The 13th Asian Control Conference (ASCC 2022)
Tutorial: Homomorphic Encryption and Its Application to Feedback Control

Encrypted Control Using Partially Homomorphic Encryption

Kaoru Teranishi

The University of Electro-Communications
Research Fellow of Japan Society for the Promotion of Science

KIMILAB

Homomorphic Encryption (1/2)

Homomorphic encryption is encryption that allows arithmetic with encrypted data.

Syntax

$\mathsf{KeyGen}(1^\lambda)$: Key-generation function takes a security parameter 1^λ and outputs a public key pk and secret key sk.

$\mathsf{Enc}(\mathsf{pk}, m)$: Encryption function takes a public key and plaintext m and outputs a ciphertext.

$\mathsf{Dec}(\mathsf{sk}, c)$: Decryption function takes a secret key and ciphertext c and outputs a plaintext.

$\mathsf{Eval}(c_1, c_2)$: Evaluation function takes two ciphertexts and outputs a ciphertext.

Homomorphic Encryption (2/2)

- Partially Homomorphic Encryption (PHE)
  - Multiplicative Homomorphic Encryption
  - Additive Homomorphic Encryption
- Somewhat Homomorphic Encryption (SWHE)
- Leveled Fully Homomorphic Encryption (LFHE)
- Fully Homomorphic Encryption (FHE)

	Arithmetic	Computation costs
PHE	**Multiplication or addition**	**Light**
SWHE/LFHE	Limited number of multiplication and addition	Medium
FHE	Any function	Heavy

Partially Homomorphic Encryption

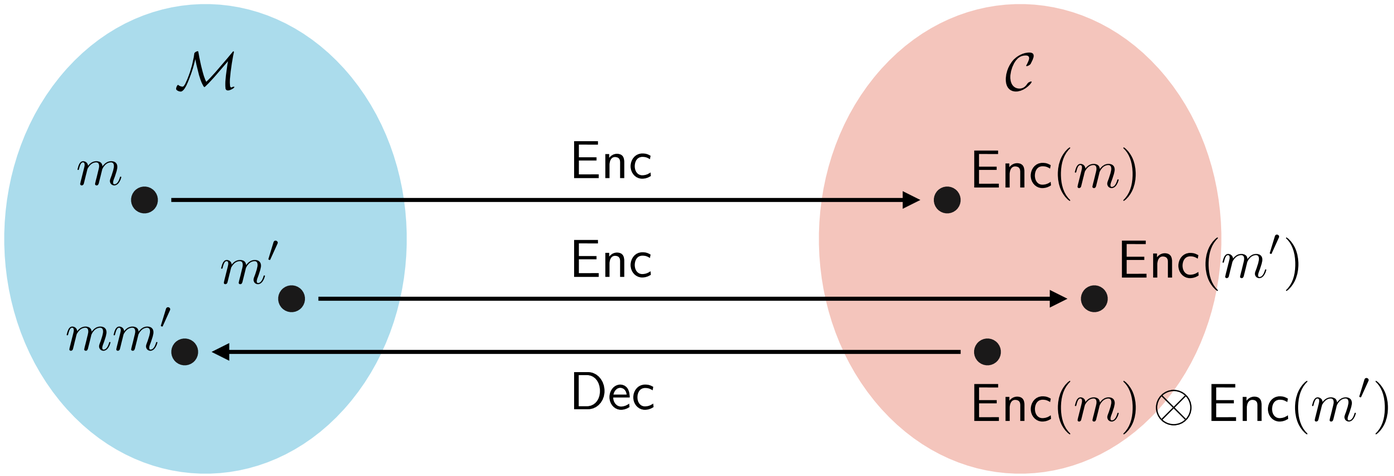
Partially homomorphic encryption is encryption that allows either addition or multiplication with encrypted data.

Multiplicative homomorphic encryption

- RSA encryption
- **ElGamal encryption**

$$\mathsf{Eval}(c, c') = c \otimes c'$$

$$\mathsf{Dec}(\mathsf{Enc}(m) \otimes \mathsf{Enc}(m')) = mm'$$



Additive homomorphic encryption

- Paillier encryption

$$\mathsf{Eval}(c, c') = c \oplus c'$$

$$\mathsf{Dec}(\mathsf{Enc}(m) \oplus \mathsf{Enc}(m')) = m + m'$$

ElGamal Encryption (1/2)

Algorithms

KeyGen : $1^\lambda \mapsto (\mathsf{pk}, \mathsf{sk}) = ((\mathbb{G}, g, p, q, h), s)$

Enc : $(\mathsf{pk}, m) \mapsto c = (c_1, c_2) = (g^r \bmod p, mh^r \bmod p)$

Dec : $(\mathsf{sk}, c) \mapsto m = {c_1}^{-s} c_2 \bmod p$

Eval : $(c, c') \mapsto (c_1 c_1' \bmod p, c_2 c_2' \bmod p)$

Cyclic group

$\mathbb{G} = \{g^i \bmod p \mid i \in \mathbb{Z}_q\}$

g: Generator q: λ-bit prime $p = 2q + 1$: Safe prime

Key generation

$s \in \mathbb{Z}_q$: Random number $h = g^s \bmod p$

$\mathcal{M} = \mathbb{G}$: Plaintext space $\mathcal{C} = \mathbb{G}^2$: Ciphertext space

ElGamal Encryption (2/2)

Encryption

$$c = (c_1, c_2) = (g^r \bmod p, mh^r \bmod p),\ m \in \mathcal{M} \qquad r \in \mathbb{Z}_q$$: Random number

Decryption

$$c_1{}^{-s} c_2 = (g^r)^{-s} m h^r = g^{-sr} m g^{sr} = m \bmod p,\ c = (c_1, c_2) \in \mathcal{C}$$

g^{-1}: Modular multiplicative inverse of g

Example: $g = 3,\ p = 11$

$$g^{-1} = 4 \neq \frac{1}{3} \quad (\because 3 \cdot 4 = 12 = 1 \bmod 11)$$

Evaluation

$$c \otimes c' = (c_1 c_1' \bmod p, c_2 c_2' \bmod p),\ c = (c_1, c_2),\ c' = (c_1', c_2')$$

Example (1/2)

Let $\lambda = 3$. Then, $q = 5$, $p = 2q + 1 = 11$, and $g = 3$ are valid parameters.

$s = 1 \in \mathbb{Z}_5$ is chosen randomly, and $h = g^s = 3^1 = 3 \bmod 11$ is computed.

A plaintext space is $\mathcal{M} = \mathbb{G} = \{g^0, g^1, g^2, g^3, g^4\} = \{1, 3, 4, 5, 9\}$. A ciphertext space is $\mathcal{C} = \mathbb{G}^2$.

Encryption

Let $m = 3, m' = 4 \in \mathcal{M}$. $r = 1, r' = 5 \in \mathbb{Z}_q$ are chosen randomly.

