UCLA | Samueli School of Engineering

NSF #1740047

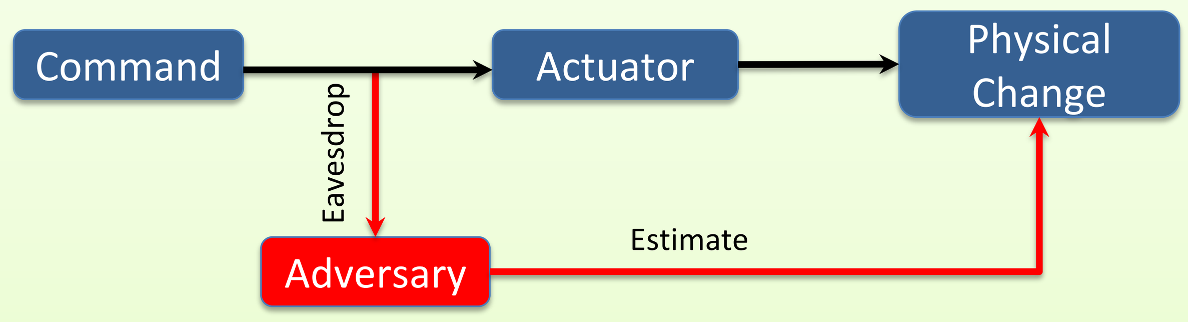
Distorting an Adversary's View in Cyber-Physical Systems

Christina Fragouli, Suhas Diggavi, Paulo Tabuada

University of California, Los Angeles

Labs: Algorithmic Research in Networked Information Flow (ARNI), Laboratory of Information Theory and Communication Systems (LICOS), The Cyber-Physical Systems Laboratory (CyPhyLab)

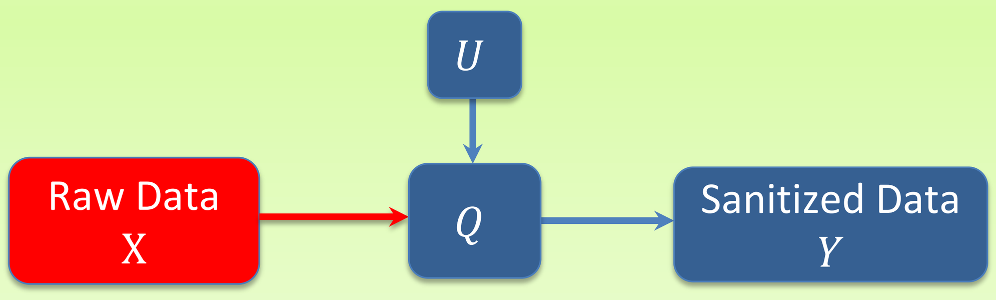
Wireless Networked Cyber Physical Systems and Security



Information Security

- Asymmetric cryptography: large overhead
- Maximizes entropy of the message given eavesdropper information
- Perfect secrecy: Unbreakable, Large keys
- Partial secrecy: Smaller keys, targeted

Randomness in Local Differential Privacy Mechanisms



$(\epsilon, R) - LDP$ Mechanism

- Raw data $X \in \{1, \cdots, k\}$
- Q is $(\epsilon, R) - LDP$ if for every $X, \acute{X} \in \{1, \cdots, k\}$, we have

$$sup \frac{Q(Y = y|X)}{Q(Y = y|\acute{X})} \leq e^{\epsilon}$$
$$H(U) \leq R$$

- For small privacy level ϵ, observing Y does not reveal whether the raw data was X or $\acute{X}$

Secure Time-Series Communication [1]

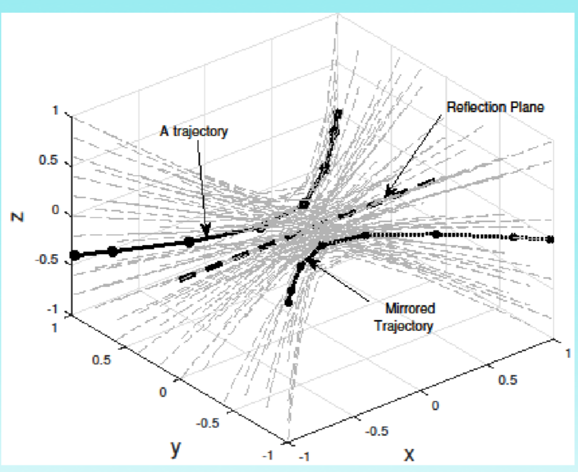
Dynamical Control System

$$X_{t+1} = A\, X_t + B\, U_t + w_t$$
$$Y_t = C\, X_t + v_t$$

- We define two distortion measures for sequential data i.e., state transitions of a control system:
  - Expected Distortion: $D_E = \frac{1}{T} \sum_t (X_t - \hat{X}_t)^2$
  - Worst Case Distortion: $D_W = \min_t \min_{\tau_t(X_t, K)} (X_t - \hat{X}_t)^2$

