A Theory of Privacy for Cyber-Physical Systems with Applications in Energy Systems

Shuo Han

Postdoctoral Researcher
Electrical and Systems Engineering
University of Pennsylvania

Joint work with: Ufuk Topcu, George J. Pappas
Future: A Sensor-Rich World

- 5 billion people to be connected by 2015
- 7 trillion wireless devices serving 7 billion people in 2017
  - 1000 wireless devices per person (!)
Privacy Concerns

Report by:
Sen. Deb Fischer (Nebraska)
Sen. Cory Booker (New Jersey)
Sen. Kelly Ayotte (New Hampshire)
Sen. Brian Schatz (Hawaii)
Privacy Concerns in Cyber-Physical Systems

Intelligent transportation systems

Location-based services

Camera networks

Building automation
Privacy Concerns in the Smart Grid

The time you jump into the shower in the morning, the time you finally lurch off that TV at night—even the time you set your home security alarm. Ontario’s privacy czar wants the province’s emerging smart grid electricity system to be protected like Fort Knox.

"This thing has to be protected like Fort Knox," says Ontario’s information and privacy commissioner Ann Cavoukian.

The Smart Grid and Privacy
Concerning Privacy and Smart Grid Technology

- California Protects the Privacy of Smart Meter Data: The California Public Utility Commission has established new rules to protect information about consumer use of “smart meter” electrical services. The California decision, the first in the country, establishes fair information practice requirements, including a consumer right of access and control, data minimization obligations, use and disclosure limitations, and data quality and integrity requirements. Electric utilities and their contractors, as well as third party who receive electricity usage data from utilities are subject to the new rules. EPIC submitted extensive comments to the Public Utility Commission regarding privacy safeguards for consumer energy usage data. For more, see EPIC Smart Grid Privacy. (Aug. 6, 2011)
- Consumer Groups Recommend Privacy Safeguards on “Smart Meter” Services: The Trans-Atlantic Consumer Dialogue (TACD), a coalition of consumer groups in Europe and North America, adopted a report on privacy and electrical services at the 12th Annual TACD meeting held recently in Brussels. The Smart Meter

Utilities work to prevent privacy backlash over smart grid

SHAWN MCCARTHY - GLOBAL ENERGY REPORTER,
OTTAWA — The Globe and Mail
Published Wednesday
Last updated Wednesday

Can Smart Grid know too much?
Hydro meter info a boon for thieves, marketers, and must be protected, privacy czar says

Toronto Star, May 12, 2010
Tanya Talaga

Tanya Talaga

Tanya Talaga

Tanya Talaga

As the grid collects information on power usage and smart meters are installed in Ontario homes to track consumption data, that personal information could represent a treasure trove for hackers, thieves or
How Should We Think About Privacy?

Users

Administrator (Google, Facebook, ...)

The Public

Adversary

Private values

Public information

Side information
The Danger of *ad hoc* Privacy Solutions

**NETFLIX**
- Dataset published for an open competition (Netflix challenge)
- Contains user ratings on movies
- Privacy solution: Anonymization

**IMDb**
- Many reviews under real names
- Strong correlation with the Netflix dataset

De-anonymization
[Narayanan and Shmatikov, 2008]

- Certain users were identified with high confidence
- Movie ratings contain sensitive information
  - Political preference
  - Religious view
Various Approaches to Privacy

- Database: [Dwork, 2006]
- Information Theory: [Sankar, Rajagopalan, Poor, 2010]
- Game Theory: [Acemoglu et al., 2015]
- Secure Multi-Party Computation: [Lindell and Pinkas, 2009]
- Control Theory: [Wu and Lafortune, 2012]
A Unified View of Privacy

- Adversary wants to infer the private value(s) by building an estimator

  \[\text{estimated}_\text{private}_\text{value}(\text{public information, side information})\]

- Privacy guarantee:

  \[\mathbb{P}(\text{estimated}_\text{private}_\text{value} \neq \text{private value})\]

  Probability of Preserving Privacy
Privacy Research for Cyber-Physical Systems

Networks

Streaming Data

Physical Constraints
• Private Distributed Charging of Electric Vehicles
  - Framework: Differential privacy

• Private Smart Metering Using Internal Energy Storage
  - Framework: Information-theoretic privacy
Electric Vehicle (EV) Charging