Ciphertexts are computed as

$$\mathsf{Enc}(\mathsf{pk}, m) = c = (c_1, c_2) = (g^r \bmod p, mh^r \bmod p) = (3^1 \bmod 11, 3 \cdot 3^1 \bmod 11) = (3, 9)$$

$$\mathsf{Enc}(\mathsf{pk}, m') = c' = (c'_1, c'_2) = (g^{r'} \bmod p, m'h^{r'} \bmod p) = (3^5 \bmod 11, 4 \cdot 3^5 \bmod 11) = (1, 4)$$

Evaluation

$$\tilde{c} = c \otimes c' = (c_1 c'_1 \bmod p, c_2 c'_2 \bmod p) = (3 \cdot 1 \bmod 11, 9 \cdot 4 \bmod 11) = (3, 3)$$

Example (2/2)

Decryption

$$\mathsf{Dec}(\mathsf{sk}, c) = {c_1}^{-s} c_2 = 3^{-1} \cdot 9 = 4 \cdot 9 = 36 = 3 \bmod 11$$

$$\mathsf{Dec}(\mathsf{sk}, c') = {c'_1}^{-s} c'_2 = 1^{-1} \cdot 4 = 1 \cdot 4 = 4 \bmod 11$$

$$\mathsf{Dec}(\mathsf{sk}, \tilde{c}) = c_1 {c'_1}^{-s} c_2 c'_2 = 3^{-1} \cdot 3 = 4 \cdot 3 = 12 = 1 \bmod 11$$

Correctness

$$m = 3, m' = 4 \in \mathcal{M}$$

$$mm' = 3 \cdot 4 = 12 = 1 \bmod 11$$

Encrypting Static Controller

State-feedback controller

$$u_t = Fx_t,\ u \in \mathbb{R}^m,\ x \in \mathbb{R}^n,\ F \in \mathbb{R}^{m \times n},\ t \in \mathbb{Z}^+$$

$$= \left[\sum_{j=1}^{n} F_{1j} x_{j,t} \quad \sum_{j=1}^{n} F_{2j} x_{j,t} \quad \cdots \quad \sum_{j=1}^{n} F_{mj} x_{j,t} \right]^\top$$

Multiplication is computed over a ciphertext space.

Addition is computed after decryption.

$$u_t = \left[\sum_{j=1}^{n} \mathsf{Dec}(\mathsf{Enc}(F_{1j}) \otimes \mathsf{Enc}(x_{j,t})) \quad \cdots \quad \sum_{j=1}^{n} \mathsf{Dec}(\mathsf{Enc}(F_{mj}) \otimes \mathsf{Enc}(x_{j,t})) \right]^\top$$

Encrypting Dynamic Controller (1/2)

Dynamic feedback controller

$$
\begin{aligned}
z_{t+1} &= Az_t + By_t \\
u_t &= Cz_t + Dy_t \qquad\qquad z \in \mathbb{R}^{n_c},\ u \in \mathbb{R}^m,\ y \in \mathbb{R}^\ell
\end{aligned}
$$

$$
\iff \underbrace{\begin{bmatrix} z_{t+1} \\ u_t \end{bmatrix}}_{\psi_t} = \underbrace{\begin{bmatrix} A & B \\ C & D \end{bmatrix}}_{\Phi} \underbrace{\begin{bmatrix} z_t \\ y_t \end{bmatrix}}_{\xi_t}
$$

$$
\psi_t = \begin{bmatrix} \sum_{j=1}^{n_c+\ell} \Phi_{1j}\xi_{j,t} & \sum_{j=1}^{n_c+\ell} \Phi_{2j}\xi_{j,t} & \cdots & \sum_{j=1}^{n_c+\ell} \Phi_{n_c+m,j}\xi_{j,t} \end{bmatrix}^\top
$$

$$
= \begin{bmatrix} \sum_{j=1}^{n_c+\ell} \mathsf{Dec}(\mathsf{Enc}(\Phi_{1j}) \otimes \mathsf{Enc}(\xi_{j,t})) & \cdots & \sum_{j=1}^{n_c+\ell} \mathsf{Dec}(\mathsf{Enc}(\Phi_{n_c+m,j}) \otimes \mathsf{Enc}(\xi_{j,t})) \end{bmatrix}^\top
$$

Encrypting Dynamic Controller (2/2)

Denote a dynamic controller by a map.

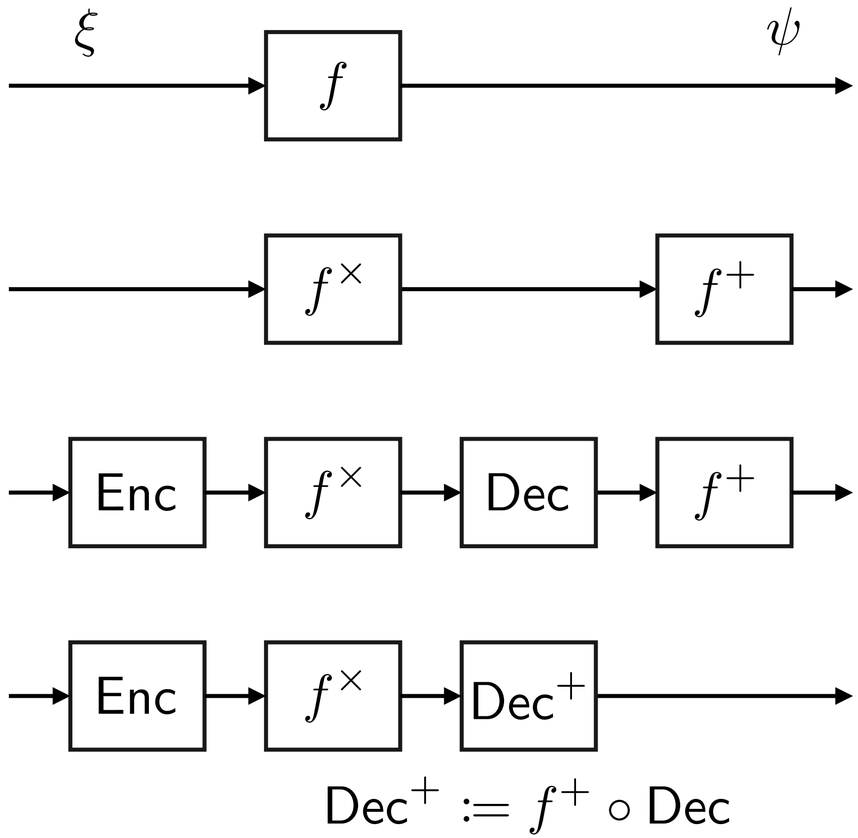
$$f : (\Phi, \xi) \mapsto \psi = \Phi\xi$$

Controller reconstruction

$$f = f^{+} \circ f^{\times}$$

$$f^{\times} : (\Phi, \xi) \mapsto \Psi = \begin{bmatrix} \Phi_{11}\xi_1 & \cdots & \Phi_{1,n_c+\ell}\xi_{n_c+\ell} \\ \vdots & \ddots & \vdots \\ \Phi_{n_c+m,1}\xi_1 & \cdots & \Phi_{n_c+m,n_c+\ell}\xi_{n_c+\ell} \end{bmatrix}$$

$$f^{+} : \Psi \mapsto \psi = \begin{bmatrix} \sum_{j=1}^{n_c+\ell} \Psi_{1j} & \cdots & \sum_{j=1}^{n_c+\ell} \Psi_{n_c+m,j} \end{bmatrix}^{\top}$$



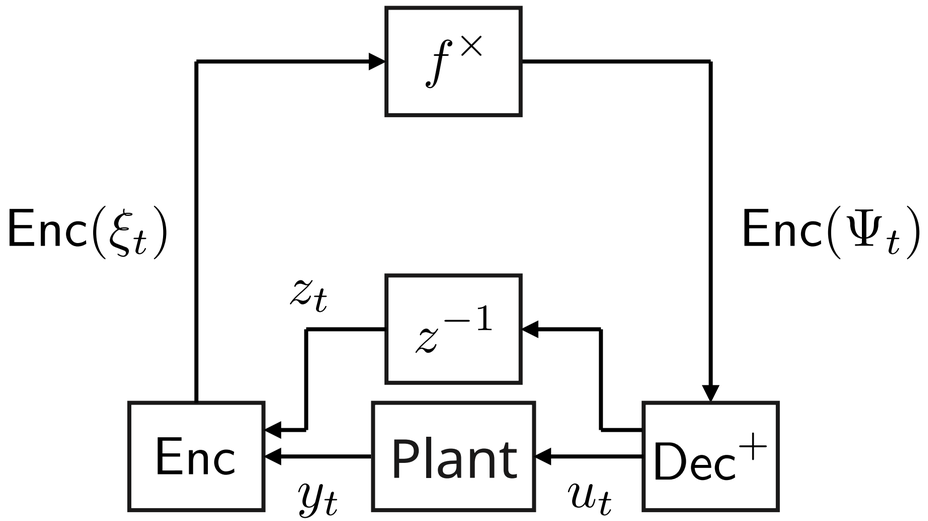
$\text{Dec}^{+} := f^{+} \circ \text{Dec}$

