top (A+BKC)^\top PBKe[k] \\ &\qquad + e[k]^\top (BK)^\top PBKe[k] \\ &\quad \leq - x[k]^\top Q x[k] + c_1 2^{-m_2} + c_2 2^{-2m_2} \qquad \text{(H.1)} \\ &\quad \leq - x[k]^\top Q x[k] + (c_1+c_2) 2^{-m_2}, \qquad \text{(H.2)} \end{aligned}$$

where

$$\begin{aligned} c_1 &= 2\sqrt{\zeta/\lambda_{\min}(P)} \sum_{i,j} |W_{ij}|, \\ c_2 &= p_y \lambda_{\max}(K^\top B^\top P B K) \end{aligned}$$

with $W = (A + BKC)^\top PBK$. The inequality in (H.1) follows from that

$$\begin{aligned}2x[k]^\top (A+BKC)^\top PBKe[k] \\ \leq & 2|x[k]^\top We[k]| \\ \leq & 2\sum_{i,j}|x_i[k]||W_{ij}||e_j[k]| \\ \leq & \left(2\sqrt{\zeta/\lambda_{\min}(P)}\sum_{i,j}|W_{ij}|\right)2^{-m_2}.\end{aligned}$$

In what follows, we select ζ so that $\mathcal{X}$ becomes an invariant set since both Q and P are positive-definite matrices. First, for all $x[k]$, we get that

$$\begin{aligned}x[k]^\top Qx[k] &\geq \lambda_{\min}(Q)x[k]^\top x[k] \\ &\geq \lambda_{\min}(Q)/\lambda_{\max}(P)x[k]^\top Px[k].\end{aligned}$$

To prove that $\mathcal{X}$ is invariant, we need to show that if $x[k] \in \mathcal{X}$ then $x[k+1] \in \mathcal{X}$. Assume that $x[k] \in \mathcal{X}$. We prove that also $x[k+1] \in \mathcal{X}$.

Case 1: Let $\lambda_{\min}(Q) \leq \lambda_{\max}(P)$; we will prove the other case later. Therefore, we get

$$\begin{aligned}x[k+1]^\top Px[k+1] \leq & \left(1-\frac{\lambda_{\min}(Q)}{\lambda_{\max}(P)}\right)x[k]^\top Px[k] \\ & + (c_1+c_2)2^{-m_2} \\ \leq & \left(1-\frac{\lambda_{\min}(Q)}{\lambda_{\max}(P)}\right)\zeta + (c_1+c_2)2^{-m_2}\end{aligned}$$

Note that $x[k+1] \in \mathcal{X}$ if $x[k+1]^\top Px[k+1] \leq \zeta$, which can be ensure by selecting ζ such that

$$\left(1-\frac{\lambda_{\min}(Q)}{\lambda_{\max}(P)}\right)\zeta + (c_1+c_2)2^{-m_2} \leq \zeta.$$

This inequality is equivalent to that

$$\frac{\lambda_{\min}(Q)}{\lambda_{\max}(P)}\zeta - \frac{2^{1-m_2}\sum_{i,j}|W_{ij}|}{\sqrt{\lambda_{\min}(P)}}\sqrt{\zeta} - c_2 2^{-m_2} \geq 0.$$

Due to the structure of the left-hand side of this inequality (being a second order polynomial in $\sqrt{\zeta}$ with a positive leading coefficient), there exists ς (the largest root of the aforementioned polynomial) such that the inequality is satisfied if $\zeta \geq \max(0,\varsigma)^2$.

Case 2: Now, let $\lambda_{\min}(Q) > \lambda_{\max}(P)$. Therefore, we get

$$x[k+1]^\top Px[k+1] \leq (c_1+c_2)2^{-m_2}.$$

To ensure that $x[k+1] \in \mathcal{X}$, we can select ζ such that

$$(c_1+c_2)2^{-m_2} \leq \zeta.$$

This inequality is equivalent to that

$$\zeta - \frac{2^{1-m_2}\sum_{i,j}|W_{ij}|}{\sqrt{\lambda_{\min}(P)}}\sqrt{\zeta} - c_2 2^{-m_2} \geq 0.$$

Following the same line of reasoning, we can show that there exists ς (the largest root of the second order polynomial in $\sqrt{\zeta}$ in the left hand side of inequality) such that the inequality is satisfied if $\zeta \geq \max(0,\varsigma)^2$.

This proves that $\mathcal{X}$ is an invariant set if $\zeta \geq \max(0,\varsigma)^2$. Now, the constant $M(x_0)$ can be chosen such as $M(x_0) = \max_{x\in\mathcal{X}}\max_{1\leq i\leq p_y}|C_i x|$, where C_i denotes the i-th row of matrix C. Finally, if n_2 is selected such that $2^{n_2-m_2-1} > M(x_0)$, it can be ensured that $|e_i[k]| \leq 2^{-m_2}$. This concludes the proof.