- User specifications may reveal private information of the users.
- **Example 1**: “Unable to charge my car between 8-10pm”
  → This user may not be at home from 8-10pm.
- **Example 2**: “Need to charge my car by a large amount at night”
  → This user may have used the car heavily during the day.
EV charging: Mathematical formulation

- Electrical vehicle (EV) charging problem [Ma, Callaway, Hiskens, 2010]
  - $T$ time steps, $n$ vehicles (i.e., $n$ users)
  - $r_i \in \mathbb{R}^T$: Charging rates (over time) of vehicle $i$
  - $U$: Assumed convex (e.g., minimal variance, minimal peak load, ...)

$$
\begin{align*}
\min \quad & U \left( \sum_{i=1}^{n} r_i \right) \\
\text{s.t.} \quad & 0 \leq r_i \leq \bar{r}_i, \quad 1^T r_i = E_i, \quad i = 1, 2, \ldots, n.
\end{align*}
$$

- Both $\bar{r}_i$ and $E_i$ can reveal private information
Differential Privacy: Setup

- With side information, an adversary may learn about user information from the output of $q$

- The goal of differential privacy: Design a mechanism that
  - preserves user privacy regardless of side information
  - approximates the query $q$ well
The mechanism $M$ is **differentially private** if

$$\mathbb{P}(M(D) \in \mathcal{R}) \leq e^\epsilon \mathbb{P}(M(D') \in \mathcal{R})$$

- For all $\mathcal{R} \subseteq \text{range}(M)$
- For all adjacent $D$ and $D'$

Cannot distinguish between $D$ and $D'$ from the output of $M$
Probability of Preserving Privacy

• Suppose an adversary wishes to know whether user $i$ is $d_i$

• In detection theory
  - Null hypothesis: “The database is $D$, with user $i$ being $d_i$.”
  - Alternative hypothesis: “The database is $D'$, with user $i$ being $d_i'$.”
  - Adversary’s rule: choose $\mathcal{R}^*$ such that
    $$M(D) \in \mathcal{R}^* \implies \text{report “user } i \text{ is } d_i”$$

• Probabilities of error
  - Type I error: $p_1 = \mathbb{P}(M(D) \notin \mathcal{R}^*)$
  - Type II error: $p_2 = \mathbb{P}(M(D') \in \mathcal{R}^*)$
If $M$ is differentially private, then:

\[
p_1 + e^\varepsilon p_2 \geq 1 \\
 e^\varepsilon p_1 + p_2 \geq 1.
\]

A lower bound on the probability of preserving privacy

\[
\min(p_1 + p_2) = \frac{2}{1 + e^\varepsilon}
\]

[Geng, 2013]
Example: Obtaining the average

- **Not** private under the differential privacy framework!
- An adversary can know any $d_i$ if he collaborates with the rest (even if user $i$ is not willing to collaborate)

**Diagram:**

- User 1: $d_1$
- User 2: $d_2$
- ...$
- User n: $d_n$

Query (computes the average)

$$q(D) = \frac{1}{n} \sum_{i=1}^{n} d_i$$

Each $d_i \in [0, 1]$

$D = \{d_i\}_{i=1}^{n}$
Solution from differential privacy

- Differentially private mechanism: Add Laplace noise to the average

\[
M(D) = \frac{1}{n} \sum_{i=1}^{n} d_i + \text{Lap}(\lambda)
\]

\[
D_1 \quad d_1 \\
\downarrow \\
\text{User 1} \\
D_2 \quad d_2 \\
\downarrow \\
\text{User 2} \\
\vdots \\
D_n \quad d_n \\
\downarrow \\
\text{User n}
\]

Mechanism (approximates the average)

- Differentially private mechanism: Add Laplace noise to the average
How large is the noise?