Example (1/2)

Consider the following dynamic controller.

$$z_{t+1} = \begin{bmatrix} 1 & 3 \\ 4 & 5 \end{bmatrix} z_t + \begin{bmatrix} 7 \\ 9 \end{bmatrix} y_t$$

$$u_t = \begin{bmatrix} 1 & 1 \end{bmatrix} z_t$$



$\mathsf{Dec}^+ := f^+ \circ \mathsf{Dec}$

Let $z_t = \begin{bmatrix} 1 & 3 \end{bmatrix}^\top$ and $y_t = 4$.

$$\Phi = \left[\begin{array}{cc|c} 1 & 3 & 7 \\ 4 & 5 & 9 \\ \hline 1 & 1 & 0 \end{array}\right], \; \xi_t = \left[\begin{array}{c} 1 \\ 3 \\ \hline 4 \end{array}\right]$$

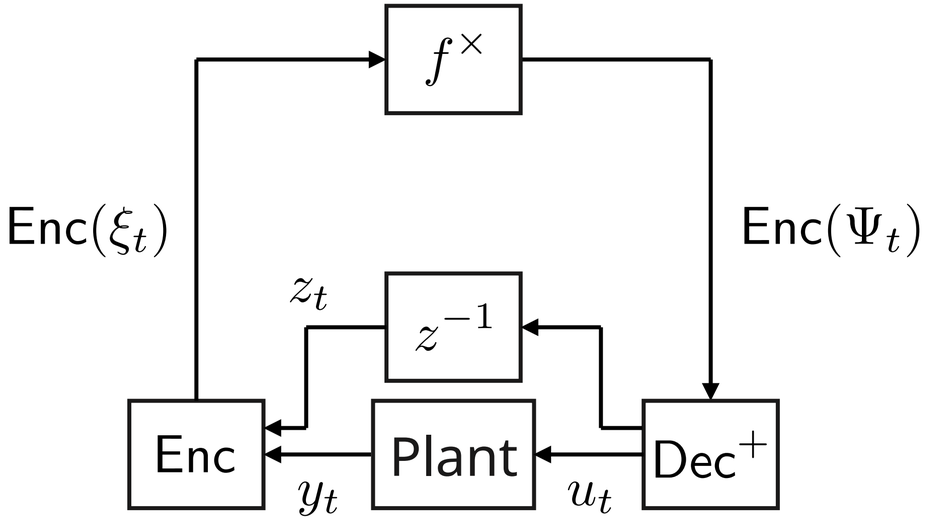
$$f^\times(\Phi, \xi_t) = \Psi_t = \begin{bmatrix} 1 \cdot 1 & 3 \cdot 3 & 7 \cdot 4 \\ 4 \cdot 1 & 5 \cdot 3 & 9 \cdot 4 \\ 1 \cdot 1 & 1 \cdot 3 & 0 \cdot 4 \end{bmatrix} = \begin{bmatrix} 1 & 9 & 28 \\ 4 & 15 & 36 \\ 1 & 3 & 0 \end{bmatrix}$$

$$f^+(\Psi_t) = \psi_t = \begin{bmatrix} 1 + 9 + 28 \\ 4 + 15 + 36 \\ 1 + 3 + 0 \end{bmatrix} = \begin{bmatrix} 38 \\ 55 \\ 4 \end{bmatrix}$$

Example (2/2)

$$f^{\times}(\Phi, \xi_t) = \Psi_t = \begin{bmatrix} 1 \cdot 1 & 3 \cdot 3 & 7 \cdot 4 \\ 4 \cdot 1 & 5 \cdot 3 & 9 \cdot 4 \\ 1 \cdot 1 & 1 \cdot 3 & 0 \cdot 4 \end{bmatrix} = \begin{bmatrix} 1 & 9 & 28 \\ 4 & 15 & 36 \\ 1 & 3 & 0 \end{bmatrix}$$

$$f^{+}(\Psi_t) = \psi_t = \begin{bmatrix} 1+9+28 \\ 4+15+36 \\ 1+3+0 \end{bmatrix} = \begin{bmatrix} 38 \\ 55 \\ 4 \end{bmatrix}$$



$$\mathsf{Dec}^{+} := f^{+} \circ \mathsf{Dec}$$

$$\mathsf{Enc}(\Phi) = \begin{bmatrix} (7,53) & (26,46) & (49,16) \\ (57,1) & (57,16) & (17,28) \\ (26,22) & (17,49) & (0,0) \end{bmatrix}, \ \mathsf{Enc}(\xi_t) = \begin{bmatrix} (4,48) \\ (22,15) \\ (49,26) \end{bmatrix}$$

$$f^{\times}(\mathsf{Enc}(\Phi), \mathsf{Enc}(\xi_t)) = \mathsf{Enc}(\Psi_t) = \begin{bmatrix} (28,7) & (41,41) & (41,3) \\ (51,48) & (15,4) & (7,20) \\ (45,53) & (20,27) & (0,0) \end{bmatrix} \xrightarrow{\mathsf{Dec}} \Psi_t = \begin{bmatrix} 1 & 9 & 28 \\ 4 & 15 & 36 \\ 1 & 3 & 0 \end{bmatrix}$$

$$f^{+}(\Psi_t) = \psi_t = \begin{bmatrix} 1+9+28 \\ 4+15+36 \\ 1+3+0 \end{bmatrix} = \begin{bmatrix} 38 \\ 55 \\ 4 \end{bmatrix}$$

Encoder and Decoder (1/4)

Encryption algorithm cannot encrypt real numbers directly.

$$\mathsf{Enc} : \mathcal{M} \to \mathcal{C}, \quad \mathcal{M} \neq \mathbb{R}$$

Controller parameters and signals are encoded to plaintexts before encryption.

$$\psi_{i,t} = \sum_{j=1}^{n_c+\ell} \mathsf{Dec}(\mathsf{Enc}(\Phi_{ij}) \otimes \mathsf{Enc}(\xi_{j,t}))$$

$\downarrow$ Encoder/Decoder

$$\psi_{i,t} = \sum_{j=1}^{n_c+\ell} \mathsf{Dcd}_\Delta(\mathsf{Dec}(\mathsf{Enc}(\mathsf{Ecd}_\Delta(\Phi_{ij})) \otimes \mathsf{Enc}(\mathsf{Ecd}_\Delta(\xi_{j,t}))))$$

Encoder: $\mathsf{Ecd}_\Delta : \mathbb{R} \to \mathcal{M}$

Decoder: $\mathsf{Dcd}_\Delta : \mathcal{M} \to \mathbb{R}$

Sensitivity: $\Delta > 0$

Encoder and Decoder (2/4)

A plaintext space does not contain negative numbers, and it is an intermittent set.

We cannot round a real number to the nearest integer for encryption.

