Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-22 (2016) 175–180

Encrypting Controller using Fully Homomorphic Encryption for Security of Cyber-Physical Systems ⋆

Junsoo Kim * **Chanhwa Lee** * **Hyungbo Shim** *
Jung Hee Cheon ** **Andrey Kim** ** **Miran Kim** **
Yongsoo Song **

* *ASRI, Dep. of Electrical and Computer Engineering, Seoul National University, Seoul, Korea.*
** *Dep. of Mathematical Sciences, Seoul National Univ., Seoul, Korea.*

Abstract: In order to enhance security of cyber-physical systems, it is important to protect the signals from sensors to the controller, and from the controller to the actuator, because the attackers often steal and compromise those signals. One immediate solution could be encrypting the signals, but in order to perform computation in the controller, they should be decrypted before computation and encrypted again after computation. For this, the controller keeps the secret key, which in turn increases vulnerability from the attacker. In this paper, we introduce the *fully homomorphic encryption (FHE)*, which is an advanced cryptography that has enabled arithmetic operations directly on the encrypted variables without decryption. However, this also introduces several new issues that have not been studied for conventional controllers. Most of all, an encrypted variable has a finite lifespan, which decreases as an arithmetic operation is performed on it. Our solution is to run multiple controllers, and orchestrate them systematically. Also, in order to slow down the decrease of the lifespan, a tree-based computation of sequential matrix multiplication is introduced. We finally demonstrate the effectiveness of the proposed algorithm with quadruple water tank example.

Keywords: Cyber-physical system, Security, Homomorphic encryption, Controller encryption

1. INTRODUCTION

As physical systems are connected to computers through network communications, real control systems can be a target of cyber attackers. Such an integration of computation (cyber part), physical process (physical part), and communication (link between cyber and physical parts), is called *cyber-physical systems* (CPSs). By its openness and connectivity nature, CPS is vulnerable to malicious attacks. Furthermore, it is much more dangerous than conventional cyber attacks by a hacker since failure or malfunction on the critical infrastructures, such as power plants and transportation systems, caused by cyber-physical attacks lead to a tremendous catastrophe (Slay and Miller, 2007; Langner, 2011). Thus, security of CPS is becoming more and more important and attracts many researchers' attention recently (Sandberg et al., 2015).

In control system community, CPSs are regarded as large-scale networked control systems. Therefore, they focus on the system theoretic properties of physical plants and try to enhance security of CPS by adopting and modifying advanced control techniques. Various control engineering methods are applied to increase security in physical layers of CPS, such as fault detection and isolation (Pasqualetti et al., 2013), robust optimal control (Amin et al., 2009), estimation theory (Lee et al., 2015), network graph theory (Sundaram and Hadjicostis, 2011), and game-theoretic approach (Zhu and Basar, 2015).

However, fundamental limitations on detectability of attacks are investigated by Pasqualetti et al. (2013) and the finding of *zero-dynamics attack*, which is in the category of stealthy attack (Teixeira et al., 2012), has made the situation difficult because, in theory, there is no way to detect the attack by any anomaly detectors such as fault detection methods (Teixeira et al., 2015). On the other hand, in order to maintain stealthiness, the attacker should continuously generate and inject signals exactly corresponding to transmission zeros of the system. This requires exact model knowledge to the attacker, and so the attacker may need to monitor input and output signals to build the model. Similarly, a recent robust zero-dynamics attack by Park et al. (2016) also requires input and output information of the plant. Therefore, the security level of CPSs can be enhanced if the feedback loop is entirely encrypted so that original messages are protected and are not revealed to adversaries.

In this regard, one can employ encryption to protect communication of information between plant and controller. See Fig. 1 (left figure). However, a drawback of conventional encryption is that the received information should be decrypted in order to compute the control input. That is, secret key must be kept inside the controller, which has possible risk to be stolen by attackers. Hence, it is desired if the computation for control input is performed without

⋆ The work of J. Kim, C. Lee, and H. Shim was supported by ICT R&D program of MSIP/IITP Grant number 14-824-09-013, Resilient Cyber-Physical Systems Research. The work of J. H. Cheon, A. Kim, M. Kim, and Y. Song was supported by IT R&D program of MSIP/KEIT [No. 0450-21060006] and Samsung Electronics Co., Ltd. (No. 0421-20150074). Corresponding author: Hyungbo Shim.

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.10.392

encrypting the data, so that the controller does not have to maintain the secret key of the encryption.

Homomorphic encryption (HE) is a cryptographic scheme that allows homomorphic operations (e.g., homomorphic addition and multiplication) on encrypted data without decryption. Since Gentry (2009) discovered the first plausible construction of *fully homomorphic encryption* (FHE) scheme, many other HE schemes have been suggested following Gentry's blueprint (Cheon and Stehlé, 2015). This in turn allows possibility that the controller does not have to maintain the secret key. The right figure in Fig. 1 illustrates the control configuration using FHE. We will call this scheme as 'encrypting controller.'

In data aggregation for smart grids, HE is used to protect the privacy of users (Li et al., 2010). However, to the best of authors' knowledge, the first attempt to employ HE in controller has been made by Kogiso and Fujita (2015). They used ElGamal (1984) encryption, but it does not allow addition between encrypted signals. In order to overcome this difficulty, the controller transmits many pieces of decrypted information to the actuator block, which are then encrypted and added to compose the control input. Unfortunately, in order to update the internal state of the controller, the outcome of this addition is also necessary in the controller. Thus, this outcome is passed to and encrypted again in the sensor block and is transmitted back to the controller. This scheme unnecessarily increases complexity of control system and requires more network throughput (or, channel capacity) of communication.

