Method for Running Dynamic Systems over Encrypted Data for Infinite Time Horizon without Bootstrapping and Re-encryption

Junsoo Kim[1], Hyungbo Shim[2], Henrik Sandberg[1], Karl H. Johansson[1]

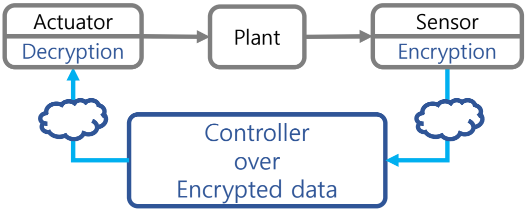
[1]KTH Royal Institute of Technology, Sweden [2]Seoul National Univ., Korea

The 60th IEEE Conference on Decision and Control

Dec. 16, 2021

Table of contents

Advantage of Encrypted control



- control operation directly over encrypted data
- protection of data even when the computation is performed
- operation without decryption key $\implies$ enhanced security

[1] Kogiso & Fujita, CDC, 2015
[2] Schulze Darup, Alexandru, Quevedo, & Pappas, Control Systems Magazine, 2021

It can be implemented with Homomorphic Encryption (HE).

Properties for $(+, \times)$:

$$\begin{aligned} c_1 &= \mathsf{Enc}(m_1) +_c \mathsf{Enc}(m_2) \\ c_2 &= \mathsf{Enc}(m_1) \times_c \mathsf{Enc}(m_2) \end{aligned} \quad \rightarrow \quad \begin{aligned} \mathsf{Dec}(c_1) &= m_1 + m_2 \\ \mathsf{Dec}(c_2) &= m_1 \times m_2 \end{aligned}$$

$+_c, \times_c$: operation over encrypted data, Enc: encryption, Dec: decryption

- In theory[1], "bootstrapping of fully HE" enables any sort of operation.
- For real-time control, the properties for $(+, \times)$ have been exploited.
  (because of computational complexity of bootstrapping)

[1] Gentry, ACM STOC, 2009

Issue when implementing dynamic systems using HE

e.g.,

$$x(t+1) = -0.25 \times x(t) + 1$$
$$x(0) = 1$$

$$\rightarrow \quad \begin{aligned} x(1) &= 0.75 \\ x(2) &= 0.8125 \\ x(3) &= 0.796875 \\ x(4) &= 0.80078125 \end{aligned}$$

(# of the decimal digits of $x(t)$ increases, despite that $|x(t)|$ is bounded.)

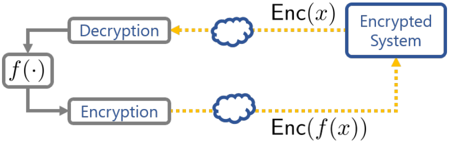
- The state is recursively multiplied by non-integer numbers, in general.
- Rounding operation is needed periodically to discard Least Significant Bits (LSB), but it is not yet possible for HE, unless the bootstrapping is used.

$$\downarrow$$

Incapability of operating for infinite time horizon

Re-encryption has been used for functions other than $(+, \times)$.

Re-encryption for $f(\cdot)$:



e.g.,

- projection for MPC (as in [Schulze Darup, IFAC WC, 2020])
- division/inversion for data driven control [Alexandru, Tsiamis, & Pappas, CDC, 2020]
- maximum operation for RL [Suh & Tanaka, ACC, 2021]
- methods based on Multi-Party Computation, assuming "non-colluding models"

for discarding LSB in linear systems:

- state re-encryption (as in [Teranishi & Kogiso, CDC, 2020])
- (exception) reset to initial value [Murguia, Farokhi, & Shames, TAC, 2020]
- output re-encryption [Kim, Shim, & Han, CDC, 2020]

However, without the presence of the decryption key, the system cannot continue the operation by itself.