Example: $g = 3$, $q = 5$, $p = 11$

$$\mathcal{M} = \{1, 3, 4, 5, 9\}$$

Let $x \in \mathbb{R}$, and $\Delta > 0$. Assume that $-\Delta q \leq x \leq \Delta q$.

$$x/\Delta \mapsto z = \begin{cases} x/\Delta, & x \geq 0 \\ x/\Delta + p, & x < 0 \end{cases} \quad \Longrightarrow \quad 1 \leq z \leq p \quad (\because p = 2q + 1)$$

Encode z to the nearest element in $\mathcal{M}$.

$$\check{x} = \min \left\{ \arg\min_{m \in \mathcal{M}} |z - m| \right\}$$

Encoder and Decoder (3/4)

Recover negative numbers.

$$\check{x} \mapsto \check{z} = \begin{cases} \check{x}, & \check{x} \leq q \\ \check{x} - p, & \check{x} > q \end{cases}$$

Remove the scaling factor of $\check{z}$.

$$\bar{x} = \Delta \check{z}$$

Consequently, we obtain

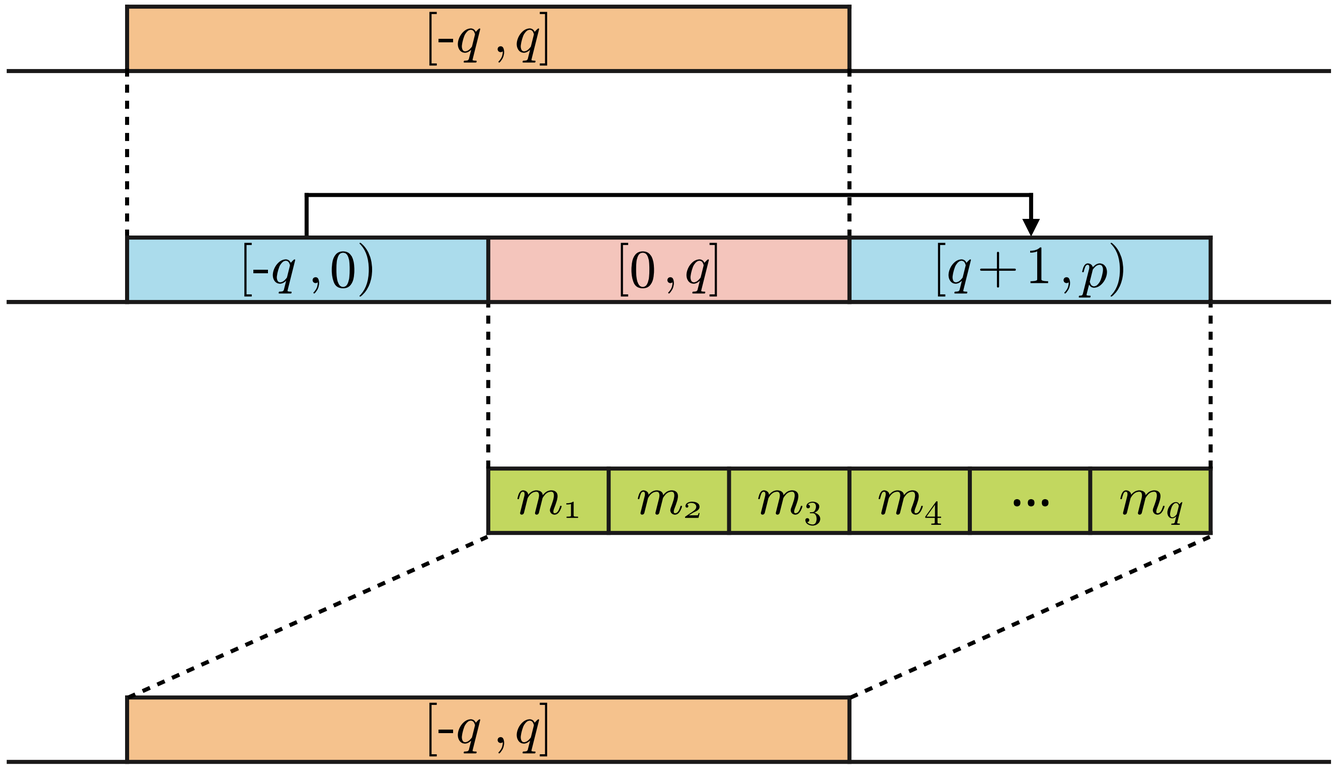
$$\mathsf{Ecd}_\Delta : \mathbb{R} \to \mathcal{M} : x \mapsto \check{x} = \min \left\{ \arg\min_{m \in \mathcal{M}} |x/\Delta + \alpha(x) - m| \right\}, \quad \alpha(x) = \begin{cases} 0, & x \geq 0 \\ p, & x < 0 \end{cases}$$

$$\mathsf{Dcd}_\Delta : \mathcal{M} \to \mathbb{R} : \check{x} \mapsto \bar{x} = \Delta(\check{x} - \beta(\check{x})), \quad \beta(\check{x}) = \begin{cases} 0, & \check{x} \leq q \\ p, & \check{x} > q \end{cases}$$

Encoder and Decoder (4/4)

$$\mathsf{Ecd}_\Delta : \mathbb{R} \to \mathcal{M} : x \mapsto \check{x} = \min\left\{\arg\min_{m\in\mathcal{M}} |x/\Delta + \alpha(x) - m|\right\}, \quad \alpha(x) = \begin{cases} 0, & x \geq 0 \\ p, & x < 0 \end{cases}$$

$$\mathsf{Dcd}_\Delta : \mathcal{M} \to \mathbb{R} : \check{x} \mapsto \bar{x} = \Delta(\check{x} - \beta(\check{x})), \quad \beta(\check{x}) = \begin{cases} 0, & \check{x} \leq q \\ p, & \check{x} > q \end{cases}$$



$\mathbb{R}$ $\quad x/\Delta, \quad \Delta > 0$

$\mathbb{R}$ $\quad z = x/\Delta + \alpha(x)$

$\mathcal{M}$ $\quad \check{x} = \min\left\{\arg\min_{m\in\mathcal{M}} |z - m|\right\}$

$\mathbb{R}$ $\quad \bar{x} = \Delta(\check{x} - \beta(\check{x}))$

$\mathsf{Ecd}_\Delta(x)$

$\mathsf{Dcd}_\Delta(\check{x})$

Example (1/2)

Let $\lambda = 3$. Then, $q = 5$, $p = 2q + 1 = 11$, and $g = 3$ are valid parameters.

A plaintext space is $\mathcal{M} = \mathbb{G} = \{g^0, g^1, g^2, g^3, g^4\} = \{1, 3, 4, 5, 9\}$.

Let $\Delta = 0.1$, then $-0.5 \leq x \leq 0.5$.

$$
\begin{aligned}
\mathsf{Ecd}_\Delta(0.2) &= \min\left\{\arg\min_{m\in\mathcal{M}} |0.2/0.1 + \alpha(0.2) - m|\right\} \\
&= \min\left\{\arg\min_{m\in\mathcal{M}} |2 - m|\right\} \\
&= \min\{1, 3\} = 1 \\
\mathsf{Ecd}_\Delta(-0.3) &= \min\left\{\arg\min_{m\in\mathcal{M}} |-0.3/0.1 + \alpha(-0.3) - m|\right\} \\
&= \min\left\{\arg\min_{m\in\mathcal{M}} |-3 + 11 - m|\right\} \\
&= 9
\end{aligned}
$$

Example (2/2)

$$\begin{aligned}\mathsf{Dcd}_\Delta(1) &= \Delta(1-\beta(1)) \\ &= 0.1 \cdot 1 = 0.1 \\ \mathsf{Dcd}_\Delta(9) &= \Delta(9-\beta(9)) \\ &= 0.1 \cdot (9-11) = -0.2\end{aligned}$$

$$\begin{aligned}0.2 - \mathsf{Dcd}_\Delta(\mathsf{Ecd}_\Delta(0.2)) &= 0.2 - 0.1 = 0.1 \neq 0 \\ -0.3 - \mathsf{Dcd}_\Delta(\mathsf{Ecd}_\Delta(-0.3)) &= -0.3 + 0.2 = -0.1 \neq 0\end{aligned}$$

Encoding and decoding cause a quantization error.

