Design Procedure for Dynamic Controllers based on LWE-based Homomorphic Encryption to Operate for Infinite Time Horizon

Junsoo Kim[1], Hyungbo Shim[1], and Kyoohyung Han[2]

[1]Seoul National Univ., Korea

[2]Samsung SDS, Korea

The 59th IEEE Conference on Decision and Control

Dec. 18, 2020

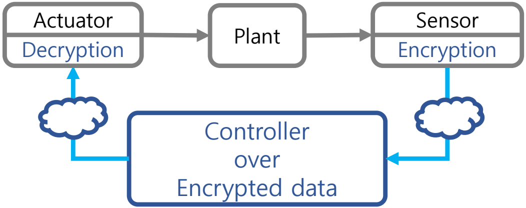
Table of contents

- Problem of running dynamic controllers over encrypted data
- Conversion of state matrix to operate for infinite time horizon[1]
- Parameter design for both security and performance

[1] J. Kim, H. Shim, and K. Han, IEEE TAC, under review, arXiv:1912.07362

Encrypted control

recent approach[1] for protecting networked controllers by encryption



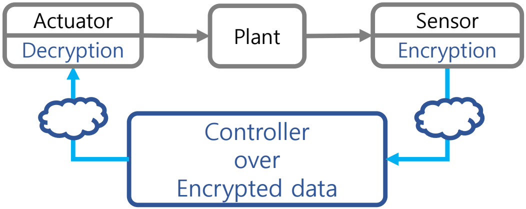
configuration:

- sensor measurements encrypted and transmitted to controller
- control operation directly performed over encrypted data
- controller output decrypted at the actuator

[1]K. Kogiso and T. Fujita, IEEE CDC, 2015

Encrypted control

recent approach[1] for protecting networked controllers by encryption



advantages:

- control data protected even when the operation is performed
- operation without decryption
  $\rightarrow$ secret key can be discarded from the controller

  (enhanced security)

[1] K. Kogiso and T. Fujita, IEEE CDC, 2015

It is based on the use of Homomorphic Encryption (HE).

property of HE:

$$\mathsf{Dec}(\mathsf{Enc}(m_1) \star \mathsf{Enc}(m_2)) = m_1 * m_2$$

Enc: encryption $\star$: operation over ciphertexts

Dec: decryption $*$: operation over plaintexts

known facts:

- In theory, any sort of operation can be done over ciphertexts, for an infinite number of times, by "bootstrapping" of fully HE[1].
- In practice, due to computational complexity of bootstrapping, only addition and multiplication over ciphertexts have been exploited.

[1] C. Gentry, ACM STOC, 2009

Challenge: Implementing dynamic controllers using HE

controller (in stable closed-loop):

$$x(t+1) = Fx(t) + Gy(t),$$
$$u(t) = Hx(t),$$

$x(t) \in \mathbb{R}^n$: state
$y(t) \in \mathbb{R}^p$: input
$u(t) \in \mathbb{R}^m$: output
(bounded)

- recursive multiplication by non-integer numbers
  $\rightarrow$ increasing number of significant digits (even if $x(t)$ bounded)

e.g.,

$$x(t+1) = -0.25 \times x(t) + 1, \quad = -25 \times 10^{-2} \times x(t) + 1, \quad x(0) = 1, \quad \rightarrow$$

$$x(1) = 0.75 = 75 \times 10^{-2}$$
$$x(2) = 0.8125 = 8125 \times 10^{-4}$$
$$x(3) = 0.796875 = 796875 \times 10^{-6}$$
$$x(4) = 0.80078125 = 80078125 \times 10^{-8}$$
$$\vdots$$

(# of significant digits ↑)

- Without bootstrapping, it is not yet possible for HE schemes to discard least significant digits, for infinitely many times.

$\downarrow$

Incapability of operating for infinite time horizon

It has been a common concern.