Problem of interest

$x(t) \in \mathbb{R}^{\mathsf{n}}$: state,
$u(t) \in \mathbb{R}^{\mathsf{m}}$: input,
$y(t) \in \mathbb{R}^{\mathsf{p}}$: output,
$x_0 \in \mathbb{R}^{\mathsf{n}}$: initial state,
$\{A, B, C, D\}$: real matrices,

Given a dynamic system over $\mathbb{R}$,

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t), \quad x(0) = x_0, \\ y(t) &= Cx(t) + Du(t), \end{aligned} \tag{$\spadesuit$}$$

($x(t), u(t), y(t)$: bounded)

the problem is to construct a system over encrypted data, such that

- it can operate without re-encryption and bootstrapping,
- it can run for an infinite time horizon, with equivalent performance.

Problem of interest

$x(t) \in \mathbb{R}^{\mathsf{n}}$: state,
$u(t) \in \mathbb{R}^{\mathsf{m}}$: input,
$y(t) \in \mathbb{R}^{\mathsf{p}}$: output,
$x_0 \in \mathbb{R}^{\mathsf{n}}$: initial state,
$\{A, B, C, D\}$: real matrices,

Given a dynamic system over $\mathbb{R}$,

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t), \quad x(0) = x_0, \\ y(t) &= Cx(t) + Du(t), \end{aligned} \tag{$\spadesuit$}$$

($x(t), u(t), y(t)$: bounded)

the problem is to convert ($\spadesuit$) to a system over $\mathbb{Z}$, which

- operates only with $(+, \times)$, without discarding LSB
- can recover $\{y(t)\}_{t=0}^{\infty}$ from the output, with a static function.

Table of contents

Advantage of state matrix as integers

conversion when $A \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$:

$$\begin{aligned}\overline{x}(t+1) &= A\,\overline{x}(t) + \left\lceil \frac{B}{\mathsf{s}} \right\rfloor \cdot \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \\ \overline{y}(t) &= \left\lceil \frac{C}{\mathsf{s}} \right\rfloor \cdot \overline{x}(t) + \left\lceil \frac{D}{\mathsf{s}^2} \right\rfloor \cdot \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \\ \overline{x}(0) &= \left\lceil \frac{x_0}{\mathsf{rs}} \right\rfloor \qquad (\clubsuit)\end{aligned}$$

$\Leftrightarrow$

given system w/ perturbation:

$$\begin{aligned}x(t+1) &= Ax(t) + Bu(t) + e_x(t) \\ y(t) &= Cx(t) + Du(t) + e_y(t) \\ x(0) &= x_0 + e_0\end{aligned}$$

$\mathsf{r} > 0$: quantization step size
$1/\mathsf{s} \geq 1$: scale factor
$e_x(t), e_y(t), e_0$: quantization error

Observation

- If $A \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}}$, then $(\clubsuit)$ operates over $(\mathbb{Z}, +, \times)$, with $\begin{matrix} x(t) \equiv \mathsf{rs} \cdot \overline{x}(t) \\ y(t) \equiv \mathsf{rs}^2 \cdot \overline{y}(t) \end{matrix}$. (without discarding LSB)
- $\left\| \begin{bmatrix} e_x(t) \\ e_y(t) \\ e_0 \end{bmatrix} \right\| \to 0$ as $\mathsf{r} \to 0$ and $\mathsf{s} \to 0$.

[1] Cheon, Han, Kim, Kim, & Shim, CDC, 2018

So, we propose conversion of state matrix to integers.

given system: (w/ perturbation)

$$x(t+1) = Ax(t) + Bu(t) + e_x(t)$$
$$y(t) = Cx(t) + Du(t)$$
$$(A \notin \mathbb{Z}^{\mathsf{n}\times\mathsf{n}})$$

Theorem

For any $\delta > 0$, $\exists\, e_x(t)$ s.t. $\|e_x(t)\| \leq \delta$ and $\exists$ periodically time varying system

$$\xi(t+1) = F_\sigma \xi(t) + G_\sigma u(t), \qquad \sigma = t \mod k, \qquad k \in \mathbb{N},$$
$$y_\xi(t) = H_\sigma \xi(t) + Du(t), \qquad \text{with } F_\sigma \in \mathbb{Z}^{l\times l}, \qquad l \in \mathbb{N},$$

s.t. $\begin{array}{c} x(t) \equiv T_\sigma \xi(t) \\ y(t) \equiv y_\xi(t) \end{array}$ with some $\{T_\sigma\}_{\sigma=0}^{k-1}$.