Quantization Error (1/2)

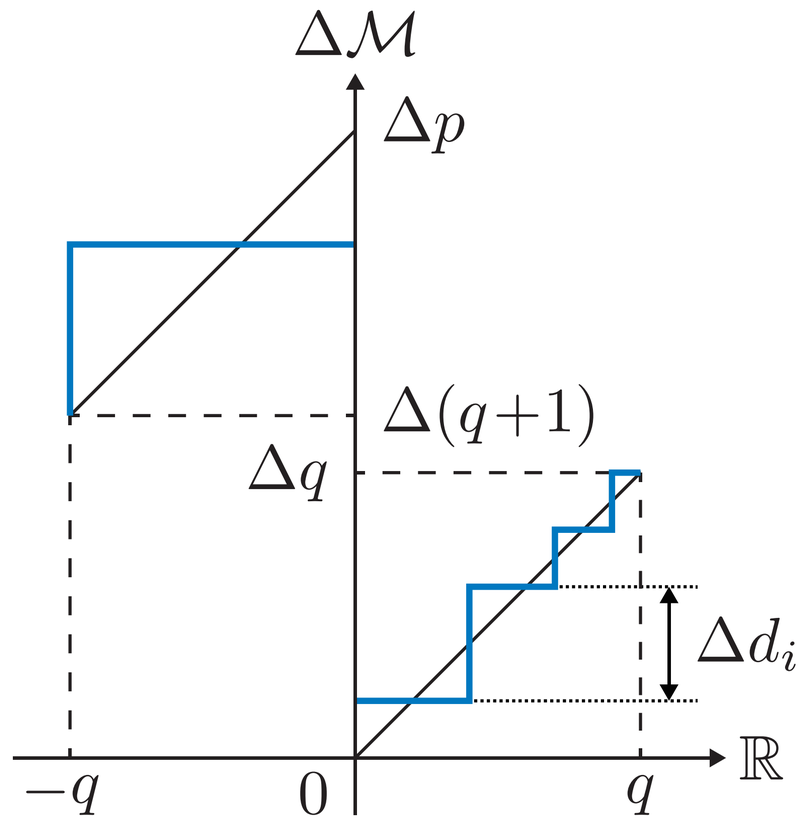
Difference between two consecutive elements

$$d_i := m_{i+1} - m_i$$

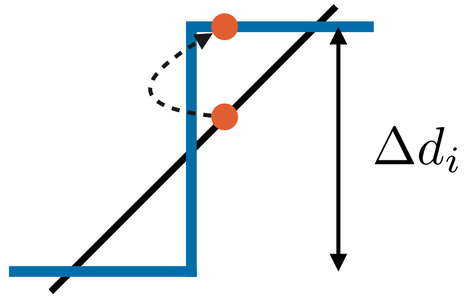
$$m_i, m_{i+1} \in \mathcal{M} = \{m_1, \ldots, m_q\},\ m_i < m_{i+1},\ i = 1, \ldots, q-1$$

Example: $\Delta = 0.1,\ g = 3,\ q = 5,\ p = 11,\ \mathcal{M} = \{1, 3, 4, 5, 9\}$

$$\Delta d_1 = 0.3 - 0.1 = 0.2$$
$$\Delta d_2 = 0.4 - 0.3 = 0.1$$
$$\Delta d_3 = 0.5 - 0.4 = 0.1$$
$$\Delta d_4 = 0.9 - 0.5 = 0.4$$



A quantization error is given as the distance between blue and black lines.



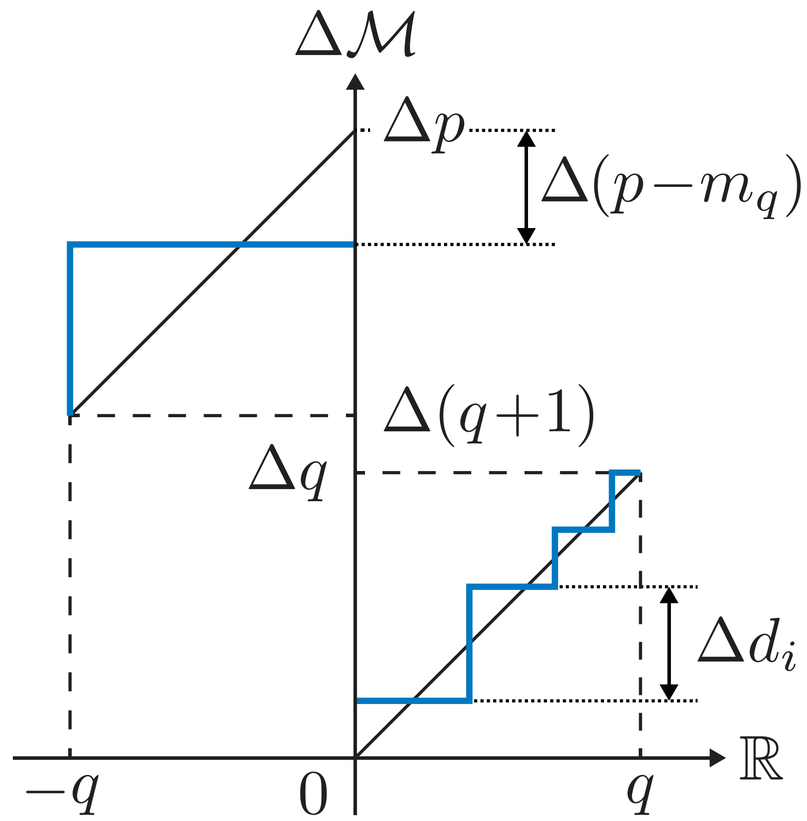
Quantization Error (2/2)

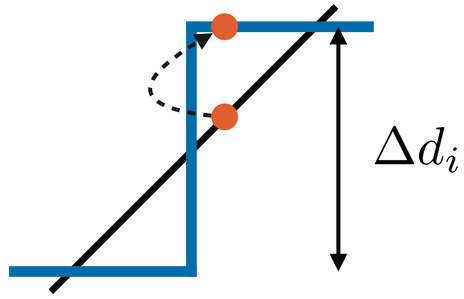
Define $d_{\max} := \max_{i=1,\ldots,q-1} \{d_i, 2(p - m_q)\}$.

Upper bound of quantization error $\tilde{x} := \mathsf{Dcd}_\Delta(\mathsf{Ecd}_\Delta((x)) - x$:

- Scalar $x \in \mathbb{R}$ $|\tilde{x}| \leq \Delta \dfrac{d_{\max}}{2}$
- Vector $v \in \mathbb{R}^n$ $\|\tilde{v}\| \leq \sqrt{n}\Delta \dfrac{d_{\max}}{2}$
- Matrix $M \in \mathbb{R}^{m \times n}$ $\|\tilde{M}\| \leq \sqrt{mn}\Delta \dfrac{d_{\max}}{2}$

A quantization error can be reduced as sensitivity Δ decreases.





