University Library



A gateway to Melbourne's research publications

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Farokhi, F;Shames, I;Batterham, N

Title:
Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption

Date:
2016

Citation:
Farokhi, F., Shames, I. & Batterham, N. (2016). Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption. Proceedings of the 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems, 49, (22), pp.163-168. Elsevier. https://doi.org/10.1016/j.ifacol.2016.10.390.

Persistent Link:
https://hdl.handle.net/11343/251421

Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption ⋆

Farhad Farokhi * **Iman Shames** * **Nathan Batterham** *

* *Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, VIC 3010, Australia (e-mails: {ffarokhi,ishames}@unimelb.edu.au and n.batterham@student.unimelb.edu.au)*

Abstract: Networked control systems with encrypted sensors measurements is considered. Semi-homomorphic encryption is used so that the controller can perform the required computation on the encrypted data. Specifically, in this paper, the Paillier encryption technique is utilized that allows summation of decrypted data to be performed by multiplication of the encrypted data. Conditions on the parameters of the encryption technique are provided that guarantee the stability of the closed-loop system and ensure certain bounds on the closed-loop performance.

Keywords: Networked control system; Privacy; 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 considerably save 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 (Amin et al., 2015; Teixeira et al., 2015; Yang et al., 2015).

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 (Teixeira et al., 2015). Eavesdropping is one of the most basic attacks that requires a relatively low amount of resources. This attack also serves as the starting part of many more sophisticated attacks (Mo and Sinopoli, 2009). 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 very 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 happen most often inside the cloud-computing services, where a third-party 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 also 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 (Paillier, 1999), which is a semi-homomorphic encryption techniques, allows summation of plain data to be performed by multiplication of the encrypted ones. On contrary, ElGamal encryption (ElGamal, 1985) allows the multiplication of plain data using the multiplication of the encrypted data. In contrast, fully-homomorphic encryption schemes, such as Gentry's encryption (Gentry, 2009), 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, in this paper, the parameters of the Paillier

⋆ The work was, in part, supported by a McKenzie Fellowship, ARC grant LP130100605, and Defence Science and Technology Group through the Research Agreement MyIP:6288.

encryption technique are determined so that the stability of the closed-loop system and its closed-loop performance can be guaranteed.

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 (López-Alt et al., 2012; Brenner et al., 2011; Ren et al., 2012; Kerschbaum, 2012; Kogiso and Fujita, 2015) and the references there-in. However, none of these studies, except (Kogiso and Fujita, 2015), have considered these techniques in networked control system. In addition, in (Kogiso and Fujita, 2015), 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.

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. Numerical examples are provided in Section 4 and the paper is concluded in Section 5.

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

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

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

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

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 $f_{n,m}^{-1} : \mathbb{Z}_{2^n} \to \mathbb{Q}(n,m)$ such that $f_{n,m}^{-1}(a) = (a - 2^n \mathbb{1}_{a \geq 2^{n-1}})/2^m$ for all $a \in \mathbb{Z}_{2^n}$, where $\mathbb{1}_p$ 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) $f_{n,m}^{-1}(f_{n,m}(b)) = b$ for all $b \in \mathbb{Q}(n,m)$;
(2) $f_{n,m}(f_{n,m}^{-1}(a)) = a$ 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 $f_{n,m}^{-1}$, 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 $f_{n,m}^{-1}(a)$ 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,

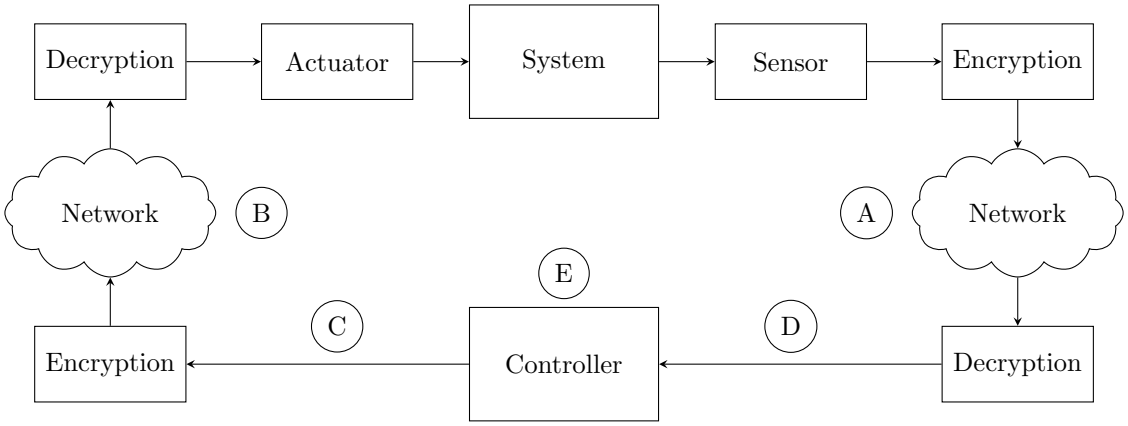


Fig. 1. The schematic diagram of a networked control system with encryption-decryption units.