$F_\sigma \in \mathbb{Z}^{l\times l}$ $\Rightarrow$ operation over $(\mathbb{Z}, +, \times)$ w/o discarding LSB $\Rightarrow$ encrypted system w/o re-encryption

Sketch of proof

Method for the conversion

Decomposition into stable/unstable part:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned} \quad \Leftrightarrow \quad \begin{aligned} z_s(t+1) &= A_s z_s(t) + B_s u(t) \\ z_u(t+1) &= A_u z_u(t) + B_u u(t) \\ y(t) &= C_s z_s(t) + C_u z_u(t) + Du(t) \end{aligned}$$

A_s: Schur stable; eigenvalue $\lambda \in \mathbb{C}$ of A_s is s.t. $|\lambda| < 1$
A_u: anti-stable; eigenvalue $\lambda \in \mathbb{C}$ of A_u is s.t. $|\lambda| \geq 1$

1. unstable part $\rightarrow$ approximation of eigenvalues to algebraic integers
2. stable part $\rightarrow$ Finite Impulse Response (FIR) approximation

1. Conversion for the unstable part

Approximation of eigenvalues to algebraic integers

Idea: for each eigenvalue $|\lambda| \geq 1$, choose $a \approx \lambda$ s.t. $a^k \in \mathbb{Z}$ with some $k \in \mathbb{N}$

e.g.,

$$\begin{aligned} z(t+1) &= 2.37 z(t) + u(t) \\ y(t) &= z(t) \end{aligned} \quad \Rightarrow \quad \begin{aligned} \tilde{z}(t+1) &= a\tilde{z}(t) + u(t) \\ \tilde{y}(t) &= \tilde{z}(t) \end{aligned}$$

- Let $a := \sqrt[5]{\lceil (2.37)^5 \rfloor} = 2.3714\ldots$ so that $a^5 = \lceil (2.37)^5 \rfloor \in \mathbb{Z}$.
- conversion:

(In general, $a = \sqrt[k]{\lceil \lambda^k \rfloor} \to \lambda$ as $k \uparrow$)

$$\xi(t) := a^{-(t \bmod 5)} \tilde{z}(t)$$

$$\downarrow$$

$$\xi(t+1) = \begin{cases} \xi(t) + a^{-(t+1 \bmod 5)} u(t), & \text{if } \ t \bmod 5 = 0,1,2,3, \\ a^5 \xi(t) + u(t), & \text{if } \ t \bmod 5 = 4, \end{cases}$$

$$\tilde{y}(t) = a^{(t \bmod 5)} \xi(t)$$

(perturbation + time-varying transformation $\rightarrow$ state matrix as integers)

For the general case, for the unstable part:

Lemma

For any $\delta > 0$ and anti-stable $A_u \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$, there exists $\tilde{A}_u \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$

$$\text{s.t.} \quad \|A_u - \tilde{A}_u\| \le \delta \quad \text{and} \quad T\tilde{A}_u^k T^{-1} \in \mathbb{Z}^{\mathsf{n}\times\mathsf{n}},$$

with some $T \in \mathbb{R}^{\mathsf{n}\times\mathsf{n}}$ and $k \in \mathbb{N}$.