Encrypted Sate-feedback Control (1/4)

State-feedback control system ($T_s = 0.01$ s)

$$x_{t+1} = \begin{bmatrix} 1.01 & -0.01 \\ 0 & 1.02 \end{bmatrix} x_t + \begin{bmatrix} 0 \\ 0.01 \end{bmatrix} u_t$$

$$u_t = \begin{bmatrix} 6.57 & -6.20 \end{bmatrix} x_t$$

ElGamal encryption

$\lambda = 256$

$q = 101869766012948509637006021075372738505236457002001536414249638898569555040363$

$p = 203739532025897019274012042150745477010472914004003072828499277797139110080727$

$g = 2$

$h = 139445883211634212476843803746321888504742645278487051155865798075341129592373$

$s = 211580294371564868356184174581642569849762480988918017341873634650074067695 23$

Encrypted Sate-feedback Control (2/4)

Feedback gain: $F = \begin{bmatrix} 6.57 & -6.20 \end{bmatrix}$

Sensitivity: $\Delta = 0.3$

Encoded gain:

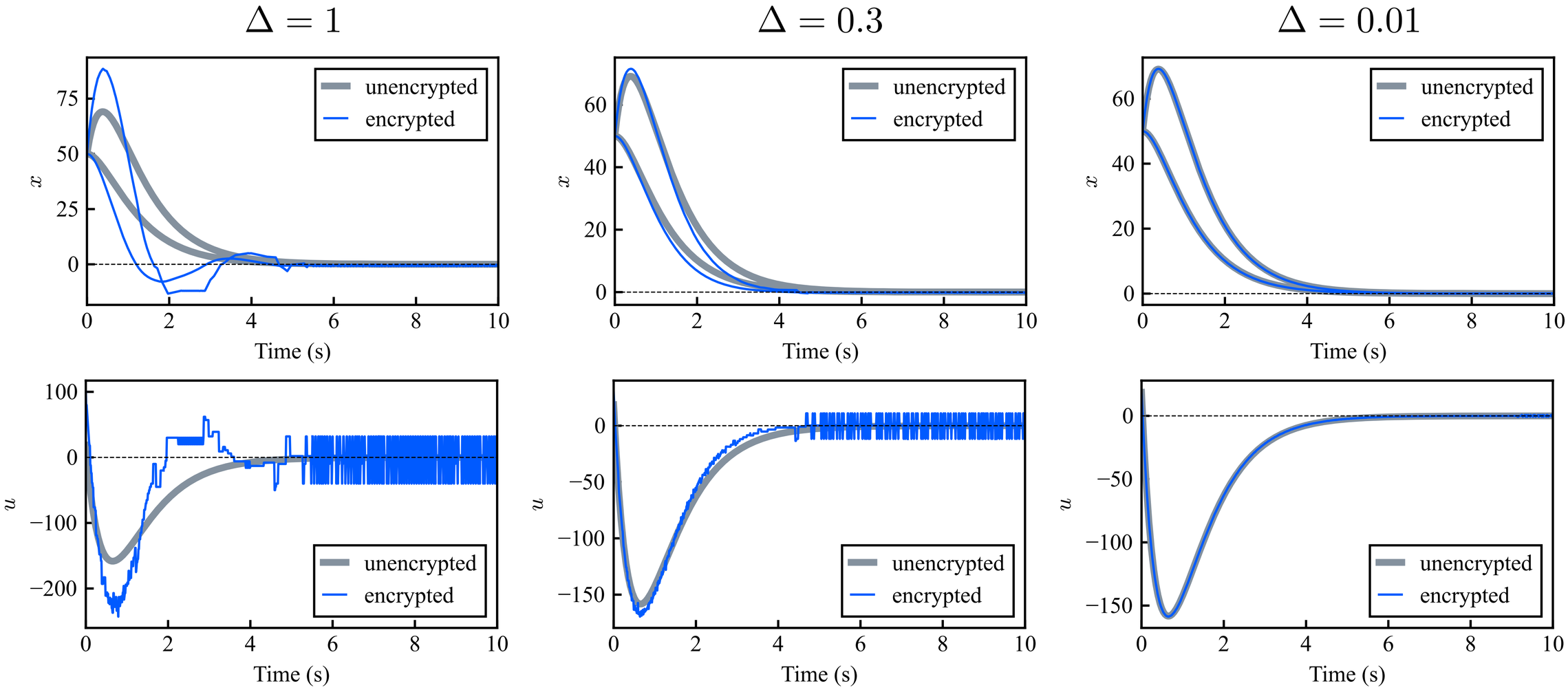
$$\mathsf{Ecd}_\Delta(F) = \begin{bmatrix} 22 & 203739532025897019274012042150745477010472914004003072828499277797139110080707 \end{bmatrix}$$

Encrypted gain:

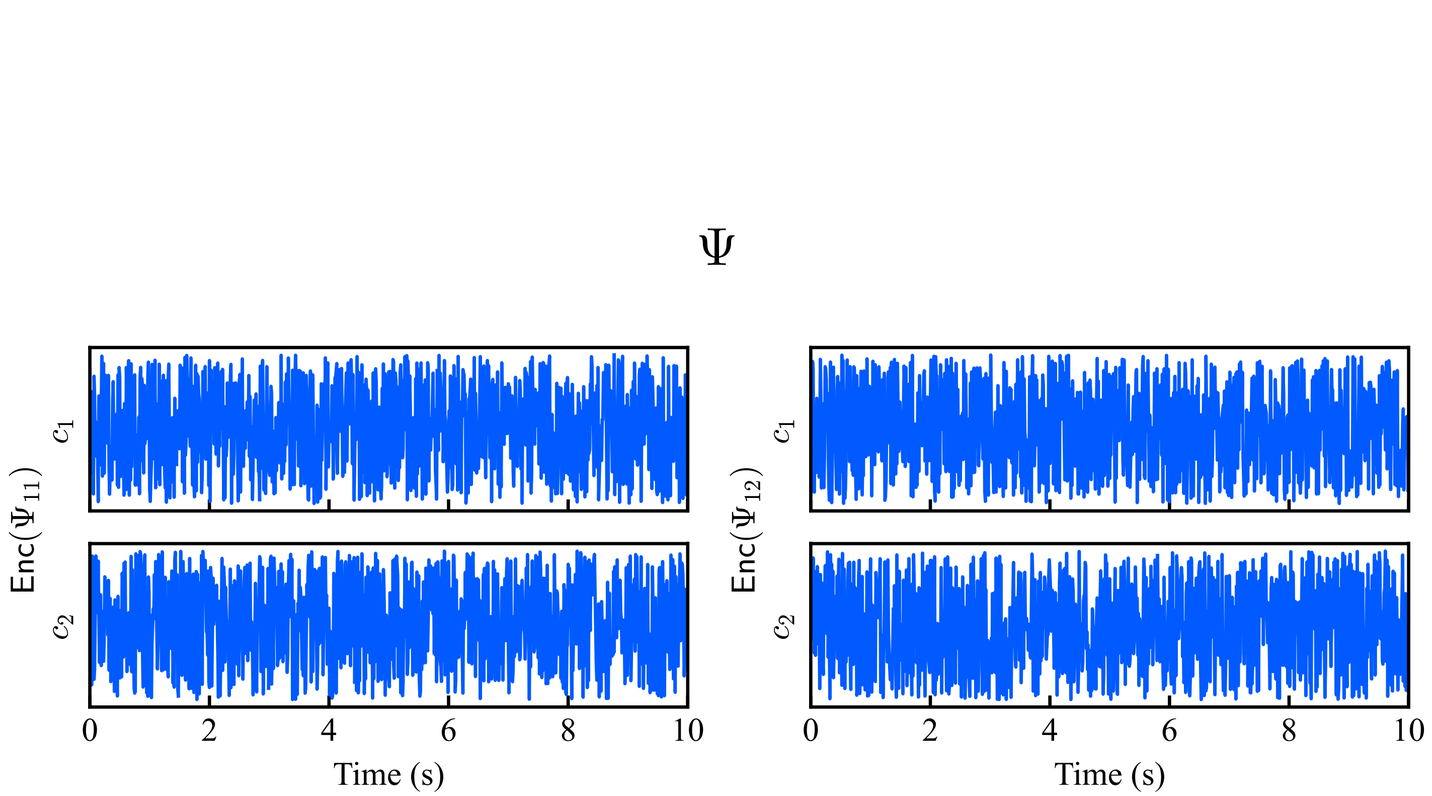
$$\mathsf{Enc}_\Delta(\mathsf{Ecd}_\Delta(F)) = \begin{bmatrix} (1.2597589288846022 \times 10^{77}, 1.758311094590806 \times 10^{77}) \\ (1.467038332740248 \times 10^{77}, 5.614086575524795 \times 10^{76}) \end{bmatrix}^\top$$

