Information-Theoretic Private Interactive Mechanism

Bahman Moraffah *Lalitha Sankar*

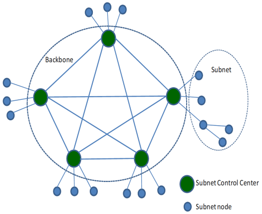
ARIZONA STATE UNIVERSITY
SCHOOL OF **Electrical, Computer, and Energy Engineering**

Allerton Conference on Communication, Control, and Computing
September 10, 2015

Outline

Motivation

- Many distributed systems need to exchange data amongst different agents (e.g., electric power systems).
- Data sharing critical for high fidelity estimation.
- However, sharing often inhibited due to privacy/ trust/ security constraints.
- Competitive Privacy:[1] Can data be shared so as to reveal specific public features of data while keeping the leakage of private features minimal?



- Determine privacy-guaranteed interactive data sharing information-theoretic mechanisms.

[1] L. Sankar, S. Kar, R. Tandon, H.V. Poor, "Competitive privacy in the smart grid", Smart Grid Communications (SmartGridComm), IEEE International Conference on, 2011

Problem Description

- Consider a two agent setup where each agent has public and private data.
- Goal is to minimize the leakage of private data while ensuring the fidelity of public data over multiple rounds.
- Develop leakage-distortion tradeoff for interactive setting for various distributions and distortion measures.

Literature Review: Utility-Privacy Tradeoff

One-shot data publishing setting:

- Sankar *et. al.*[2] introduced an information-theoretic formulation of the utility-privacy tradeoff problem.
- Utility modeled as distortion and privacy captured via a mutual information based leakage.
- Database modeled as an n-length sequence from an i.i.d source.
- Utility-privacy tradeoff captured by the set of achievable distortion-leakage tuples.

Interactive setting:

- Sankar *et. al.*[3] consider a two-agent setup with Gaussian distributed correlated observations at each agent.
- Optimal utility-privacy tradeoff region shown to be achieved by a Gaussian privacy mechanism.
- Focus of this talk is on the interactive setting with general distributions and distortions.

[2] L. Sankar, S. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information theoretic approach" Information forensics and security, IEEE transaction on , vol. 8, no. 6 June 2013

[3] L. Sankar, S. Kar,R. Tandon, H.V. Poor, "Competitive privacy in the smart grid", Smart Grid Communications (SmartGridComm), IEEE International Conference on, 2011

Literature Review: Relationship to Interactive Source Coding:

- Utility-privacy tradeoff problem does not involve encoders and decoders.
- Mutual information used as a measure of information leakage.
  - Thus, leakage-distortion optimizations have a flavor of rate-distortion optimizations.
- Much work on interactive source coding problem by Kaspi[4] and Ma *et. al.*.[5]

[4] A. Kaspi, " Two-way source coding with fidelity criterion" Information theory, IEEE Transaction on, vol 31 no. 6, Nov 1985,

[5] N. Ma, P. Ishwar, P. Gupta, "Interactive source coding for function computation in collocated networks" Information theory, IEEE Transaction on, vol 58, no. 7,2012.

Literature Review: Information Bottleneck

Information Bottleneck

- Goal is to minimize the compression rate of public data subject to constraint on the log-loss distortion of private data.[6]
- In our problem we minimize information leakage of the private feature while lower bounding the (mutual) information of the public feature.

One-way non-interactive setting

- Under log-loss distortion and mutual information leakage Makhdoumi *et. al.*[7] developed tradeoff region.
- Use an algorithm based on the agglomerative information bottleneck algorithm.

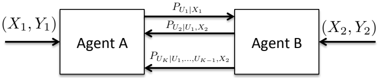
We generalize an algorithmic solution and highlight the advantages of multiple rounds of data sharing to reduce leakage.

[6] N. Tishby, F. Pereira, and, W. Bialek, "The information bottleneck method" DBLP: journals/corr/physics-004057.2000.

[7] A. Makhdoumi, S. Salamatian, N. Fawaz, and, M. Medard,"From the information bottleneck to the privacy funnel, Information Theory Workshop(ITW), 2014 IEEE, Nov 2014, pp.501-505 ".