Appendix I. Proof of Theorem 1

First, we show that the set $\mathcal{X}' := \{x \in \mathbb{R}^{p_x} \,|\, x^\top Px \leq (c_1+c_2)2^{-m}(\lambda_{\min}(P)/\lambda_{\min}(Q)+1)\}$ is an invariant set. To do so, we prove that if $x[k] \in \mathcal{X}'$, then $x[k+1] \in \mathcal{X}'$. One of the following two cases occur.

Case 1: Assume that $x[k] \in \mathcal{X}'$ and $x[k]^\top Px[k] \geq (c_1+c_2)2^{-m}\lambda_{\min}(P)/\lambda_{\min}(Q)$. In this case, $x[k+1]^\top Px[k+1] - x[k]^\top Px[k] < 0$ because

$$\begin{aligned}x[k+1]^\top Px[k+1] - x[k]^\top Px[k] \\ \leq & -\lambda_{\min}(Q)x[k]^\top x[k] + (c_1+c_2)2^{-m} \\ \leq & -(\lambda_{\min}(Q)/\lambda_{\min}(P))x[k]^\top Px[k] + (c_1+c_2)2^{-m}\end{aligned}$$

with the controller $u[k] = K\tilde{y}_i[k]$. Hence, $x[k+1] \in \mathcal{X}'$.

Case 2: Assume that $x[k] \in \mathcal{X}'$ and $x[k]^\top Px[k] \leq (c_1+c_2)2^{-m}\lambda_{\min}(P)/\lambda_{\min}(Q)$. In this case, $x[k+1]^\top Px[k+1] - x[k]^\top Px[k]$ is not necessarily negative and, thus, the value of the Lyapunov function might increase. The increase is however bounded as $x[k+1]^\top Px[k+1] - x[k]^\top Px[k] \leq (c_1+c_2)2^{-m}$. Therefore, $x[k+1]^\top Px[k+1] \leq (c_1+c_2)2^{-m}(\lambda_{\min}(P)/\lambda_{\min}(Q)+1)$, where the inequality follows from that $x[k]^\top Px[k] \leq (c_1+c_2)2^{-m}\lambda_{\min}(P)/\lambda_{\min}(Q)$.

Now, we need to prove that the set $\mathcal{X}'$ is an attractive set. This follows from that

$$\begin{aligned}x[k+1]^\top Px[k+1] - x[k]^\top Px[k] \\ \leq & -(\lambda_{\min}(Q)/\lambda_{\min}(P))x[k]^\top Px[k] + (c_1+c_2)2^{-m} \\ \leq & 0,\end{aligned}$$

where the second inequality is because $x[k]^\top Px[k] \geq (c_1+c_2)2^{-m}\lambda_{\min}(P)/\lambda_{\min}(Q)$ if $x[k] \notin \mathcal{X}'$.

Note that, evidently, if all the trajectories of the system converge to $\mathcal{X}'$, they also converge to $\mathcal{B}((c_1+c_2)2^{-m}(1/\lambda_{\min}(Q)+1/\lambda_{\min}(P)))$

To be able to use the results of Proposition 3, 5, and 6, the outcome of all the summations and the multiplications should not over flow or under flow from the set $\mathbb{Q}(n,m)$. Therefore, $n \geq p_y + n_1 + n_2$ and $m \geq m_1 + m_2$ must be selected to ensure this property. These numbers are calculated based on the worst-case scenarios (very large or very small numbers are multiplied and summed). The rest of the proof follows from the application of Propositions 3, 5, and 6.

Appendix J. Proof of Proposition 9

Observe $\chi_{ji} = \{(x, w)|wx - w\tilde{x}_i[k] = v_{ji}[k], x, w \in \mathbb{Q}(n, m)\}$. It can be seen that one obtains $|\Omega_{ji}^{+}|$ via the change of variables $\varphi = w(x + 2^{n-m})2^{2m}$ and $\vartheta = 2^m w$ and letting $\alpha_i^{+} = (\tilde{x}_i[k] + 2^{n-m})2^m$ and $\beta_{ji} = 2^{2m} v_{ji}[k]$. Noting that the aforementioned change of variables are equivalent to $w = 2^{-m}\vartheta$ and $x = 2^{-m}\vartheta^{-1}\varphi - 2^{n-m}$ completes the proof for the first statement. The second statement can be established in a similar fashion as well. The third statement is a direct consequence of the first and the second statements.