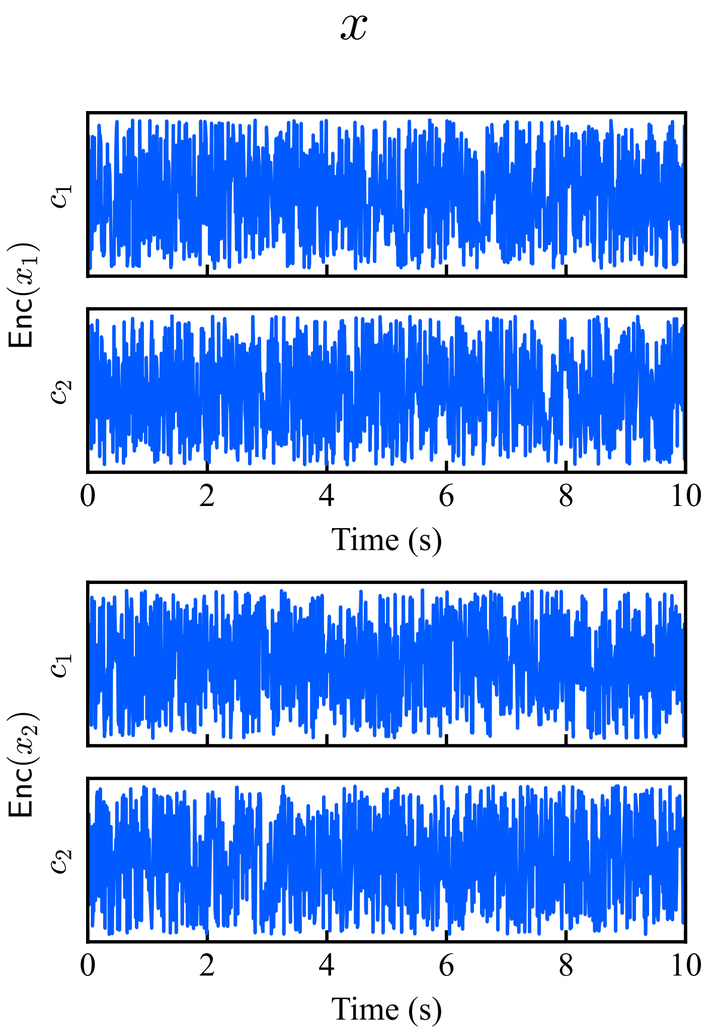
Encrypted Sate-feedback Control (3/4)

Initial value: $x_0 = \begin{bmatrix} 50 & 50 \end{bmatrix}^\top$



Encrypted Sate-feedback Control (4/4)





Encrypted PI Control (1/3)

Plant ($T_s = 0.1$ s)

$$x_{t+1} = \begin{bmatrix} 0.35 & -0.16 \\ 0.13 & 0.98 \end{bmatrix} x_t + \begin{bmatrix} 0.031 \\ 0.004 \end{bmatrix} u_t$$

$$y_t = \begin{bmatrix} 0 & 1 \end{bmatrix} x_t$$

PI controller ($K_p = 15.34$, $K_i = 15.62$)

$$w_{t+1} = w_t + \begin{bmatrix} T_s & -T_s \end{bmatrix} \begin{bmatrix} r_t \\ y_t \end{bmatrix}$$

$$u_t = K_i w_t + \begin{bmatrix} K_p & -K_p \end{bmatrix} \begin{bmatrix} r_t \\ y_t \end{bmatrix}$$

$$\iff \quad \begin{bmatrix} w_{t+1} \\ u_t \end{bmatrix} = \begin{bmatrix} 1 & T_s & -T_s \\ K_i & K_p & -K_p \end{bmatrix} \begin{bmatrix} w_t \\ r_t \\ y_t \end{bmatrix}$$

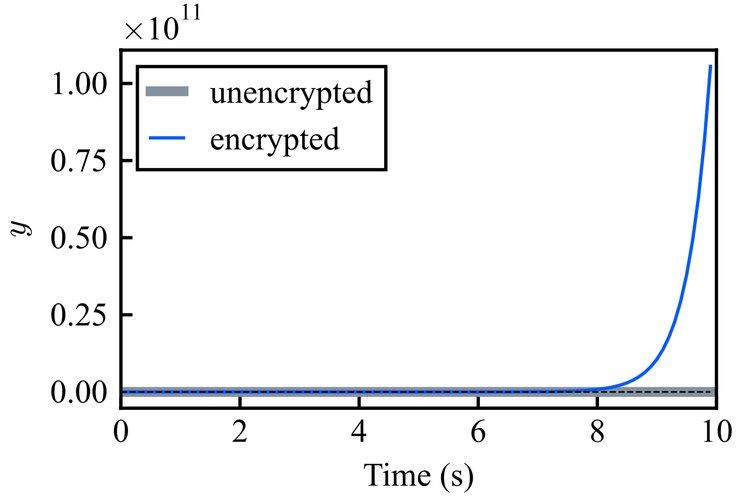
$$\psi_t = \begin{bmatrix} w_{t+1} \\ u_t \end{bmatrix}, \ \Phi = \begin{bmatrix} 1 & T_s & -T_s \\ K_i & K_p & -K_p \end{bmatrix} = \begin{bmatrix} 1 & 0.1 & -0.1 \\ 15.62 & 15.34 & -15.34 \end{bmatrix}, \ \xi_t = \begin{bmatrix} w_t \\ r_t \\ y_t \end{bmatrix}$$

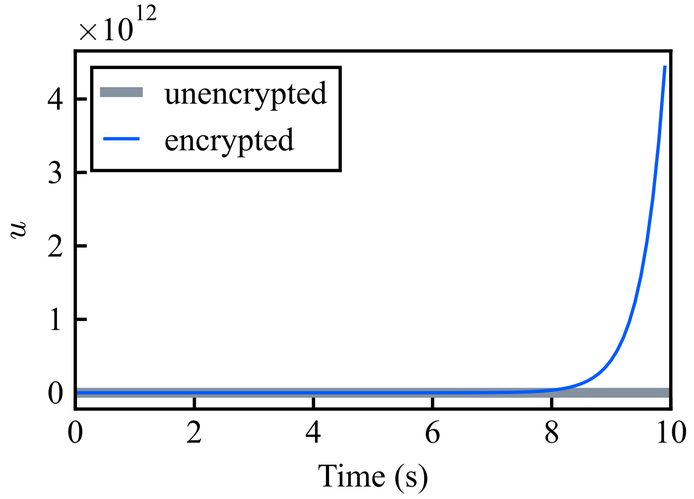
r: Reference

Encrypted PI Control (2/3)