System Model

- Consider a two-way interactive model, where agents A and B generate n-length i.i.d. sequences (X_1^n, Y_1^n) and (X_2^n, Y_2^n), respectively.
- The public data at both agents are denoted by $X_{(\cdot)}^n$ and the correlated private data by $Y_{(\cdot)}^n$.



- Without loss of generality, we assume that agent A initiates the interaction and K is even.

K-interactive Privacy Mechanism

Definition

A K-interactive privacy mechanism $(n, K, \{P_{1i}\}_{i=1}^{K/2}, \{P_{2i}\}_{i=1}^{K/2}, D_1, D_2, L_1, L_2)$ is a collection of K probabilistic mappings such that agent A shares data in the odd rounds beginning with round 1 and agent B shares in the even rounds such that:

$$\begin{cases} P_{11} : \mathcal{X}_1^n \to \mathcal{U}_1^n \\ P_{1,\frac{i+1}{2}} : (\mathcal{X}_1^n, \mathcal{U}_1^n, \mathcal{U}_2^n, \ldots, \mathcal{U}_{i-1}^n) \to \mathcal{U}_i^n & \textit{for} \quad i = 3, 5, \ldots, K-1 \\ P_{2,\frac{i}{2}} : (\mathcal{X}_2^n, \mathcal{U}_1^n, \ldots, \mathcal{U}_{i-1}^n) \to \mathcal{U}_i^n & \textit{for} \quad i = 2, 4, \ldots, K \end{cases}$$

At the end of K-rounds A and B reconstruct sequences $\hat{X}_2^n$ and $\hat{X}_1^n$, respectively, where $\hat{X}_1^n = g_2(X_2^n, U_1^n, \ldots, U_K^n)$ and $\hat{X}_2^n = g_1(X_1^n, U_1^n, \ldots, U_K^n)$, and g_1 and g_2 are appropriately chosen functions.

Cont'd.

The set of $K/2$ mechanism pairs $\{P_{1j}, P_{2j}\}_{j=1}^{\frac{K}{2}}$ is chosen to satisfy

$$\frac{1}{n}\sum_{i=1}^{\infty} E(d_1(X_{1i}, \hat{X}_{1i})) \leq D_1 + \epsilon$$

$$\frac{1}{n}\sum_{i=1}^{\infty} E(d_2(X_{2i}, \hat{X}_{2i})) \leq D_2 + \epsilon$$

$$\frac{1}{n} I(Y_1^n; U_1^n, \ldots, U_K^n, X_2^n) \leq L_1 + \epsilon$$

$$\frac{1}{n} I(Y_2^n; U_1^n, \ldots, U_K^n, X_1^n) \leq L_2 + \epsilon$$

where $d_1(\cdot,\cdot)$ and $d_2(\cdot,\cdot)$ are the given distortion measures.

Leakage-Distortion Region Theorem

Theorem

For target distortion pair (D_1, D_2), and for a K-round mechanism the leakage-distortion region is given as

$$\begin{aligned}\{(L_1, L_2, D_1, D_2) : L_1 &\geq I(Y_1; U_1, \dots, U_K, X_2),\\ L_2 &\geq I(Y_2; U_1, \dots, U_K, X_1),\\ E(d_1(X_1, \hat{X}_1)) &\leq D_1,\\ E(d_2(X_2, \hat{X}_2)) &\leq D_2\}\end{aligned}$$

such that for all k, the following Markov chains hold:

$$Y_1 \leftrightarrow (U_1, \dots, U_{2k-1}, X_2) \leftrightarrow U_{2k}$$
$$Y_2 \leftrightarrow (U_1, \dots, U_{2k-2}, X_1) \leftrightarrow U_{2k-1}$$

with $|\mathcal{U}_l| \leq |\mathcal{X}_{i_l}|.(\prod_{j=1}^{l-1} |\mathcal{U}_j|) + 1$ *where* $i_l = 1$ *if* l *is odd and* $i_l = 2$ *if* l *is even.*

Sum Leakage-Distortion Function

- Assume interaction from agent A such that the last round of interaction is from agent B to agent A.

