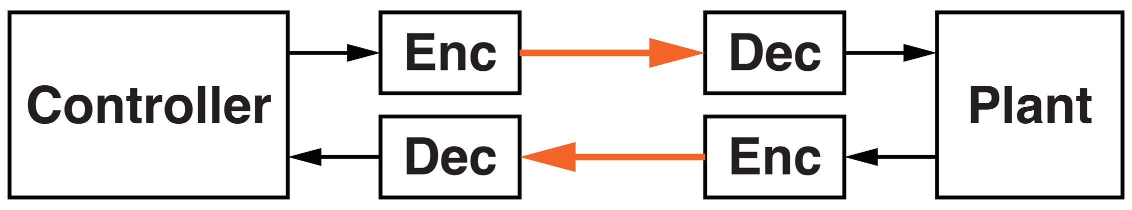
8th IFAC Workshop on Distributed Estimation and Control in Networked Systems, September 17, 2019, Chicago, IL, USA.

# Control-theoretic Approach to Malleability Cancellation by Attacked Signal Normalization

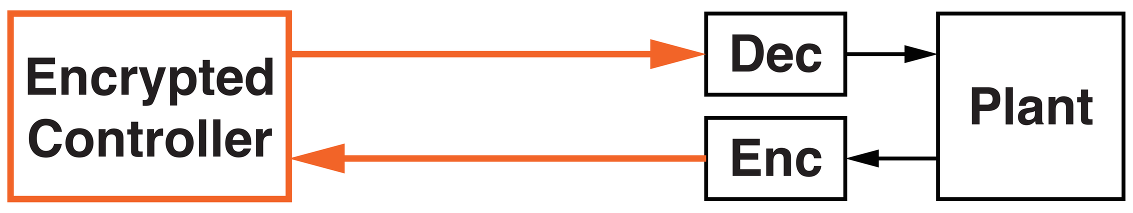
Kaoru Teranishi and Kiminao Kogiso, The University of Electro-Communications

## Encrypted Control System

**Conventional control system**




**Encrypted control system [1, 2]**




Encrypted control is a cryptographic approach to security enhancement for networked control systems. In this method, controller parameters and signals over network links are encrypted.

**Homomorphic encryption** $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

Key generation $\mathsf{Gen} : \mathcal{S} \to \mathcal{K}$

Encryption $\mathsf{Enc} : \mathcal{M} \to \mathcal{C}$

Decryption $\mathsf{Dec} : \mathcal{C} \to \mathcal{M}$

$$\begin{array}{ccc} m, m' & \longrightarrow & m \circ m' \\ \Big\downarrow \mathsf{Enc} & & \Big\uparrow \mathsf{Dec} \\ \mathsf{Enc}(m), \mathsf{Enc}(m') & \longrightarrow & \mathsf{Enc}(m) \bullet \mathsf{Enc}(m') \end{array}$$

Homomorphism $\mathsf{Dec}(\mathsf{Enc}(m) \bullet \mathsf{Enc}(m')) = m \circ m'$

$\mathcal{S}$: Security Parameters, $\mathcal{K}$: Key Pairs, $\mathcal{M}$: Plaintext sp., $\mathcal{C}$: Ciphertext sp.

**ElGamal encryption (Multiplicatively homomorphic encryption)**

$\mathsf{Dec}(\mathsf{Enc}(m) * \mathsf{Enc}(m')) = mm'$ $\quad *$: Hadamard product

**Paillier encryption (Additively homomorphic encryption)**

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

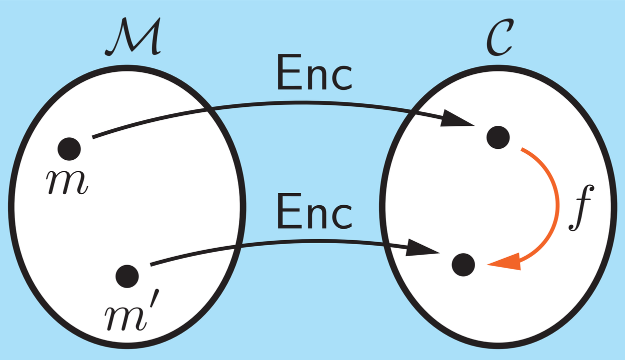
## Malleability

***Definition***

$\mathcal{E}$ is malleable.