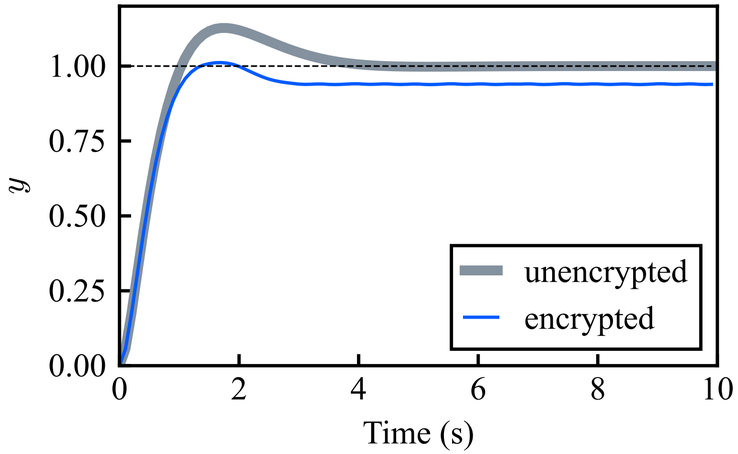
$\lambda = 256,\ r_t = 1$

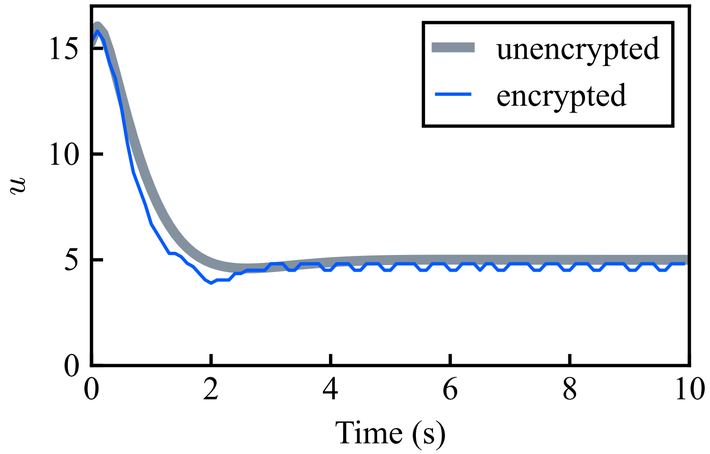
$\Delta = 1$



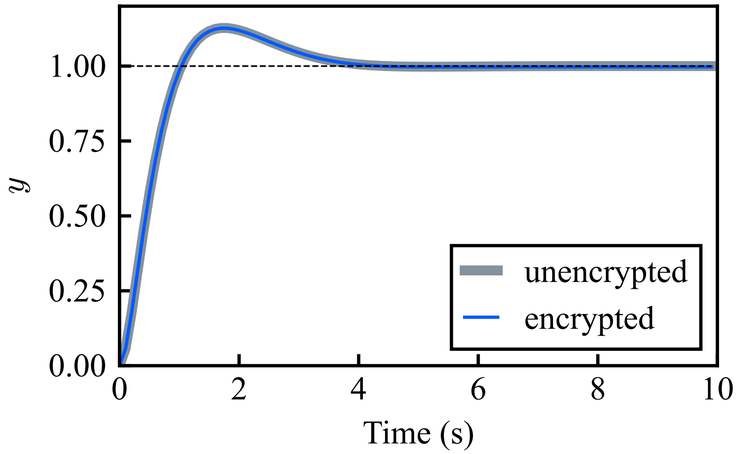


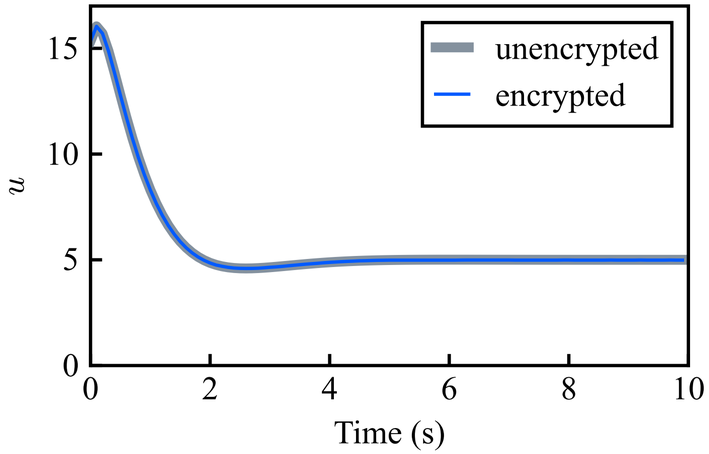
$\Delta = 0.01$



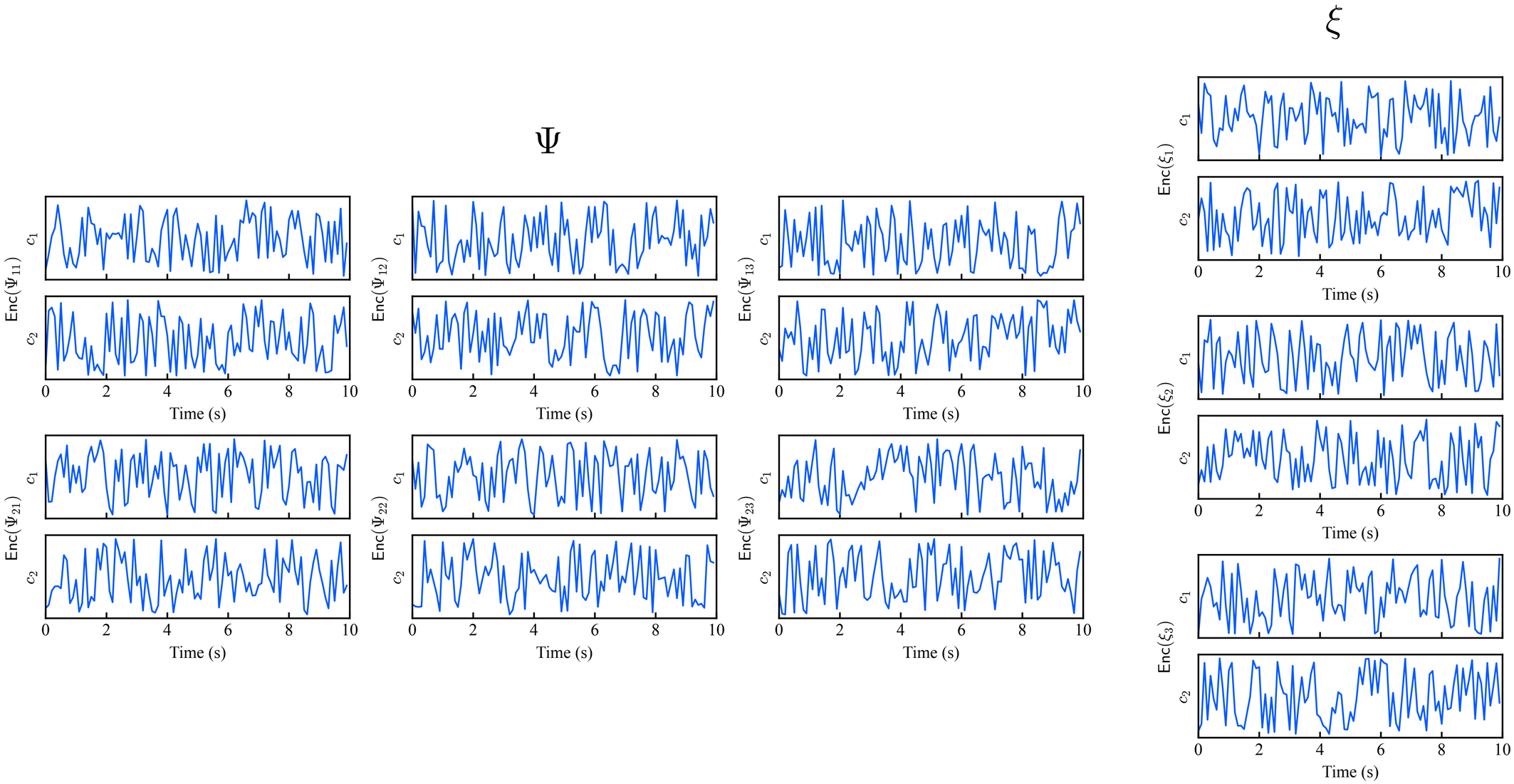


$\Delta = 0.0001$





Encrypted PI Control (3/3)



Conclusion

- Encrypted control with multiplicative homomorphic encryption is realized by controller reconstruction.
- Controller parameters and signals need to be encoded into a plaintext space before encryption.
- Encoding and decoding cause quantization errors.
- Quantization errors can be reduced by decreasing a scaling parameter.