Definition

Define a compact subset of a finite Euclidean space as

$$\mathcal{P}_K^A := \{P_{U^K|X_1,Y_1,X_2,Y_2} : P_{U^K|X_1,Y_1,X_2,Y_2} = P_{U_1|X_1} P_{U_2|U_1,X_2} \ldots, P_{U_K|U^{K-1},X_2},$$
$$E(d_1(X_1,\hat{X}_1)) \leq D_1, E(d_1(X_2,\hat{X}_2)) \leq D_2\}$$

Definition

The sum leakage-distortion function from agent A over K rounds is

$$L^A_{sum,K}(D_1,D_2) = \min_{P_{U^K|X_1,Y_1,X_2,Y_2} \in \mathcal{P}_K^A} \{I(Y_1;U_1,\ldots,U_K,X_2) + I(Y_2;U_1,\ldots,U_K,X_1)\}.$$

Interaction Reduces Leakage: Illustration

- Let (X_1, X_2) be a DSBS(p) with $P_{X_1,X_2}(0,0) = P_{X_1,X_2}(1,1) = \frac{1-p}{2}$ and $P_{X_1,X_2}(1,0) = P_{X_1,X_2}(0,1) = \frac{p}{2}$.
- (X_1, Y_1) and (X_2, Y_2) are correlated as follows:

$$\begin{aligned} Y_1 &= X_1 + Z_1 \qquad & Z_1 &\sim Ber(p) \\ Y_2 &= X_2 + Z_2 \qquad & Z_2 &\sim Ber(p) \end{aligned}$$

  and Z_1 and Z_2 are independent of X_1 and X_2.
- Let $d_A = 0$ and consider an erasure distortion measure $d_B(\cdot,\cdot)$ as:

$$d_B(x_1, \hat{x}_1) = \begin{cases} 0, & \text{if } \hat{x}_1 = x_1 \\ 1, & \text{if } \hat{x}_1 = e \\ \infty, & \text{if } \hat{x}_1 = 1 - x_1. \end{cases}$$

Theorem

With one round from agent A to agent B, the optimal solution is

$$L^A_{sum,1}(0, D_2) = 2 - [(1 - D_2)H(p) + (1 + D_2)H(2p(1-p))].$$

Sum Leakage for $K = 2$

- Consider the sum leakage-distortion for for two-round of interaction starting from agent B in round 1 and returning from A to B in round 2, $K = 2$.
- Set the conditional distribution $P_{U_1|X_2}$ as a $BSC(\alpha)$ and $P_{U_2|X_1,U_1}$ as in the following table and let $\hat{X}_1 = U_2$.

$P_{U_2\|X_1,U_1}$	$u_2 = 0$	$u_2 = e$	$u_2 = 1$
$x_1 = 0, u_1 = 0$	$1-\beta$	β	0
$x_1 = 1, u_1 = 0$	0	1	0
$x_1 = 0, u_1 = 1$	0	1	0
$x_1 = 1, u_1 = 1$	0	β	$1-\beta$

- For $p = 0.03$, $\alpha = 0.35$, and $\beta = 0.55$,
  $L^B_{sum,2}(0, D_2) = I(Y_2; U_1, X_1) + I(Y_1; U_2|U_1, X_2) = 1.1876$
- Corresponding distortion is $D_2 = E(d(X_1, \hat{X}_1)) = 0.8116$.
- By comparison, the one-round setting for this distortion is $L^A_{sum,1}(0, 0.8116) = 1.3832$.

Gaussian Sources: Interactive Mechanism

- Consider $(X_1, Y_1) \sim N(0, \Sigma_{X_1,Y_1})$, $(X_2, Y_2) \sim N(0, \Sigma_{X_2,Y_2})$, and $(X_1, X_2) \sim N(0, \Sigma_{X_1,X_2})$.
- For jointly Gaussian sources subject to mean square error distortion constraints, one round of interaction suffices to achieve the Leakage-distortion bound.

