Theory and Applications of Encrypted Control Systems for Cyber Security

The 13th International Workshop on Security (IWSEC)
@Tohoku University, Sep. 3rd to Sep. 5th, 2018

Rikuna Baba†, Kiminao Kogiso†, Osamu Kaneko†, Masako Kishida‡, and Kenji Sawada†
†: The University of Electro-Communications ‡: The National Institute of Informatics

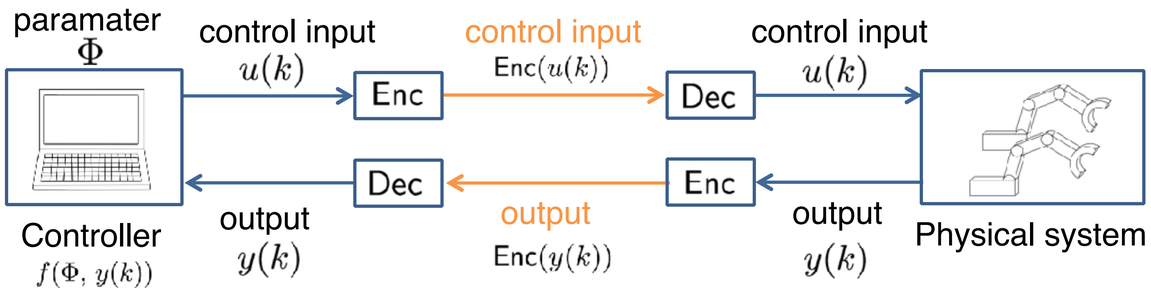
Abstract

We introduce an encrypted control system (ECS) that is a novel concept and an implementation method for cyber-security enhancement in the control engineering field[1]. Using a public key encryption scheme, ECSs can not only conceal signals and parameters inside a controller but also make it easy to detect cyber-attacks. We show that linear controllers can be constructed in the form of ECS and that the ECS is practical and effective using our developed testbed control system.

Encrypted Control System

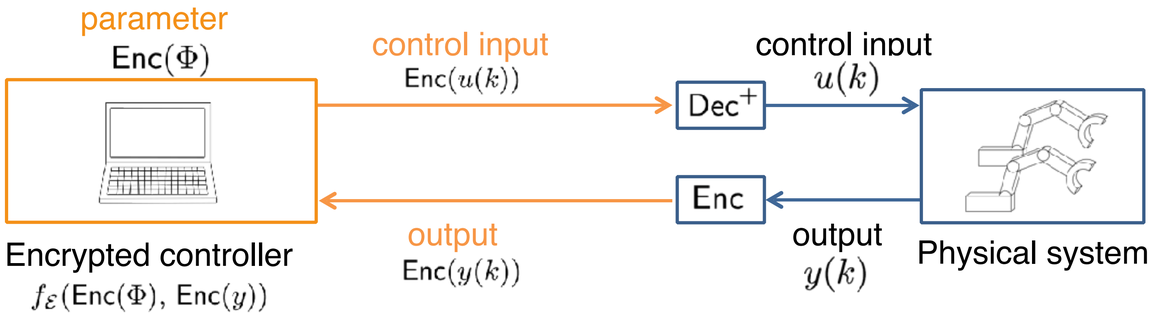
Traditional control system

Only signals over communication links are encrypted.



Encrypted control system

Not only signals over communication links but also parameters of the controller are encrypted.



Controller Encryption

ElGamal encryption scheme $\mathcal{E} = (\mathrm{Gen},\, \mathrm{Enc},\, \mathrm{Dec})$

- Gen(key generation): public key $k_p = (\mathbb{G}, q, g, h)$, private key $k_s = s$
- Enc(encryption): $\mathrm{Enc}(k_p,\, m) := (g^r \mod p,\, mh^r \mod p) = (c_1,\, c_2) = C$
- Dec(decryption): $\mathrm{Dec}(k_s,\, C) := c_2(c_1^s)^{-1} \mod p = m'$

m: plain text C: cipher text

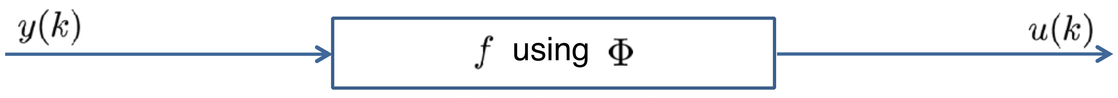
Multiplicative homomorphism

$\mathrm{Enc}(m_1 \times m_2) = \mathrm{Enc}(m_1) * \mathrm{Enc}(m_2)$ $*$: Hadamard product modulo p