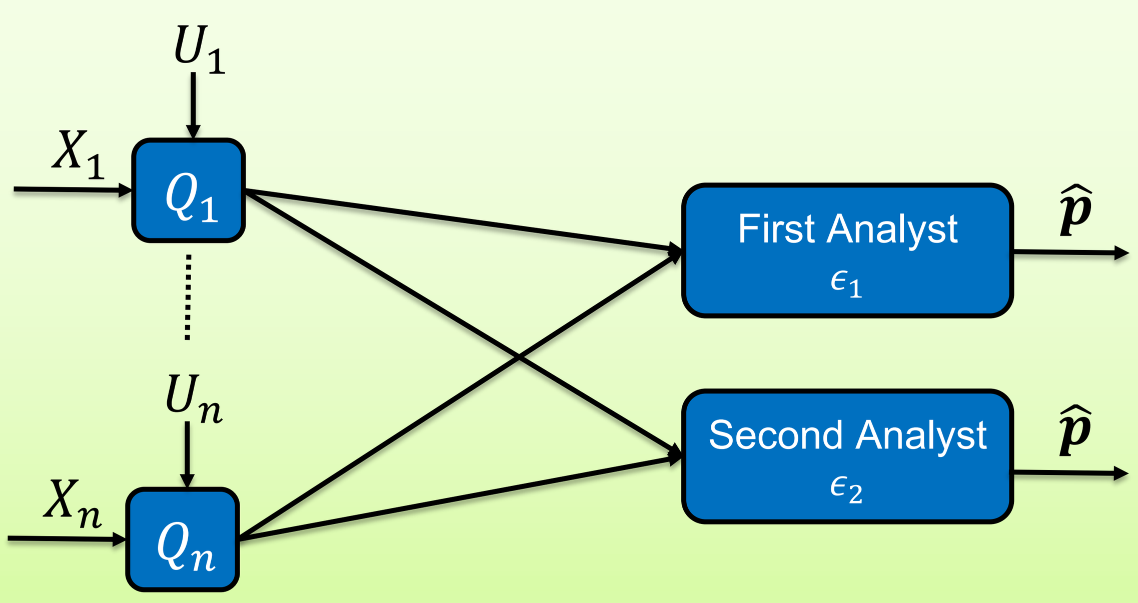
Goal:

- Maximize Distortion by designing encoding functions τ_t



For Average Case:
- Mirror across hyperplanes for certain symmetric distributions
- Hyperplane can be picked with just one bit of key

Multi-Level Privacy [2]



Model:

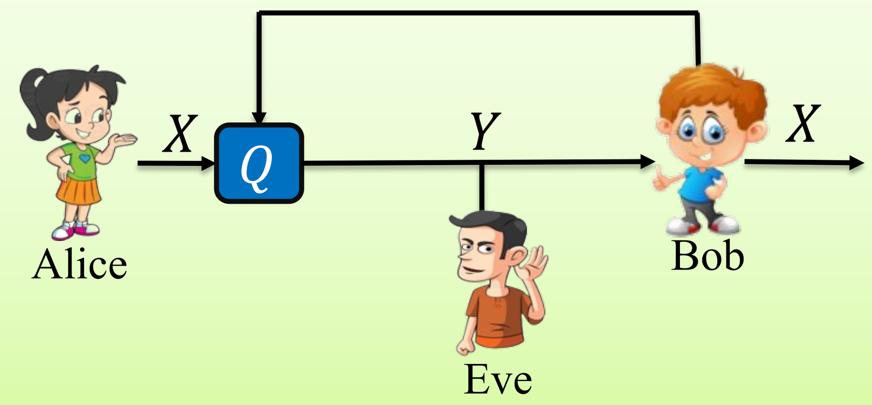
- n users, each has a sample $X_i \sim \boldsymbol{p}$
- d analysts want to estimate $\boldsymbol{p}$
- Each user i has a random key U_i

Goal:

- Design DP-mechanisms $\{Q_i : i \in [n]\}$: $Q_i = f(X_i, U_i)$
- To preserve privacy of each user
- To minimize the risk minimization of each analyst

$$r^{\ell}_{\epsilon,R,n,k} = \inf_{\hat{\boldsymbol{p}}} \inf_{Q_i} \sup_{\boldsymbol{p}} E[\ell(\hat{\boldsymbol{p}}(Y^n), \boldsymbol{p})]$$