Theorem

For the private interactive mechanism, the leakage-distortion region under mean square error distortion constraints consist of all tuples (L_1, L_2, D_1, D_2) *satisfying*

$$L_1 \geq \frac{1}{2}\log\left(\frac{\sigma^2_{Y_1}}{\alpha^2 D_1 + \sigma^2_{Y_1|X_1,X_2}}\right)$$

$$L_2 \geq \frac{1}{2}\log\left(\frac{\sigma^2_{Y_2}}{\beta^2 D_2 + \sigma^2_{Y_2|X_1,X_2}}\right)$$

where $\alpha = \frac{cov(X_1,Y_1)}{\sigma^2_{Y_1}}$ *and* $\beta = \frac{cov(X_2,Y_2)}{\sigma^2_{Y_2}}$.

Leakage-Distortion Region under Log-Loss Distortion

Theorem

For the K-round interaction mechanism the leakage-distortion region under log-loss distortion, is given by:

$$\begin{aligned}\{(L_1, L_2, D_1, D_2) : L_1 &\geq I(Y_1; U_1, \ldots, U_K, X_2),\\ L_2 &\geq I(Y_2; U_1, \ldots, U_K, X_1),\\ D_1 &\geq H(X_1 | U_1, \ldots, U_K, X_2)\\ D_2 &\geq H(X_2 | U_1, \ldots, U_K, X_1)\}.\end{aligned}$$

- Distortion bounds in leakage-distortion region under log loss distortion can be rewritten as:

$$\begin{aligned}I(X_1; U_1, \ldots, U_K, X_2) &\geq \tau_1\\ I(X_2; U_1, \ldots, U_K, X_1) &\geq \tau_2.\end{aligned}$$

- The optimization problem is not convex because of the non-convexity of the feasible region.
- Problem closely related (an interactive version) to the information bottleneck problem.

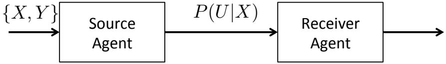
Sum-Leakage vs. Distortion under Log-loss

- Recall: K-round sum leakage under log-loss:

$$\begin{aligned} \underset{\{P_{1k},P_{2k}\}_{k=1}^{K/2}}{\text{minimize}} \quad & \sum_{i,j=1,i\neq j}^{2} I(Y_i;U_1,\ldots,U_K,X_j) \\ \text{subject to} \quad & ,I(X_1;U_1,\ldots U_K,X_2)\geq\tau_1 \\ & I(X_2;U_1,\ldots U_K,X_1)\geq\tau_2. \end{aligned}$$

- Simplest version of interactive privacy problem: K=1 (non-interactive) with $X_2 = Y_2 = \emptyset$.

$$\min_{P(U|X):I(X;U)\geq\tau} I(Y;U).$$



- Makhdoumi *et. al.* refer to the optimization problem as *privacy funnel*.[8]

[8] A. Makhdoumi, S. Salamatian, N. Fawaz, and, M. Medard,"From the information bottleneck to the privacy funnel, Information Theory Workshop(ITW), 2014 IEEE, Nov 2014, pp.501-505 ".

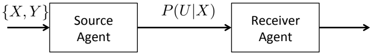
Sum-Leakage vs. Distortion under Log-loss: Privacy Funnel

- Privacy funnel is dual of information bottleneck problem.
- Information bottleneck problem is a well-studied problem introduced by Tishby.[9]
- Can Information bottleneck problem be generalized to interactive setting and applied?

[9] N. Tishby, F. Pereira, and, W. Bialek, "The information bottleneck method" DBLP: journals/corr/physics-004057.2000.

Information Bottleneck

- A single-source agent and single-receive agent setting ($X_2 = \emptyset$ and $Y_2 = \emptyset$).



- The information bottleneck problem minimizes the compression rate between X and U, while preserving a measure of the average information between U and Y such that$Y \leftrightarrow X \leftrightarrow U$ forms a Markov chain

$$\min_{P(U|X): I(Y;U) \geq \tau} I(X;U).$$

- Agglomerative Information bottleneck algorithm is a method to construct a locally optimal solution. In this method, compression rate is minimized by reducing the cardinality of $\mathcal{U}$.

Agglomerative Information Bottleneck Method

- Agglomerative Information bottleneck algorithm is a method to construct a locally optimal solution.[10] In this method, compression rate is minimized by reducing the cardinality of $\mathcal{U}$. propose an *agglomerative* algorithm.
- It begins with $\mathcal{U} = \mathcal{X}$ and reduces the cardinality of U until the constraints on both X and Y are satisfied.
- Slonim *et. al.* proved this algorithm converges to a local minima of the optimization problem.
- Makhdoumi *et. al.* applied the agglomerative information bottleneck algorithm to privacy funnel problem.