- Laplace distribution: \( X \sim \text{Lap}(\lambda) \iff p_X(x) \propto \exp(-|x|/\lambda) \)

- In the Laplace mechanism, \( \lambda \) depends on two quantities:

\[
\lambda = \Delta / \epsilon
\]

- **Level of privacy** \( \epsilon \) (smaller means more private)

\[
P(M(D) \in \mathcal{R}) \leq e^\epsilon P(M(D') \in \mathcal{R})
\]

- **Sensitivity** of the query \( q \)

\[
\Delta = \max_{D,D'} |q(D) - q(D')|
\]

  - For all adjacent \( D \) and \( D' \)
  - For computing the average: \( \Delta = 1/n \)

Can be difficult to compute for a given problem!
Distributed EV charging

\[
\begin{align*}
\min_{\{r_i\}_{i=1}^{n}} & \quad U \left( \sum_{i=1}^{n} r_i \right) \\
\text{s.t.} & \quad r_i \in C_i, \quad i = 1, 2, \ldots, n.
\end{align*}
\]

- Distributed projected gradient descent [Gan et al., 2013]

\[
p^{(k)} := \nabla U \left( \sum_{i=1}^{n} r_i^{(k)} \right) \quad r_i^{(k+1)} := \Pi_{C_i} \left( r_i^{(k)} - \alpha_k p^{(k)} \right)
\]

- Gradient \( p^{(k)} = \nabla U \left( \sum_{i=1}^{n} r_i^{(k)} \right) \) is broadcast to all users
  - May lead to privacy issues: projection operation depends on \( C_i \)

**Database:** \( D = \{C_i\}_{i=1}^{n} \)

**Query:** \( q = (p^{(1)}, p^{(2)}, \ldots, p^{(K)}) \)
Differentially Private Projected Gradient Descent

Initialize \( \{ r_i^{(1)} \}_{i=1}^n \) arbitrarily

For \( k = 1, 2, \ldots, K \), repeat:

1. If \( k = 1 \), then choose \( w_k = 0 \);
2. Else draw \( w_k \in \mathbb{R}^T \) from the distribution \( \exp \left( -\frac{2\epsilon\|w_k\|}{K(K-1)L\Delta} \right) \)
3. Compute
\[
\hat{p}^{(k)} := \nabla U \left( \sum_{i=1}^n r_i^{(k)} \right) + w_k
\]

4. For \( i = 1, 2, \ldots, n \), compute:
\[
r_i^{(k+1)} := \Pi_{C_i} (r_i^{(k)} - \alpha_k \hat{p}^{(k)})
\]

Output: \( \{ r_i^{(K+1)} \}_{i=1}^n \)

\( w_k \): Noise ("vector Laplace")
\( \Delta \): Sensitivity of projection
Sensitivity of Projection

Definition:

\[ \Delta := \max_{i \in [n]} \max \left\{ \| \Pi_{C_i}(r) - \Pi_{C'_i}(r) \| : r \in \mathbb{R}^T, C_i \text{ and } C'_i \text{ are adjacent} \right\}. \]

- In general, difficult to compute
- But can be computed for some cases
Computing the Sensitivity

- For EV charging, the set $C_i$ is given by
  \[ \{ r_i : 0 \leq r_i \leq \bar{r}_i, \quad 1^T r_i = E_i \} \]
- Adjacency relation: $C_i$ and $C'_i$ are adjacent if
  \[ \| \bar{r}_i - \bar{r}'_i \|_1 \leq \delta r, \quad |E_i - E'_i| \leq \delta E \]

(\( \delta r \) and \( \delta E \) are design choices that encode the private events)

**Theorem:** The sensitivity for the EV charging problem is given by
\[
\Delta = 2\delta r + \delta E
\]

Proof based on the optimality condition.
Solution Sensitivity of Optimization Problems

- Projection $\Pi_{C_i}$: Constrained least-squares problem

$$\begin{align*}
\min_{x} & \quad \|x - x_0\|^2 \\
\text{s.t.} & \quad 0 \leq x \leq a, \quad 1^T x = b.
\end{align*}$$

- Local solution sensitivity analysis

[Fiacco et al., 1976]

$$\begin{align*}
\nabla^2 L \cdot \dot{x} + \sum_{i=1}^{p} \nabla g_i \cdot \dot{\lambda}_i + \sum_{i=1}^{q} \nabla h_i \cdot \dot{\nu}_i + \frac{\partial}{\partial \theta} (\nabla L) &= 0 \\
\lambda_i^* \nabla g_i \cdot \dot{x} + g_i \dot{\lambda}_i + \lambda_i^* \frac{\partial g_i}{\partial \theta} &= 0, \\
\nabla h_i \cdot \dot{x} + \frac{\partial h_i}{\partial \theta} &= 0.
\end{align*}$$