conversion:

$$\begin{aligned} z(t+1) &= A_u z(t) + B_u u(t) \\ y(t) &= C_u z(t) \end{aligned} \quad \Rightarrow \quad \begin{aligned} \tilde{z}(t+1) &= \tilde{A}_u \tilde{z}(t) + B_u u(t) \\ \tilde{y}(t) &= C_u \tilde{z}(t) \end{aligned}$$

$$\downarrow \;\; \xi(t) := T\tilde{A}_u^{-(t \bmod k)} \tilde{z}(t)$$

$$\xi(t+1) = \begin{cases} \xi(t) + T\tilde{A}_u^{-(t+1 \bmod k)} B_u u(t), & \text{if } t \bmod k = 0, \cdots, k-2, \\ T\tilde{A}_u^k T^{-1} \xi(t) + T B_u u(t), & \text{if } t \bmod k = k-1, \end{cases}$$

$$\tilde{y}(t) = C_u \tilde{A}_u^{(t \bmod k)} T^{-1} \xi(t)$$

(perturbation + time-varying transformation → state matrix as integers)

2. Conversion for the stable part

Finite Impulse Response (FIR) approximation for the stable part:

$$\begin{aligned} z_s(t+1) &= A_s z_s(t) + B_s u(t) \quad \in \mathbb{R}^{\mathsf{n}_s} \\ y_s(t) &= C_s z_s(t) \end{aligned}$$

$$\downarrow$$

$$\begin{bmatrix} \tilde{z}_{s,1}(t+1) \\ \tilde{z}_{s,2}(t+1) \\ \vdots \\ \tilde{z}_{s,k}(t+1) \end{bmatrix} = \begin{bmatrix} 0 & I_{\mathsf{n}_s} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I_{\mathsf{n}_s} \\ 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} \tilde{z}_{s,1}(t) \\ \tilde{z}_{s,2}(t) \\ \vdots \\ \tilde{z}_{s,k}(t) \end{bmatrix} + \begin{bmatrix} B_s \\ A_s B_s \\ \vdots \\ A_s^{k-1} B_s \end{bmatrix} u(t) \quad \in \mathbb{R}^{k\mathsf{n}_s}$$

$$\tilde{y}_s(t) = C_s \tilde{z}_{s,1}(t)$$

- FIR $\Rightarrow$ state matrix as integers
- A_s is Schur stable $\Rightarrow$ $\left\| \begin{bmatrix} z_s(t) - \tilde{z}_{s,1}(t) \\ y_s(t) - \tilde{y}_s(t) \end{bmatrix} \right\| \to 0$ as $k \uparrow$.

Main result

proposed implementation over $(\mathbb{Z}, +, \times)$, with F_σ as integers:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) + e_x(t) \\ y(t) &= Cx(t) + Du(t) + e_y(t) \\ x(0) &= x_0 + e_0 \end{aligned} \quad \Leftrightarrow \quad \begin{aligned} \overline{\xi}(t+1) &= F_\sigma \overline{\xi}(t) + \left\lceil \frac{G_\sigma}{\mathsf{s}} \right\rfloor \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \\ \overline{y}(t) &= \left\lceil \frac{H_\sigma}{\mathsf{s}} \right\rfloor \overline{\xi}(t) + \left\lceil \frac{D}{\mathsf{s}^2} \right\rfloor \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \\ \overline{\xi}(0) &= \left\lceil \frac{\xi_0}{\mathsf{rs}} \right\rfloor, \qquad \sigma = t \mod k, \end{aligned}$$

where $\begin{bmatrix} e_x(t) \\ e_y(t) \\ e_0 \end{bmatrix}$: (approximation error) + (quantization error), so that $\begin{aligned} x(t) &\equiv \mathsf{rs} \cdot T_\sigma \overline{\xi}(t) \\ y(t) &\equiv \mathsf{rs}^2 \cdot \overline{y}(t) \end{aligned}$

Theorem

- It can operate using HE without re-encryption, for inf. time horizon.
- $\left\| \begin{bmatrix} e_x(t) \\ e_y(t) \\ e_0 \end{bmatrix} \right\| \to 0$ as $\mathsf{r} \to 0$, $\mathsf{s} \to 0$, and $k \to \infty$.
- Assuming that the (closed-loop) system is stable w.r.t. $\{e_x(t), e_y(t), e_0\}$, the performance is guaranteed.