[10] N. Slonim and N. Tishby, "Agglomerative information bottleneck", Proc. of Neural Information Processing System(NIPS-99)1999.

Agglomerative Information Bottleneck Method

Agglomerative Information Bottleneck

Algorithm 1: Agglomerative information bottleneck algorithm

Input: τ and $P_{X,Y}$

1: **Initialization:** $\mathcal{X} = \mathcal{U}$ and $P_{U|X}(U|X) = \mathbf{1}_{\{\mathbf{u}=\mathbf{x}\}}$

2: **while** there exist i' and j' such that $I(Y; U^{i'-j'}) \geq \tau$ **do** among

3: those i', j', let

4: $\{u_i, u_j\} = argmax I(X;U) - I(X;U^{i'-j'})$

5: **Merge** $\{u_i, u_j\} \rightarrow u_{ij}$

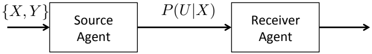
6: **Update** $\mathcal{U} = \{\mathcal{U} - \{u_i, u_j\}\} \cup \{u_{ij}\}$ and $P_{U|X}$

7: **Output** $P_{U|X}$

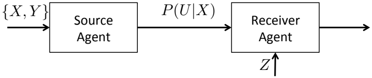
- Let U^{i-j} be the resulting U from merging u_i and u_j according to $P(u_{ij}|x) = P(u_i|x) + P(u_j|x)$.

Interaction under Log-loss: Agglomerative Approach

- Agglomerative algorithm is known for the non-interactive setting (K=1) **without** correlated side information at receiver agent.



- What if receiver agent has side information?

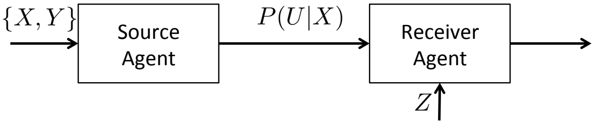


- How can agglomerative algorithm be applied?
- This is the first step to develop an algorithm for an interactive setting.
- Recall: The iterative setting involves multiple rounds and in each round we transmit to a receiver agent with correlated side information.

Merge and Search Algorithm

- Consider a one-round setting ($K = 1$) with side information at receiver agent.
- The sum-leakage optimization problem under log-loss is given by:

$$\min_{P(U|X)} I(Y;U,Z) \quad \text{s.t.} \quad I(X;U,Z) \geq \tau_1$$



- Relative to agglomerative information bottleneck problem: here U is replaced by the tuple (U,Z) and $P(U|X)$ by $P(U,Z|X) = P(U|X)P(Z|X)$.
- Merge-and-search algorithm: In the k-th iteration, indices i and j are chosen such that $I(X;U^k_{ij},Z) \geq \tau_1$ where U^k_{ij} is the resulting from merging u_i and u_j while maximizing $I(Y;U^{k-1}|Z) - I(Y;U^k_{ij}|Z)$ where U^{k-1} is the output of the algorithm in round $(k-1)$.

Agglomerative Iterative Algorithm for $K = 2$

- Consider the two-round setting ($K = 2$).
- By using merge-and-search algorithm iteratively the mechanism (P_{11}, P_{21}) can be found.
- In the first round, for a point-to-point setting with side information X_2, the distribution $P_{U_1|X_1}$ can be found.
- In the second round, the cardinality of U_2 is reduced to decrease $I(Y_2; U_1, U_2, X_1)$ using P_{U_1,X_1} computed during the first round. This reduction is computed by merging elements of U_2 conditioned on U_1 and X_2.

Agglomerative Iterative Algorithm

Algorithm: Agglomerative Iterative Algorithm

For $k = 1, \ldots, K/2$

R(2k-1): $\min I(Y_1; X_2, U_1, \ldots, U_{2k-2}, U_{2k-1})$

over $P(U_{2k-1}|X_2, U_1, \ldots, U_{2k-2})$

s.t. $I(X_1; U_{2k_1}|X_2, U_1, \ldots, U_{2k-2}) \geq \tau_{2k-1}$

Input (2k-1): $P(X_1, Y_1), P(U_{2k-2}, \ldots, U_1, X_1, X_2), \tau_{2k-1}$

Apply the merge-and-search algorithm to find local optimum.