Local sensitivity of primal & dual variables

- For EV charging, we need:

$$\begin{align*}
\frac{\partial x^*}{\partial a} \quad \text{and} \quad \frac{\partial x^*}{\partial b}
\end{align*}$$

integration

Global sensitivity

$$\|x^*(a, b) - x^*(a', b')\|$$
Simulation results

- $n = 100,000, \ T = 52$
- Choose $\epsilon = 0.1$ (common choice in diff. privacy)
- Objective: Minimal load variance

Optimal solution: “Valley filling”

Fluctuation in diff. private solution due to Laplace noise
Suboptimality Analysis

• How does noise affect the optimality?
• Observation: Gradient descent becomes stochastic gradient descent

Theorem: The (expected) suboptimality of the differentially private distributed algorithm is given by

$$\mathbb{E} \left[ U \left( \sum_{i=1}^{n} \hat{r}_i^{(K+1)} \right) - U^* \right] \leq O \left( T^{1/4} \left( \Delta / n\epsilon \right)^{1/4} \right)$$

• Note:
  - Under optimal choice of the number of iterations
  - Same suboptimality: larger $n \rightarrow$ smaller $\epsilon$ (more privacy)
• Private Distributed Charging of Electric Vehicles
  - Framework: Differential privacy

• Private Smart Metering Using Internal Energy Storage
  - Framework: Information-theoretic privacy
Advanced Metering Infrastructure (Smart Meters)

Difference from conventional meters:
Very high time resolution!
Privacy Concerns in Smart Meters

Non-Intrusive Load Monitoring

- Other names: Energy/load disaggregation
- Based on the “signatures” of different appliances
- The types of appliances are related to life patterns

[Kolter and Johnson, 2011]
**Smart Meter with Internal Energy Storage**

![Diagram of user and smart meter with power consumption flow]

**Goal:**
Use internal energy storage to hide patterns in power consumption

[McDaniel and McLaughlin, 2009]
Model Description

Energy usage
\[ X_t \in \{0, 1, \ldots, n\} \]
(random process)

Battery control policy
\[ \Delta B_t = B_t - B_{t-1} \]

Reported energy usage
\[ Y_t \]

Output equation:
\[ Y_t = X_t + B_t - B_{t-1} \]

Battery control policy:
\[ B_t = B_t(X_{1:t}, Y_{0:t-1}, B_{0:t-1}) \]
Why Not Differential Privacy?

- Physical constraints
  - Battery has maximum capacity
  - Noise perturbation required by DP may not be feasible
  - Privacy guarantee is lost in the presence of constraints: [Backes and Meiser, 2014]

- Information-theoretic privacy
  - Algorithm first, then privacy analysis
  - Allows a wider class of private algorithms
Probability of Preserving Privacy

- Mutual information as a metric of privacy: \( I(X; Y) \)

**Fano’s inequality:** For any random variables \( X \) and \( Y \), suppose one would like to estimate \( X \) from \( Y \) by constructing an estimator \( \hat{X}(Y) \). Then we have:

\[
\mathbb{P}(\hat{X}(Y) \neq X) \geq \frac{H(X) - I(X; Y) - 1}{\log_2 |\mathcal{X}|}
\]

- Probability of the attacker making an error
- \( \mathcal{X} \): alphabet of \( X \)

“Less mutual information => higher probability of preserving privacy”
Information-Theoretic Metric of Privacy

\[ \bar{I}(X; Y) \triangleq \sup_t I(X_t; Y) \]

\[ = \sup_t \lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T) , \]

Mutual information between:
\( X_t \) and “observations up to \( T \)

For any given time slot

All possible observations

“Energy consumption within any single time slot”
Comparison with Previous Work

- Previous work on information-theoretic privacy:
  - [Kalogridis et al., 2010]
  - [Varodayan and Khisti, 2011]
  - [Tan et al., 2013]
  - [Yao and Venkitasubramaniam, 2014]

\[
I(X; Y) \triangleq \lim_{t \to \infty} \frac{1}{t} I(X_1, X_2, \ldots, X_t; Y_1, Y_2, \ldots, Y_t)
\]

(mutual information rate)

“Probability of error for estimating the entire input sequence”

- Our information-theoretic metric of privacy

\[
\bar{I}(X; Y) = \sup_t \lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T),
\]

“Probability of error for estimating any single entry in the sequence” (stronger)
Evaluation of Information-Theoretic Privacy

- This talk: Focus on the evaluation problem
  - For a given control policy, evaluate its level of privacy
  - The problem of designing the optimal control policy is more difficult!