Existing results consider:

- static operation or finite time operation [A,C,D]
- use of fully HE with bootstrapping [B]
  $\rightarrow$ expensive computational cost
- re-encryption of controller state [E,F,G]
  $\rightarrow$ additional communication channel
- reset of the state [H]
  $\rightarrow$ performance degradation

---

[1] [A] Farokhi, Shames, and Batterham, IFAC Necsys 2016, IFAC CEP 2017
[B] Kim, Lee, Shim, Cheon, Kim, Kim, and Song, IFAC NecSys 2016
[C] Schulze Darup, Redder, Shames, Farokhi, and Quevedo, IEEE CSL 2018
[D] Alexandru, Morari, and Pappas, IEEE CDC 2018
[E] Teranishi, Shimada, and Kogiso, IEEE CDC 2019
[F] Schulze Darup, IFAC WC 2020
[G] Suh and Tanaka, arXiv 2020
[H] Murguia, Farokhi, and Shames, IEEE TAC 2020

Table of contents

- Problem of running dynamic controllers over encrypted data
- Conversion of state matrix to operate for infinite time horizon[1]
- Parameter design for both security and performance

[1] J. Kim, H. Shim, and K. Han, IEEE TAC, under review, arXiv:1912.07362

Motivation from systems having state matrix as integers

e.g.,

$$x(t+1) = -1 \times x(t) + \frac{\lceil e^{-t} \times 10^3 \rfloor}{10^3}, \qquad x(0) = 0.675, \qquad \rightarrow \qquad \begin{aligned} x(0) &= 0.675 = 675 \times 10^{-3} \\ x(1) &= 0.325 = 325 \times 10^{-3} \\ x(2) &= 0.043 = 43 \times 10^{-3} \\ x(3) &= 0.092 = 92 \times 10^{-3} \\ &\vdots \end{aligned}$$

state matrix as integers without scaling $\rightarrow$ fixed scale factor

$+\ x(t)$ bounded under closed-loop stability $\rightarrow$ fixed # of significant digits

[1] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, IEEE CDC 2018

Motivation from systems having state matrix as integers

controller with $F \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$:

$$x(t+1) = Fx(t) + Gy(t),$$
$$u(t) = Hx(t),$$

quantized controller without scale factor for F:

$$\overline{x}(t+1) = F\overline{x}(t) + \left\lceil \frac{G}{\mathsf{s}} \right\rfloor \cdot \overline{y}(t),$$
$$\overline{u}(t) = \left\lceil \frac{H}{\mathsf{s}} \right\rfloor \cdot \overline{x}(t),$$

$\overline{y}(t) := \left\lceil \frac{y(t)}{\mathsf{r}} \right\rfloor \in \mathbb{Z}^{\mathsf{p}}$: quantized input

$\mathsf{r} > 0$: quantization step size

$1/\mathsf{s} \geq 1$: scale factor

Observation

- Under stability, $\mathsf{rs} \cdot \overline{x}(t) \approx x(t)$ for all $t \geq 0$. (fixed scale factor)
- With $F \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$, it operates without discarding least significant digits.

  $\rightarrow$ It can be implemented using only $(+, \times)$ over encrypted data, to operate for an infinite time horizon.

[1] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, IEEE CDC 2018

Proposed approach: Conversion of state matrix to integers

proposed conversion:

$$x(t+1) = Fx(t) + Gy(t) = (F - RH)x(t) + Gy(t) + Ru(t), \quad R \in \mathbb{R}^{\mathsf{n}\times\mathsf{m}}$$
$$u(t) = Hx(t)$$

$$\downarrow \qquad z(t) := Tx(t)$$

$$z(t+1) = T(F - RH)T^{-1}z(t) + TGy(t) + TRu(t),$$
$$u(t) = HT^{-1}z(t),$$

Q. Is it always possible to have $T(F - RH)T^{-1}$ as integers?

A. Yes.

Lemma

Given (F, H), there exists (T, R) such that $T(F - RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$.

Q. How to find (T, R) in practice?

Method for the conversion

Proof of Lemma

Lemma

Given (F, H), there exists (T, R) such that $T(F - RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$.

1. Wlog, the pair (F, H) is observable.

   If not, consider Kalman observability decomposition

$$
\begin{aligned}
z_1(t+1) &= F_1 z_1(t) + G_1 y(t) \\
z_2(t+1) &= F_{21} z_1(t) + F_{22} z_2(t) + G_2 y(t) \\
u(t) &= H_1 z_1(t) + J y(t)
\end{aligned}
$$

   and take the observable z_1-system only.

Lemma

Given (F, H), there exists (T, R) such that $T(F - RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$.