In this paper, we employ FHE for computation of encrypted signals. Use of FHE in the control system is new, and so, there may be potential difficulties. One of apparent difficulties is so-called 'bootstrapping' the encrypted variable. Unlike the plaintext variable (the term indicating un-encrypted information), the encrypted variable (which is often called ciphertext) has a lifespan which decreases whenever operation such as multiplication or addition is performed. We will briefly review this phenomenon in Section 2. During the bootstrapping of encrypted variable is performed, the controller cannot operate. To overcome this difficulty, we propose running multiple controllers and a 'catch-up' method that allows resetting the controller state (after bootstrapping) without decrypting any variables in the controller (Section 4). In addition, decrease of lifespan is proportional to the number of matrix multiplications. In order to slow down the decrease rate of lifespan as the multiplication is repeated, we develop a 'tree-based multiplication algorithm' (Section 5). This algorithm increases the lifespan of encrypted variables from the order of h to 2^h by using additional h memory and computation.

More potential issues may be

- Size of encrypted variable: When a variable is encrypted, its size usually increases. As this size increases, more network throughput is required. In this paper, a symmetric key HE is used for encryption since it is simpler and faster than by a public key HE and moreover, the size of ciphertexts can be compressed using a pseudo random number generator (PRNG) by substituting their random part as a seed. We also assume the actuator and the sensor are designed by a trusted party and they share the same symmetric key. If it is not the case, the secret keys in the actuator and the sensor should be different, and it is necessary to use a public key HE between them.
- Speed of arithmetic operation: Speed of arithmetic operation on the encrypted variable is slow than on the plaintext. While this problem needs more attention from the cryptography community, the controller design should also take into account this point. In this paper, controller parameters are not encrypted in order to speed up the operations. Multiplication between plaintext and encrypted variable is much faster than between both encrypted variables. As we consider linear controllers, only products of the plaintext gains and the encrypted (controller) states/inputs are necessary.

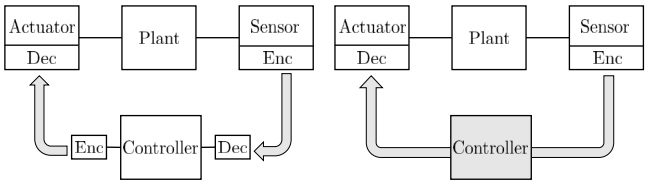

Fig. 1. Configurations with conventional encryption and with FHE

As a showcase, we will illustrate in Section 6 the use of FHE for the water-tank system, that has been used as a testbed of cyber-physical security (Teixeira et al., 2012).

2. FULLY HOMOMORPHIC ENCRYPTION

Notation. All logarithms are base 2 unless otherwise indicated. The usual dot product of two vectors is denoted by $\langle \cdot, \cdot \rangle$. For a real number r, $\lfloor r \rceil$ denotes the nearest integer to r. For a positive integer q, we use $\mathbb{Z} \cap [-q/2, q/2)$ as a representative of $\mathbb{Z}_q$. We use $x \leftarrow \mathcal{D}$ to denote the uniform sampling x according to distribution $\mathcal{D}$. For a set S, $U(S)$ denotes the uniform distribution on S. For a positive number σ, we denote $\mathcal{D}_\sigma$ the discrete Gaussian distribution of parameter σ. Throughout the paper, we let λ denote the security parameter: all known valid attacks against the cryptographic scheme under scope should take $\Omega(2^\lambda)$ bit operations. [1]

2.1 Learning With Errors (LWE)

The LWE problem was introduced by Regev (2005) as a generalization of learning parity with noise. Suppose that positive integers n and $q \geq 2$ are given. For $s \in \mathbb{Z}_q^n$ and a distribution χ over $\mathbb{Z}$, we define $A_{q,\chi}^{\mathsf{LWE}}(s)$ as the distribution obtained by sampling $a \leftarrow U(\mathbb{Z}_q^n)$ and $e \leftarrow \chi$, and returning $c = (b, a) \in \mathbb{Z}_q^{n+1}$ where $b = \langle a, \boldsymbol{s} \rangle + e$.

Let $\mathcal{D}$ be a distribution on $\mathbb{Z}_q^n$. The learning with errors problem, denoted by $\mathsf{LWE}_{n,q,\chi}(\mathcal{D})$, is to distinguish arbitrarily many independent samples chosen according to $A_{q,\chi}^{\mathsf{LWE}}(\boldsymbol{s})$ for a fixed $\boldsymbol{s} \leftarrow \mathcal{D}$, from $U(\mathbb{Z}_q^{n+1})$.

The LWE problem is self-reducible, that is, $\mathsf{LWE}_{n,q,\chi}(\mathcal{D})$ can be reduced to $\mathsf{LWE}_{n,q,\chi}(U(\mathbb{Z}_q^n))$ for any distribution $\mathcal{D}$. It was shown that the hardness of $\mathsf{LWE}_{n,q,\chi}(U(\mathbb{Z}_q^n))$ can be established by reductions to approximate short vector problems in worst-case lattices (Regev, 2005; Peikert,

[1] One writes $f(n) = \Omega(g(n))$ if and only if there exists $M > 0$ and $n_0 \in \mathbb{Z}$ such that $|f(n)| \geq M\,|g(n)|$ for all $n \geq n_0$.