$\iff \exists m, m' \in \mathcal{M},\ \exists f : \mathcal{C} \to \mathcal{C}$

s.t. $f(\mathsf{Enc}(m)) = \mathsf{Enc}(m')$




**ElGamal encryption (Multiplicatively homomorphic encryption)**

$f : (c_1, c_2) \mapsto (c_1, kc_2), \quad (c_1, c_2) = \mathsf{Enc}(m), \quad \mathsf{Dec}(f(c_1, c_2)) = km$

**Paillier encryption (Additively homomorphic encryption)**

$f : c \mapsto c^k, \quad c = \mathsf{Enc}(m), \quad \mathsf{Dec}(f(c)) = km$

Malleability is a property of cryptosystems that a ciphertext can be generated from another ciphertext without decryption. The objective of this study is to propose a novel attack using malleability for encrypted control systems and control-theoretic cancellation method of the attack.

## Pole-Assignment Attack

***Definition***

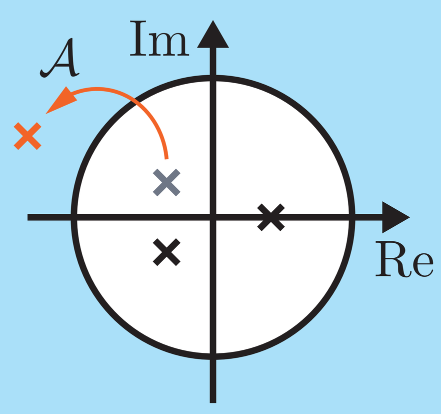
We call

$$\mathcal{A} : \Lambda \to \tilde{\Lambda},$$

a pole-assignment attack if

$$|\Lambda| = |\tilde{\Lambda}|, \quad \Lambda \neq \tilde{\Lambda},$$

where $\Lambda$ is a set of poles of an original control system, and $\tilde{\Lambda}$ is a set of poles of an attacked control system.

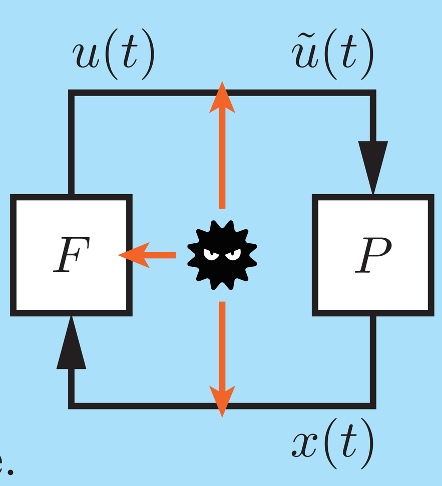



***Theorem***

Given a state-feedback gain $F$ such that $A + BF$ is Schur. If $F$, $x(t)$, or $u(t)$ is falsified into $\tilde{u}(t) = ku(t) = kFx(t)$ with

$$k > \frac{n + |\mathrm{tr}(A)|}{|\mathrm{tr}(BF)|},$$

then the closed-loop system becomes unstable.




By using malleability, adversaries can conduct pole-assignment attacks even if control systems are encrypted. This type of attacks is called ***malleability-based pole-assignment attacks***.

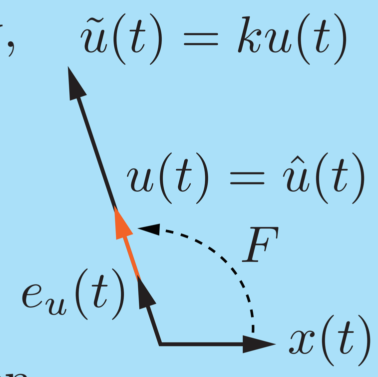
## Cancellation Method

***Theorem***

Suppose that $F$, $x(t)$, or $u(t)$ is falsified. Now, we design a new input with normalization

$$\hat{u}(t) = \|F_R x(t)\| e_u(t), \quad e_u(t) = \frac{\tilde{u}(t)}{\|\tilde{u}(t)\|},$$

where $F_R$ is a right triangle matrix, which is given by the QR decomposition of $F$, such as $F = F_Q F_R$, and $F_Q$ is an orthogonal matrix. Then, the closed-loop system achieves asymptotic stability.




***Corollary***

We can modify the new input as follows:

$$\hat{u}(t) = \left\| F_{R^{2s+1}} \left( \prod_{j=1}^{s} F_{R^{2j-1}Q} \right)^{\top} x(t) \right\| \frac{\tilde{u}(t)}{\|\tilde{u}(t)\|},$$

where $F_{R^{2s+1}}$ is a right triangle matrix given by $2s+1$ times of QR decomposition, and $F_{R^{2j-1}Q}$ is a corresponding orthogonal matrix for $F_{R^{2j}}$.

The proposed method cancels malleability-based pole-assignment attacks without controller information. Even if adversaries eavesdrop obfuscated feedback gain, they cannot obtain the controller information.