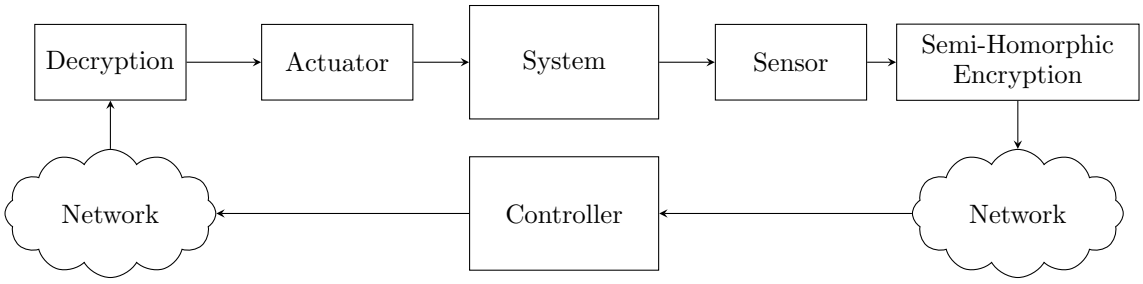


Fig. 2. The schematic diagram of a networked control system with semi-homomorphic encryption-decryption units.

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 $bb' \in \mathbb{Q}(n,m)$,

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

Proof. See Appendix D. □

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

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] (Paillier, 1999). 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 $N = pq$;
  - Set $\lambda = \text{lcm}(p-1, q-1)$ and $\mu = \lambda^{-1} \bmod N$, where $\text{lcm}(a,b)$ 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 (Paillier, 1999), 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

[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.

result identifies a few cases in which the multiplication is implementable.

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 (Wang and Davison, 1973; Anderson and Clements, 1981). 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 (Serre, 2010, 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 $\|K - \bar{K}\|_F \le \epsilon(\bar{K})$. The following results can be proved.

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 $m_1 \ge \lceil -\log_2(\epsilon(\bar{K})/\sqrt{p_u p_y}) \rceil$ and $n_1 \ge \lceil m_1 + 1 + \log_2(\max_{i,j} |\bar{K}_{ij}|) \rceil$. Then, $A + BKC$ is Schur.

Proof. See Appendix G. □

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 $L_{ji} = f_{n+2m,0}(2^m K_{ji})$ to the controller
\# Sensors
for $i = 2, \dots, p_y$ **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 $j = 2, \dots, p_u$ **do**
  Set $w_j[k] = z_1^{L_{j1}} \bmod N^2$
  for $i = 2, \dots, p_y$ **do**
    Compute $w_j[k] = (w_j[k](z_i^{L_{ji}} \bmod N^2)) \bmod N^2$
  end for
  Transmit $w_j[k]$ to the actuators
end for
\# Actuators
for $j = 2, \dots, p_u$ **do**
  Implement $u_j[k] = D(w_j[k]) \bmod 2^{n+2m}/2^{2m}$
end for

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 $n_2 \ge \lceil m_2 + 1 + \log_2(M(x_0)) \rceil$.

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

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

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. □

Contrary to the previously-described scenario, it could be of interest to encrypt the controller parameters instead