Table of contents

Method for encrypting both signals and matrices

- Any additively HE can be applied, with encrypting $\{x(t), u(t), y(t)\}$ only.
- To encrypt $\{F_\sigma, G_\sigma, H_\sigma, D\}$ as well, the method of [1] can be used.
  - use of "GSW" scheme for recursive multiplication of $\mathsf{Enc}(F_\sigma)$:

$$\mathbf{x}^+ = \mathsf{Enc}(F_\sigma) \times_c \mathbf{x} \quad \rightarrow \quad \mathsf{Dec}(\mathbf{x}^+) = F_\sigma \cdot \mathsf{Dec}(\mathbf{x}) + \Delta$$

($\mathbf{x}$: encrypted state)

  - Unlike most other schemes, it allows $\times_c$ infinite number of times, where the error growth Δ can be controlled.

[1] Kim, Shim, & Han, under review for TAC, arXiv:1912.07362

Method for choosing the size of message space

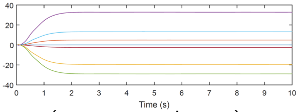
Technically, the encrypted system operates over $\mathbb{Z}_q = \{0, 1, 2, \cdots, q-1\}$:

$$\bar{\xi}(t+1) = F_\sigma \bar{\xi}(t) + \left\lceil \frac{G_\sigma}{\mathsf{s}} \right\rfloor \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \mod q, \qquad \bar{\xi}(0) = \left\lceil \frac{\xi_0}{\mathsf{rs}} \right\rfloor \mod q,$$

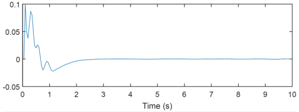
$$\bar{y}(t) = \left\lceil \frac{H_\sigma}{\mathsf{s}} \right\rfloor \bar{\xi}(t) + \left\lceil \frac{D}{\mathsf{s}^2} \right\rfloor \left\lceil \frac{u(t)}{\mathsf{r}} \right\rfloor \mod q,$$

where $q \in \mathbb{N}$ has been chosen to cover the ranges of $\{x(t), u(t), y(t)\}$.

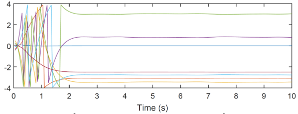
$\rightarrow$ In fact, it is enough to cover the range of the output $y(t)$ only.



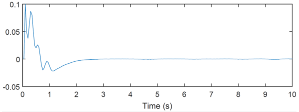
(un-encrypted state)



(un-encrypted output)



(encrypted state)

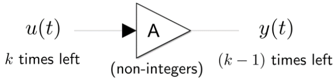


(encrypted output)

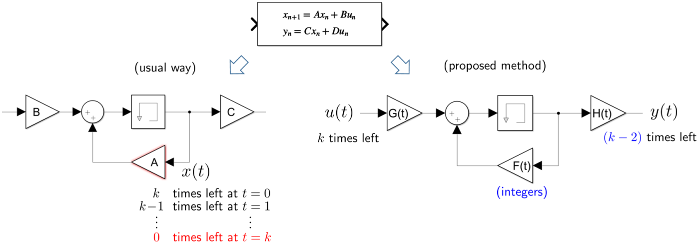
[1] Kim, Shim, & Han, under review for TAC, arXiv:1912.07362

Conclusion

Without use of bootstrapping and re-encryption,
# of multiplication by non-integers is limited for encrypted messages.



By conversion of the state matrix to integers, we have proposed that linear systems can be encrypted to run for an infinite time horizon.



Thank you!

Email: junsoo@kth.se / Homepage: junsookim4.wordpress.com