## Numerical Example

**Plant**

$$A = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ -1 & -2 & -1 \end{bmatrix}, \ B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

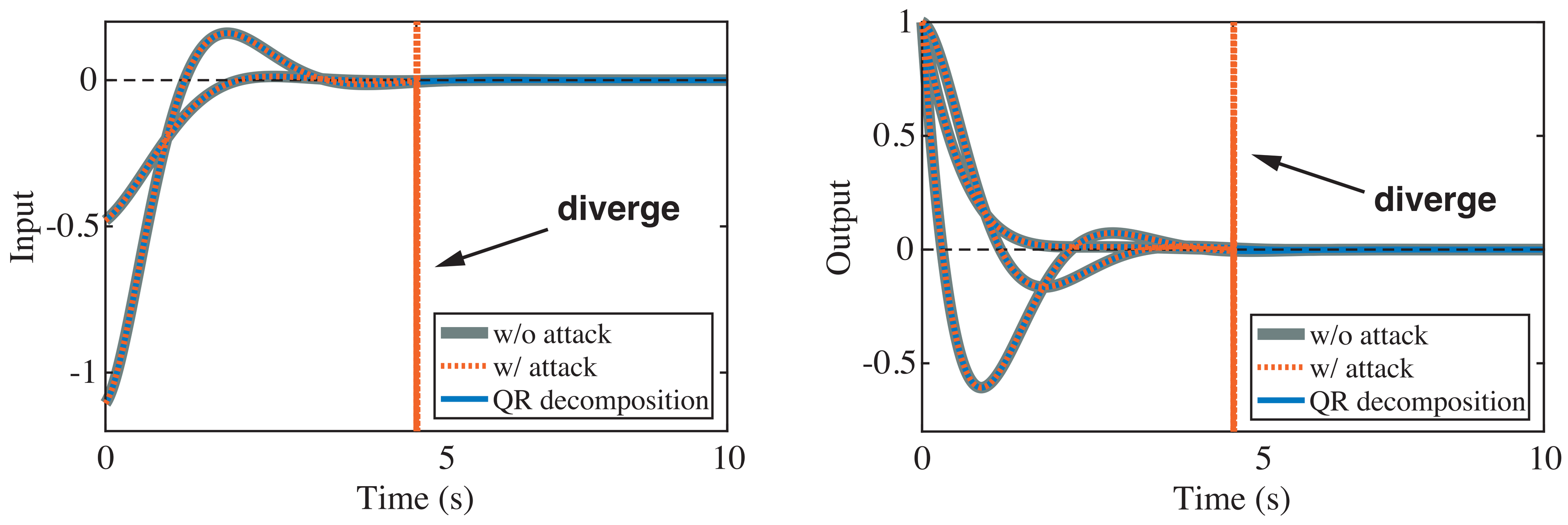
This plant is discretized with a sampling time of 10 ms.

**State-feedback gain**

$$F = \begin{bmatrix} -0.51 & -0.12 & 0.15 \\ -0.12 & -0.98 & -0.01 \end{bmatrix}, \ F_{R^3} F_{RQ}^{\top} = \begin{bmatrix} -0.42 & -0.83 & 0.09 \\ 0.31 & -0.54 & -0.12 \end{bmatrix}$$

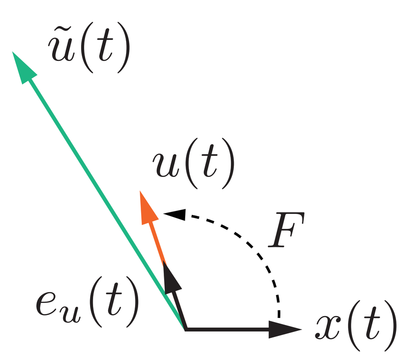
**Malleability-based pole-assignment attack**

$$k = 4019 > \frac{3 + |2.9980|}{|-0.0015|} \simeq 4018$$




## Future Work

**Partial falsification**




The proposed method cannot be capable for ***partial falsification attacks*** because the attacks change the length of an input vector and rotate it. The authors will extend the proposed method so that it cancels scalar multiplication and rotation.

**Detection method**

Although the proposed method does not need a detection process, it is also crucial to detect malleability-based pole-assignment attacks.

**Computational complexity**

The proposed method may maintain the real-time property. The authors will investigate the computational complexity of the proposed method.

[1] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," *IEEE Conference on Decision and Control*, 2015, pp. 6836-6843.
[2] F. Farokhi, I. Shames and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Engineering Practice*, vol. 67, pp. 13-20, 2017.