2. Find R such that the eigenvalues of $F - RH$ are integers.

e.g., $$\mathrm{eig}(F) = \{\lambda_1,\ \cdots,\ \lambda_{m_1},\ \sigma_1 \pm j\omega_1,\ \cdots,\ \sigma_{m_2} \pm j\omega_{m_2}\}$$

$\downarrow$ pole-placement

$$\mathrm{eig}(F - RH) = \{\lceil\lambda_1\rfloor,\ \cdots,\ \lceil\lambda_{m_1}\rfloor,\ \lceil\sigma_1\rfloor \pm j\lceil\omega_1\rfloor,\ \cdots,\ \lceil\sigma_{m_2}\rfloor \pm j\lceil\omega_{m_2}\rfloor\}$$

Method for the conversion

Proof of Lemma

Lemma

Given (F, H), there exists (T, R) such that $T(F - RH)T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$.

3. Transform $F - RH$ into Jordan canonical form.

$$T(F - RH)T^{-1}$$

$$= \begin{bmatrix} \lceil\lambda_1\rfloor & & & & & & & \\ & \ddots & & & & & & \\ & & \lceil\lambda_{m_1}\rfloor & & & & & \\ & & & \lceil\sigma_1\rfloor & \lceil\omega_1\rfloor & & & \\ & & & -\lceil\omega_1\rfloor & \lceil\sigma_1\rfloor & & & \\ & & & & & \ddots & & \\ & & & & & & \lceil\sigma_{m_2}\rfloor & \lceil\omega_{m_2}\rfloor \\ & & & & & & -\lceil\omega_{m_2}\rfloor & \lceil\sigma_{m_2}\rfloor \end{bmatrix} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$$

Result

- converted controller over $(\mathbb{Z}, +, \times)$:

$$\overline{z}(t+1) = T(F - RH)T^{-1}\overline{z}(t) + \left\lceil \frac{TG}{\mathsf{s}} \right\rfloor \overline{y}(t) + \left\lceil \frac{TR}{\mathsf{s}} \right\rfloor \lceil \mathsf{s}^2 \cdot \overline{u}(t) \rfloor$$

$$\overline{u}(t) = \left\lceil \frac{HT^{-1}}{\mathsf{s}} \right\rfloor \overline{z}(t),$$

($\lceil \mathsf{s}^2 \cdot \overline{u}(t) \rfloor$ is considered as external input,
i.e., newly encrypted signal transmitted from actuator)

- under closed-loop stability, $\forall \epsilon > 0$, $\exists \mathsf{r}, \mathsf{s}$ s.t. $\|\mathsf{r}\mathsf{s}^2 \cdot \overline{u}(t) - u(t)\| \leq \epsilon$, $\forall t$.

Theorem

Based on the conversion,
linear dynamic controllers can be implemented over encrypted data

- to operate for an infinite time horizon, with equivalent performance,
- without decryption, reset, or bootstrapping for the state $\overline{z}(t)$,
- using only $(+, \times)$ over ciphertexts.

Table of contents

To take advantage of recent LWE[1]-based encryption, effect of injected errors must be considered.

benefits of LWE-based schemes:

- post-quantum cryptosystem
- allows both $(+, \times)$

further benefits[2] of [GSW13]:

- multiplication over encrypted data infinitely many times
- easy implementation

Issue: They all necessarily inject errors for security.
$\rightarrow$ error suppression by stability
$\rightarrow$ appropriate parameter design required for control performance

e.g., $\mathbf{c}_1 = \mathsf{Enc}(m_1)$, $\mathbf{c}_2 = \mathsf{Enc}(m_2)$

$\rightarrow$ $\mathsf{Dec}(\mathsf{Mult}(\mathbf{c}_1, \mathbf{c}_2)) = m_1 m_2 + \Delta$, Δ: error growth

$\rightarrow$ $\mathbf{c}_2' = \mathsf{Enc}(\mathsf{L} m_2)$, $\mathsf{L} \in \mathbb{N} \implies \mathsf{Dec}(\mathsf{Mult}(\mathbf{c}_1, \mathbf{c}_2')) = \mathsf{L} \cdot m_1 m_2 + \Delta$

$\implies$ increasing L to deal with error growth

Q. Constraints or issues when increasing L?

[1] Learning With Errors problem, introduced in [O. Regev, JACM 2009]
[2] Gentry, Sahai, and Waters, CRYPTO 2013

Conditions that should not be affected when increasing L

- desired λ-bit security:

$$n \log q \geq k_1 \lambda \left(\log^2 q + k_2\right) =: f_1(\lambda, q) \implies n = n(\mathsf{L})$$

n: ciphertext dimension, q: modulus

- size of plaintext space that covers the range of $u(t)$:

$$q \geq \frac{(\mathrm{range}(u(t)) + 2\epsilon + \mathsf{r}) \cdot \mathsf{L}}{\mathsf{rs}^2} =: f_2(\mathsf{L}, \mathsf{r}, \mathsf{s}) \implies q = q(\mathsf{L})$$

- $(1/\mathsf{r}, 1/\mathsf{s})$ should be chosen large to suppress errors due to quantization.