- The policy under consideration: [McDaniel and McLaughlin, 2009]

Best-effort policy: \( B_t = [Y_{t-1} - X_t + B_{t-1}]_0^m \)

Truncation operation: \([x]_0^m = \begin{cases} x, & 0 \leq x \leq m, \\ 0, & x < 0, \\ m, & x > m. \end{cases}\)

What the policy does: Try to make \( Y_t = Y_{t-1} \).
Illustration of the Best-Effort Policy

True energy consumption

Smart meter output
Is the New Privacy Metric Well-Defined?

\[ \bar{I}(X; Y) = \sup_t \lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T), \]

**Proposition (Monotonicity):** For any \( t \) and \( T_1 < T_2 \), we have

\[ I(X_t; Y_1, Y_2, \ldots, Y_{T_1}) \leq I(X_t; Y_1, Y_2, \ldots, Y_{T_2}). \]

**Proposition (Boundedness):** For any \( t \) and \( T \), we have

\[ I(X_t; Y_1, Y_2, \ldots, Y_T) \leq H(X_t) < \infty \]

- Supremum exists: Follows from boundedness
- Limit exists: Follows from the monotone convergence theorem
### Numerical Results

$$I(X_t; Y_1, Y_2, \ldots, Y_T) \text{ grows monotonically with } T \text{ and is upper bounded}$$
Computing the Privacy Metric

- We know $I(X_t; Y_1, Y_2, \ldots, Y_T) \leq H(X_t)$

  \[ \bar{I}(X; Y) = \sup_t \lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T), \]

  equality: trivial privacy guarantee
  (zero probability of error from Fano’s ineq.)

- Need to compute the metric:

- For the smart meter problem, this can be computed when:
  - $X_t$ is an i.i.d. random process $\Rightarrow (B_t, Y_t)$ is a Markov chain
  - The initial state $(B_0, Y_0)$ follows the stationary distribution
Proposition: If the distribution of \((B_0, Y_0)\) is the stationary distribution, then we have

\[
\sup_t I(X_t; Y) = \lim_{t \to \infty} I(X_t; Y)
\]

Hard to compute Can be approximated by making \(t\) large enough

\[
\bar{I}(X; Y) \approx 0.460
\]
**Numerical Results**

- **$I(X_t; Y)$**
- **$\mathbb{P}(\hat{X}_t(Y) \neq X_t)$**

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n$</th>
<th>$I(X_t; Y)$</th>
<th>$\mathbb{P}(\hat{X}_t(Y) \neq X_t)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.460</td>
<td>0.124</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.303</td>
<td>0.188</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0.224</td>
<td>0.229</td>
</tr>
</tbody>
</table>

Probability of error in the best case:

$$\mathbb{P}(\hat{X}_t(Y) \neq X_t) = 0.5$$

- $m = 3$ large or small in practice?
  - Depends on the duration of time slots
  - Microwave: 5 mins
  - Laundry machine: 30 mins

$n$: maximum consumption (within 1 slot)
$m$: battery capacity
Summary

• Unified view of privacy from **probability of preserving privacy**

• Part 1: Differential privacy
  - Privacy: Defined via the adjacency relation $\text{Adj}(\cdot, \cdot)$
  - Conversion to prob. of preserving privacy: Hypothesis testing

• Example application 1: Private distributed EV charging
  - Noise in the gradients
  - Magnitude of noise determined from sensitivity analysis
  - Quantification on the trade-off between privacy and utility

• Part 2: Information-theoretic privacy
  - Privacy: Defined via involved variables (e.g., $X_t$ and $Y_{1:T}$)
  - Conversion to prob. of preserving privacy: Fano’s inequality

• Example application 2: Private smart meters using energy storage
  - Numerical evaluation of the privacy metric
  - Nontrivial privacy guarantees