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

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: $u[k]$

Set $n = p_y + n_1 + n_2$ and $m = m_1 + m_2$
\# Control designer
Compute $K \in \arg\min_{K' \in \mathbb{Q}(n,m)^{p_u \times p_y}} \|K' - \bar{K}\|_F$
Transmit $L_{ji} = E(f_{n+2m,0}(2^m K_{ji}); r)$ to the controller
\# Sensors
for $i = 2, \ldots, p_y$ **do**
  Construct $\tilde{y}_i[k]$ by projecting $y_i[k]$ in $\mathbb{Q}(n, m)$
  Transmit $\bar{y}_i[k] = f_{n+2m,0}(2^m \tilde{y}_i[k])$ to the controller
end for
\# Controller
for $j = 2, \ldots, p_u$ **do**
  Set $w_j[k] = L_{j1}^{\bar{y}_1[k]} \bmod N^2$
  for $i = 2, \ldots, p_y$ **do**
    Compute $w_j[k] = (w_j[k](L_{ji}^{\bar{y}_i[k]} \bmod N^2)) \bmod N^2$
  end for
  Transmit $w_j[k]$ to the actuators
end for
\# Actuators
for $j = 2, \ldots, p_u$ **do**
  Implement $u_j[k] = D(w_j[k]) \bmod 2^{n+2m}/2^{2m}$
end for

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. NUMERICAL EXAMPLE

In this section, the application of Algorithm 1 to derive a nonholonomic vehicle to a desired location is demonstrated. The vehicle motion is assumed to be governed by

$$\dot{x}_1 = v\cos\theta, \tag{4}$$
$$\dot{x}_2 = v\sin\theta, \tag{5}$$
$$\dot{\theta} = \omega, \tag{6}$$

where $x = [x_1, x_2]^\top$ and θ denote the position and the heading of the vehicle, respectively. Moreover, v and ω are respectively the speed and the angular velocity of the vehicle and are used as control inputs. The feedback linearization of the type introduced in (De Luca et al., 2000) is employed where

$$\dot{v} = u_1\cos\theta + u_2\sin\theta \tag{7}$$
$$\omega = \frac{-u_1\sin\theta + u_2\cos\theta}{v}, \tag{8}$$

with u_1 and u_2 used as control inputs of the feedback linearized system. It is assumed that this linearizing control is implemented locally and Algorithm 1 is used to compute u_1 and u_2. Note that under (7) and (8) the dynamics of x_1 and x_2 are akin to those of two decoupled double integrators with inputs u_1 and u_2. It is assumed that outputs of the feedback linearized system, x_1 and x_2, as well as the desired destination are projected onto $\mathbb{Q}(5, 5)$ and are encrypted using random prime numbers in $[2^{127}, 2^{128}]$. This ensures that an eavesdropper can neither figure out the current nor the desired destination of the vehicle. The controller is a proportional controller with integer coefficients. The average necessary times for encryption, control input computation, and decryption on a 2.8 GHz Intel Core i7 MAC laptop using Python 3.4 are respectively $2.84ms$, $2.93ms$, and $0.96ms$. The first and the second states (position) trajectories of the vehicle are depicted in Figure 3 where the desired destination is $[5, -4]^\top$.

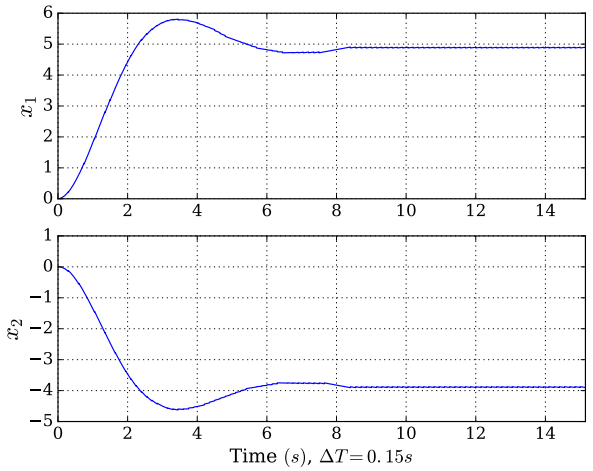


Fig. 3. The coordinates of a nonholonomic vehicle with encrypted feedback control.

5. CONCLUSIONS

In this paper, networked control systems with encrypted sensors measurements were considered. It was assumed that 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. 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.

REFERENCES

Amin, S., Schwartz, G.A., Cardenas, A.A., and Sastry, S.S. (2015). Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure. *IEEE Control Systems*, 35(1), 66–81.

Anderson, B.D. and Clements, D.J. (1981). Algebraic characterization of fixed modes in decentralized control. *Automatica*, 17(5), 703–712.

Brenner, M., Wiebelitz, J., Von Voigt, G., and Smith, M. (2011). Secret program execution in the cloud applying homomorphic encryption. In *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference*, 114–119.

De Luca, A., Oriolo, G., and Vendittelli, M. (2000). Stabilization of the unicycle via dynamic feedback linearization. In *6th IFAC Symp. on Robot Control*, 397–402.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), 469–472.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, STOC '09, 169–178.