Encryption of controller

1. consider a controller $f : \begin{cases} x(k+1) &= Ax(k) + By(k) \\ u(k) &= Cx(k) + Dy(k) \end{cases}$,

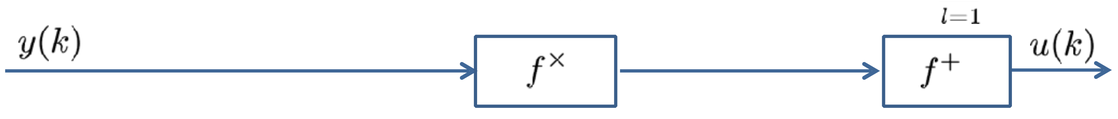
$$\Leftrightarrow \begin{bmatrix} x(k+1) \\ u(k) \end{bmatrix} = f(\Phi,\, \xi(k)) = \Phi\xi(k) \quad \Phi := \begin{bmatrix} A & B \\ C & D \end{bmatrix} \quad \xi := \begin{bmatrix} x \\ y \end{bmatrix}$$



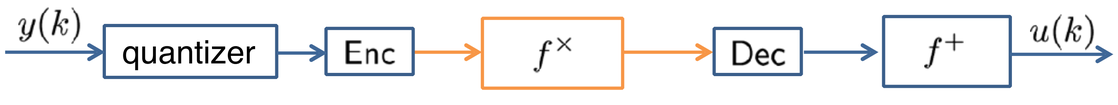
traditional controller

2. divide the controller into $f = f^+ \circ f^\times$ with

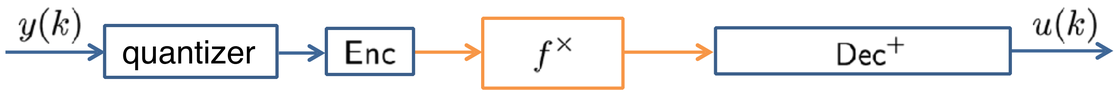
$$f^\times(\Phi,\, \xi) := [\Phi_1\xi_1 \quad \Phi_2\xi_2 \quad \cdots \quad \Phi_\beta\xi_\beta] =: \Psi \text{ and } f^+(\Psi) := \sum_{l=1}^{\beta} \Psi_l \,,$$



3. insert encryption and decryption schemes and a quantizer that converts real numbers to plain texts, and



4. update the decryption block.



Encrypted controller

Experimental Validation

- The encrypted control method enables to be implemented in a practical control system without degradation of the intended control performance.

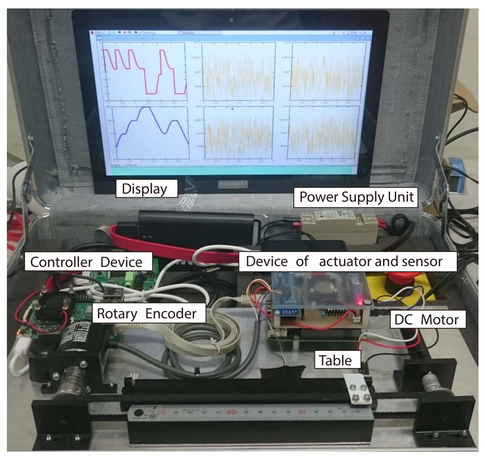
Encrypted PID control[2]

- a position control system with a DC motor
- encryption key: 10, 20, 26 bit
- 26 bit key encryption:

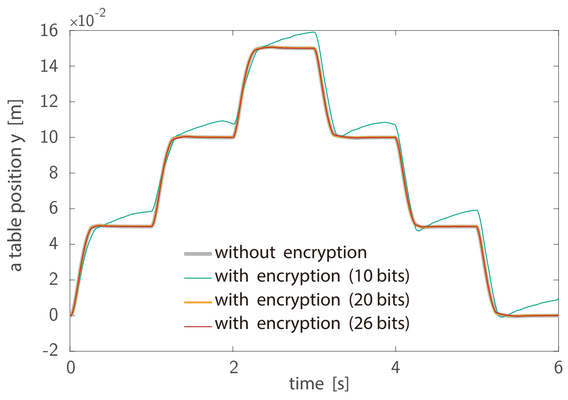
P gain: 3.9×10^{-2} (52069496, 49119951)

I gain : 3.0×10^{-1} (6597337, 42680223)