Output (2k-1): $P(U_{2k-1}|X_1, X_2, U_1, \ldots, U_{2k-2})$

R(2k): $\min I(Y_2; X_1, U_1, \ldots, U_{2k-1}, U_{2k})$

over $P(U_{2k}|X_1, U_1, \ldots, U_{2k-1})$

s.t. $I(X_2; U_{2k}|X_1, U_1, \ldots, U_{2k-1}) \geq \tau_{2k}$

Input (2k): $P(X_2, Y_2), P(U_{2k-1}, \ldots, U_1, X_1, X_2), \tau_{2k}$

Apply the merge-and-search algorithm to find local optimum.

Output (2k): $P(U_{2k}|X_1, X_2, U_1, \ldots, U_{2k-1})$

Output : $P(U_1|X_1), \ldots, P(U_K|U_1, \ldots, U_{K-1}, X_2)$

Gaussian Sources Under Log-Loss Distortion

- Tishby *et. al.* proved the mapping $P_{U|X}$ that minimizes the information bottleneck problem for jointly Gaussian sources is Gaussian.[11]

$$\begin{aligned} \min_{\substack{P_{U|X} \\ Y \leftrightarrow X \leftrightarrow U}} \quad & I(X;U) \\ \text{subject to} \quad & I(Y;U) \geq \tau. \end{aligned}$$

- For the non-interactive (one-way) single source and single receiver agent setting with the leakage-distortion tradeoff, the optimal leakage-minimizing mechanism is Gaussian.

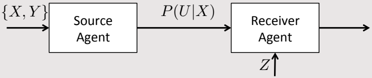
$$\begin{aligned} \min_{\substack{P_{U|X} \\ Y \leftrightarrow X \leftrightarrow U}} \quad & I(Y;U) \\ \text{subject to} \quad & I(X;U) \geq \tau. \end{aligned}$$

[11] G. Chechik, A. Globerson, N. Tishby, and, Y. Weiss, “The information bottleneck for Gaussian variables” In journal of Machine Learning Research/2004.

Optimality of a One-Round Gaussian Private Interactive Mechanism

Lemma

Suppose (X, Y) and (X, Z) are jointly Gaussian and let $P_{U|X}$ be a privacy mechanism such that $U \leftrightarrow X \leftrightarrow Z$ forms a Markov chain. The optimal mechanism $P_{U|X}$ minimizing $I(Y; U, Z)$ subject to $I(X; U, Z) \geq \tau$ is Gaussian.

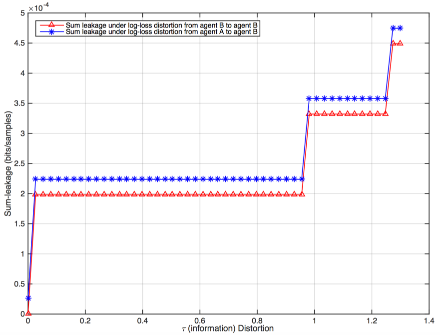


Theorem

Consider a two-agent interactive setting with log-loss distortion and jointly Gaussian sources. The optimal leakage-distortion region can be achieved in one round of interaction.

Illustration of the Results

- The US Census dataset is a sample of US population from 1994. X_1 =(age, gender), X_2 = (ethnicity, gender), Y_1 =(work class), and, Y_2 =(income level).
- Find the optimal solution by using agglomerative interactive privacy algorithm and compute sum leakage for the two round and the one round interactive mechanism under log-loss distortion at agent B.
- Let $d_A = 0$ and d_B be the log-loss distortion measure.
- The blue curve with stars is the leakage for one round from A to B. The red curve with triangles denotes the sum leakage starting from B to A and back to B.



Conclusions

- A K-round private interactive mechanism between two agents with correlated sources was introduced, and the leakage-distortion region for general distortion functions was determined.
- A K-round private interactive mechanism under log-loss distortion was introduced.
- Sum leakage under log loss distortion and an algorithm to find an optimal mechanism for that were introduced.