Hespanha, J.P. (2009). *Linear Systems Theory*. Princeton University Press.

Kerschbaum, F. (2012). Outsourced private set intersection using homomorphic encryption. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, 85–86.

Kogiso, K. and Fujita, T. (2015). Cyber-security enhancement of networked control systems using homomorphic encryption. In *Proceedings of the 54th Annual Conference on Decision and Control*, 6836–6843.

López-Alt, A., Tromer, E., and Vaikuntanathan, V. (2012). 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*, 1219–1234.

Mo, Y. and Sinopoli, B. (2009). Secure control against replay attacks. In *Procceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, 911–918.

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

Ren, K., Wang, C., and Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, (1), 69–73.

Serre, D. (2010). *Matrices: Theory and Applications*. Graduate Texts in Mathematics. Springer New York.

Teixeira, A., Sou, K.C., Sandberg, H., and Johansson, K.H. (2015). Secure control systems: A quantitative risk management approach. *Control Systems, IEEE*, 35(1), 24–45.

Wang, S.H. and Davison, E.J. (1973). On the stabilization of decentralized control systems. *Automatic Control, IEEE Transactions on*, 18(5), 473–478.

Yang, L., Chen, X., Zhang, J., and Poor, H.V. (2015). Cost-effective and privacy-preserving energy management for smart meters. *Smart Grid, IEEE Transactions on*, 6(1), 486–495.

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

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

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 $f^{-1}(f(b))$ can be further simplified to

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

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 $\bar{b}, \bar{b}' \in \mathbb{Q}(n+2m, 0)$. 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
$$\begin{aligned} &E(t;r)E(t';r') \bmod N^2 \\ &\quad = (N+1)^{t+t'}(rr')^N \bmod N^2 \\ &\quad = E(t+t'; rr'),\ \forall r, r' \in \mathbb{Z}_N^*, \forall t, t' \in \mathbb{Z}_N, \end{aligned}$$
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 $(A+BKC)^\top P(A+BKC) - P = -Q < 0$ (Hespanha, 2009, p. 71). Let $e[k] = y[k] - \tilde{y}[k]$. Assume that $|e_i[k]| \leq 2^{-m_2}$ for all k. First, it is proved that $\mathcal{X} := \{x \in \mathbb{R}^{p_x} \,|\, x^\top P x \leq \zeta\}$ for an appropriately selected ζ is an invariant set. 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
$$\begin{aligned} c_1 &= 2\sqrt{\zeta/\lambda_{\min}(P)} \sum_{i,j} |W_{ij}|, \\ c_2 &= p_y \lambda_{\max}(K^\top B^\top P B K). \end{aligned}$$
The inequality in (H.1) follows from that
$$\begin{aligned} &2x[k]^\top (A+BKC)^\top PBKe[k] \\ &\quad \leq 2|x[k]^\top W e[k]| \\ &\quad \leq 2 \sum_{i,j} |x_i[k]||W_{ij}||e_j[k]| \\ &\quad \leq \left(2\sqrt{\zeta/\lambda_{\min}(P)} \sum_{i,j} |W_{ij}| \right) 2^{-m_2}, \end{aligned}$$
where $W = (A+BKC)^\top PBK$. Evidently, $x[k+1]^\top P x[k+1] - x[k]^\top P x[k] < 0$ if $x[k]^\top Q x[k] \geq (c_1 + c_2) 2^{-m_2}$. This proves that $\mathcal{X}$ is an invariant set if $\zeta = \max(x_0^\top P x_0, (c_1 + c_2) 2^{-m_2})$. 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, note that
$$\begin{aligned} &x[k+1]^\top P x[k+1] - x[k]^\top P x[k] \\ &\quad \leq -x[k]^\top \lambda_{\min}(Q) x[k] + (c_1 + c_2) 2^{-m} \end{aligned}$$

with the controller $u[k] = K\tilde{y}_i[k]$. Hence, $x[k+1]^\top P x[k+1] - x[k]^\top P x[k] < 0$ if $x[k] \in \{x \in \mathbb{R}^{p_x} \mid \|x\|_2^2 \geq (c_1+c_2)2^{-m}/\lambda_{\min}(Q)\}$. Therefore, if the controller $u[k] = K\tilde{y}_i[k]$ is correctly calculated, the states converge to the set $\mathcal{B}(2^{-m}(c_1+c_2)/\lambda_{\min}(Q))$. 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.