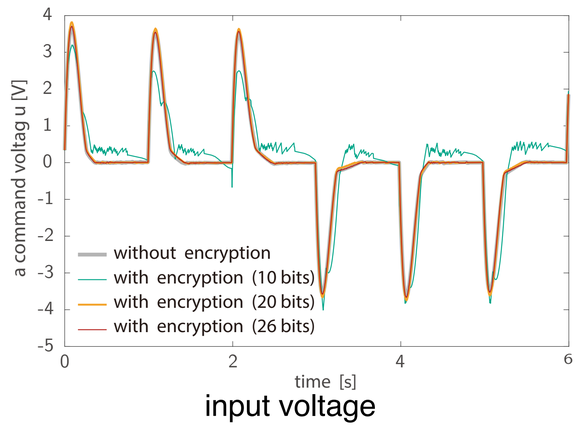
D gain: 2.0×10^{-5} (28459067, 41208506)



developed control system



position of table

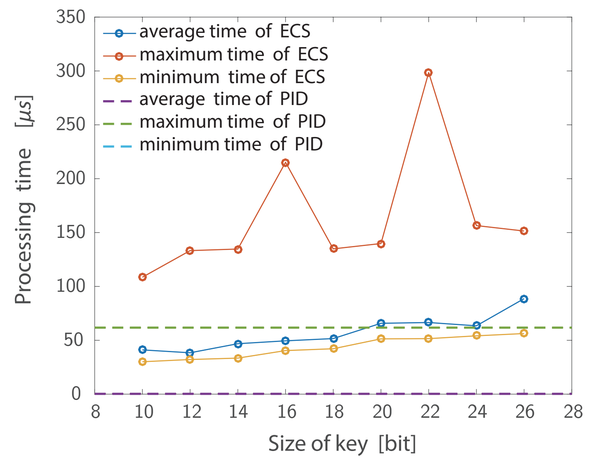


input voltage

Computation time

- Computation cost of the encrypted controller is small enough to be real time.

- 10 to 26 bit key: less than 300 μs
- 128 bit key : 6.05 ms



Other Applications

- observer-based controller, model predictive control, fictitious reference iterative tuning[3], and dynamic quantization[4].

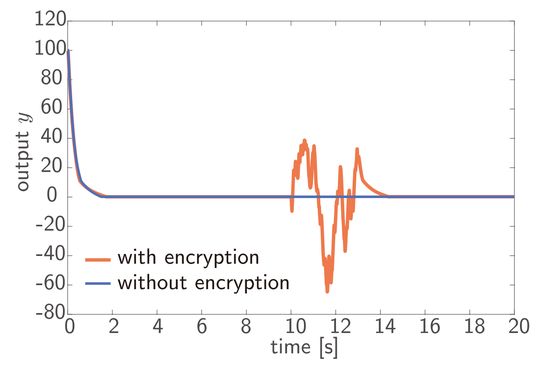
Attack Detection

- ESCs have high sensitivity against falsification attacks and make it easy to detect.

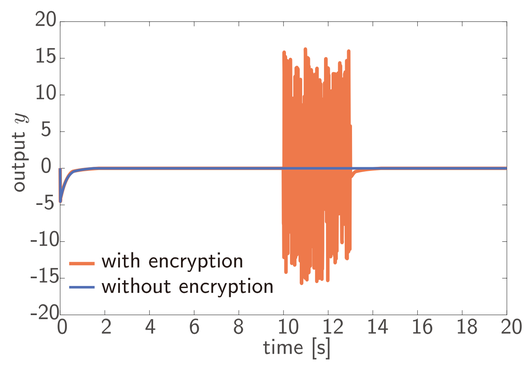
Parameter falsification

$$\begin{bmatrix} 60587507 & 37816909 & 24742046 \\ 59724473 & 2405667 & 38398549 \\ 59518779 & 5935792 & 37459168 \end{bmatrix} \rightarrow 24742049$$

steady state (10 to 13 sec)



position of table



input voltage

Future Work

In future work, we consider the fusion of ECS and fictitious reference iterative tuning.

Reference

[1] K. Kogiso and T. Fujita: Cyber-security enhancement of networked control systems using homomorphic encryption, *IEEE Conference on Decision and Control*, pp. 6838-6843, 2015.
[2] K. Kogiso, R. Baba and K. Masahiro: Development and examination of encrypted control systems, *IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, ThBT4.4, 2018.
[3] S. Souma, O. Kaneko and T. Fujii: A new method of a controller parameter tuning based on input-output data -Fictitious Reference Iterative Tuning-, *8th IFAC Workshop on Adaptation and Learning in Control and Signal Processing*, pp. 789-794, 2004.
[4] M. Kishida: Encrypted control system with quantizer, arXiv:1807.06717v1 [cs.SY], 2018.