Parameter design

To satisfy all conditions, define the other parameters as functions of L, and then increase L.

Result

implemented controller with effect of injected errors:

$$\overline{z}(t+1) = T(F-RH)T^{-1}\overline{z}(t) + \left\lceil \frac{TG}{\mathsf{s}} \right\rfloor \overline{y}(t) + \left\lceil \frac{TR}{\mathsf{s}} \right\rfloor \left\lceil \mathsf{s}^2 \cdot \overline{u}(t) \right\rfloor + \Delta_z(t, \mathsf{L})$$

$$\overline{u}(t) = \left\lceil \frac{HT^{-1}}{\mathsf{s}} \right\rfloor \overline{z}(t) + \Delta_u(t, \mathsf{L}),$$

Theorem

- With the proposed design, $\exists\, k_1 > 0, k_2 > 0$ s.t.

$$\left\| \begin{bmatrix} \Delta_z(t, \mathsf{L}) \\ \Delta_u(t, \mathsf{L}) \end{bmatrix} \right\| \le \frac{k_1 (\log \mathsf{L})^{k_2}}{\mathsf{L}} \to 0 \quad \text{as} \quad \mathsf{L} \to \infty.$$

- Under closed-loop stability, given $\epsilon > 0$ and $\lambda > 0$, $\exists(\mathsf{L}, \mathsf{r}, \mathsf{s}, n, q)$ s.t.
  - $\| \mathsf{rs}^2 \cdot \overline{u}(t) - u(t) \| \le \epsilon$, for all $t \ge 0$.
  - the cryptosystem guarantees λ-bit security.

Conclusion

Two issues that hinder unlimited arithmetic operation,
which have been handled with bootstrapping in cryptography:

- recursive multiplication by non-integer numbers
  $\rightarrow$ solved by conversion of state matrix with re-encrypted controller output
- growth of injected errors under recursive operation
  $\rightarrow$ solved by closed-loop stability with parameter design

It enables dynamic controllers to operate over encrypted data

- for infinite time horizon with desired performance and security,
- without use of bootstrapping, decryption, or reset of the state.

Thank you for your time!

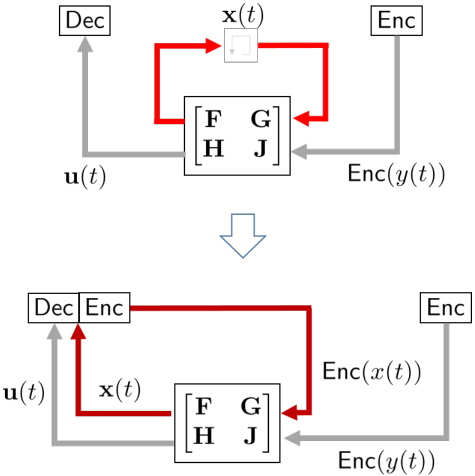
email: kjs9044@snu.ac.kr

homepage: kjs9044.wordpress.com / post.cdsl.kr

Re-encryption of the state is not considered as a solution.

recursive state update:

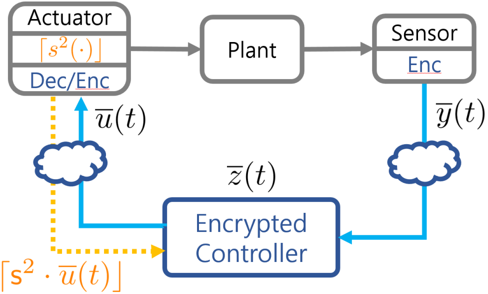
state re-encryption:



Re-encryption of state enables operation for infinite time horizon, but

- it increases network throughput, proportionally to the state dimension.
- controller state decrypted at the actuator $\Longrightarrow$ security issue

Instead, we make use of re-encrypted controller output.



It is based on the rationale that

- transmission of $\mathbf{u}(t)$ to actuator is necessary for control,
- so it can be re-encrypted and transmitted back to controller, as long as the communication is bi-directional.