Results [2]: Private-Recoverability



Necessary and Sufficient Conditions to Design Q

- The number of keys must be at least the same as the output size that must be at least the same as the input size: $|U| \geq |Y| \geq |X|$
- The entropy of the private key must satisfy: $H(U) \geq H(U^s_{min})$

$$U^s_{min} \sim q^s_{min} = \left[\frac{e^{\epsilon}}{s(e^{\epsilon} - 1) + k}, \cdots, \frac{1}{s(e^{\epsilon} - 1) + k}\right]$$

- The entropy of this key is less than what is required for one-time pad

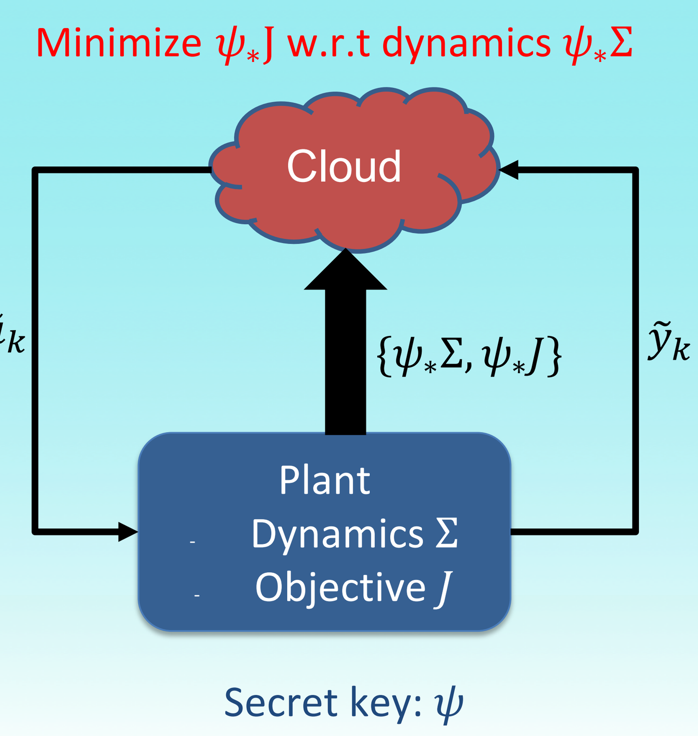
Privacy in Control over the Cloud [3]

Motivation

- Control input can be calculated by minimizing an objective function (e.g., model predictive control)
- Control over the cloud requires communication of *private data* - vulnerable to *eavesdropping* attacks

Results

- Created a lightweight encoding scheme using isomorphisms of control systems
- Cloud is unable to learn the state, the dynamics, or the objective
- Proposed a measure of privacy (in terms of the dimension of uncertainty set)
- Quantified privacy loss with side knowledge



Algorithm

1) **Handshaking**: Plant encodes Σ and J with ψ, and sends them to the cloud
2) **Plant operation:**
   - **Encoding:** Measure y_k and send encoded $\tilde{y}_k = \psi_* y_k$ to the cloud
   - **Optimization:** Cloud uses $\tilde{y}_k$ to find input $\tilde{u}_k$ minimizing $\psi_* \Sigma$ w.r.t dynamics $\psi_* J$, send $\tilde{u}_k$
   - **Decoding:** Decode $u_k = \psi_*^{-1} \tilde{u}_k$ and apply it to the actuators

References

[1] G. Agarwal, M. Karmoose, S. Diggavi, C. Fragouli, P. Tabuada. "Distorting an adversary's view in cyber-physical systems", CDC 2018, arXiv 2019

[2] A.M. Girgis, D. Data, K. Chaudhuri, C. Fragouli, S. Diggavi. "Privacy-Utility-Randomness Trade-offs in Local Differential Privacy", arXiv 2019

[3] A. Sultangazin, P. Tabuada. "Symmetries and Privacy in Control Over the Cloud: Uncertainty Sets and Side Knowledge", CDC 2019

Project Directions

- Distorting security for passive attacks in CPS dynamical systems
- Secure state estimation with actuator and sensor attacks
- Privacy with input-distortion metrics
- Privacy in control over the cloud
- Privacy of networked control over the cloud
- Privacy with coded wireless broadcasting
- Secure lightweight entity authentication
- **Publication output:** The work during the reporting period resulted in 12 publications and 3 in submission.
- **REU achievement:** We supported two students for REU during June-August 2019 including a female student with whom two papers are in submission. The students worked on implementing drone localization through beaconing, which we will use for privacy.