Information-Theoretic Private Interactive Mechanism

Bahman Moraffah

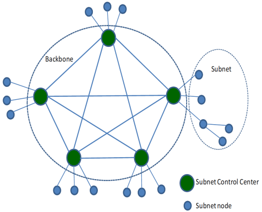
Arizona State University

August 19, 2015

Overview

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.

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 thesis 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

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]
- Closely related is work by Ma *et. al.*.
  - Our approach on conditions when interaction helps is similar to Ma. [6]

---

[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.

[6] N. Ma, P. Ishwar "The infinite message limit of two terminal interactive source coding" Information theory, IEEE Transaction on, vol 31, no. 6, 2013.

Information Bottleneck

- Goal is to minimize the compression rate of public data subject to constraint on the log-loss distortion of private data.[7]
- 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.*[8] developed tradeoff region.
- Use an algorithm based on the agglomerative information bottleneck algorithm.

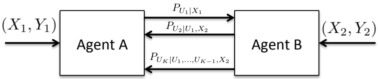
We generalize an algorithmic solution and highlight the advantages of multiple rounds of data sharing to reduce leakage.

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

[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 ".

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 $Y_{(\cdot)}^n$.



- We assume that the private data is hidden and can only be leaked through the public data.
- 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:

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

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

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

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

$$\begin{aligned} Y_1 \leftrightarrow (U_1, \ldots, U_{2k-1}, X_2) \leftrightarrow U_{2k} \\ Y_2 \leftrightarrow (U_1, \ldots, U_{2k-2}, X_1) \leftrightarrow U_{2k-1} \end{aligned}$$

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.

- 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

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

Property of $L_{sum,k}$

Lemma

For all k:
(1) $L^A_{sum,(k-1)} \geq L^A_{sum,k}$. Similarly, $L^B_{sum,(k-1)} \geq L^B_{sum,k}$.
(2) $L^B_{sum,(k-1)} \geq L^A_{sum,k}$. Similarly, $L^A_{sum,(k-1)} \geq L^B_{sum,k}$.

Proof.

For all k,

- (1) follows from the fact that any $(k-1)$-round interactive mechanism starting at one of the agent (e.g., A) can be considered as special case of k-round interactive mechanism starting at the same agent with $P_{U_k|U^{k-1},X_1} = 0$.
- The bounds in (2) follows from the fact that any $(k-1)$-round interactive mechanism initiated at B (resp. A) can be considered as a special case of a k-round interactive mechanism initiated at A (resp. B) with $P_{U_1|X_1} = 0$ (resp. $P_{U_1|X_2} = 0$).

□

Definition

$L_{sum,\infty} := \lim_{k\to\infty} L^A_{sum,k} = \lim_{k\to\infty} L^B_{sum,k}$.

- From previous lemma, $L^A_{sum,k}$ and $L^B_{sum,k}$ are both non-increasing in k and bounded from below, and thus their limits exist.
- From previous lemma, $L^A_{sum,k-1} \geq L^B_{sum,k} \geq L^A_{sum,k+1}$ Thus, taking limits, since both $L^A_{sum,k}$ and $L^B_{sum,k}$ converge, we have that

$$L_{sum,\infty} := \lim_{k\to\infty} L^A_{sum,k} = \lim_{k\to\infty} L^B_{sum,k}.$$

Therefore, $L_{sum,\infty}$ is well-defined.

- From both a theoretical and an application viewpoint, it is of much interest to understand whether interaction reduces privacy leakage or if a single round of data sharing suffices for a fixed privacy budget (leakage constraint).
- Ma *et. al.* considered interactive source coding problem and discussed conditions under which interaction helps.[9]
- Ma's approach can be applied to our interactive leakage-distortion problem with both public and private variables.

[9] N. Ma, P. Ishwar. "The infinite message limit of two terminal interactive source coding" Information theory, IEEE Transaction on, vol 31, no. 6.

Leakage Reduction Function

- To characterize $L_{sum,\infty}$, introduce a *leakage-reduction function*.

Definition

The leakage reduction function for a K-round interactive mechanism initiated at agent A is defined as

$$\eta_K^A(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) := H(Y_1) + H(Y_2) - L_{sum,K}^A(D_1, D_2)$$
$$= \max_{P_{U^K|X_1,Y_1,X_2,Y_2} \in \mathcal{P}_K^A} [H(Y_1|U^K, X_2) + H(Y_2|U^K, X_1)]$$

- $\eta_K^A(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$ depends on the distributions $P_{X_1,Y_1|X_2}$ and $P_{X_2,Y_2|X_1}$.
- Evaluating η_K^A is equivalent to evaluating $L_{sum,K}^A$.
- η_K^A and η_K^B are non-decreasing functions of K.
- For $\eta_\infty = \lim_{K\to\infty} \eta_K^A$, we have $L_{sum,\infty}^A = H(Y_1) + H(Y_2) - \eta_\infty$.
- $L_{sum,0}^A = L_{sum,0}^B = L_{sum,0} = I(Y_1; X_2) + I(Y_2; X_1)$.
- $\eta_0 = H(Y_1|X_2) + H(Y_2|X_1)$.

Marginal-Perturbation-Closed Family of Joint Distributions

- $\eta_K^A = \max_{P_{U^K|X_1,Y_1,X_2,Y_2} \in \mathcal{P}_K^A} [H(Y_1|U^K, X_2) + H(Y_2|U^K, X_1)]$ depends on P_{X_1,Y_1,X_2,Y_2} only through $P_{X_2,Y_2|X_1}$ and $P_{X_1,Y_1|X_2}$.

Definition

The marginal perturbation set $\mathcal{P}_{X_2,Y_2|X_1}$ for a given joint distribution P_{X_1,Y_1,X_2,Y_2} is defined as

$$\mathcal{P}_{X_2,Y_2|X_1}(P_{X_1,Y_1,X_2,Y_2}) = \{P'_{X_1,Y_1,X_2,Y_2} : P'_{X_1,Y_1,X_2,Y_2} << P_{X_1,Y_1,X_2,Y_2}, P'_{X_2,Y_2|X_1} = P_{X_2,Y_2|X_1}\}$$

where " $<<$ " is majorizing operator.

- $\mathcal{P}_{X_1,Y_1|X_2}(P_{X_1,Y_1,X_2,Y_2})$ can similarly be defined.
- $\eta_K^A(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$ depends on the distributions $P_{X_2,Y_2|X_1}$ and $P_{X_1,Y_1|X_2}$.
- Sufficient to focus on the family of distributions which is closed with respect to $\mathcal{P}_{X_2,Y_2|X_1}$ and $\mathcal{P}_{X_1,Y_1|X_2}$.

Definition

A family of joint distributions $\mathcal{P}_{X_1,Y_1,X_2,Y_2}$ is marginal-perturbation-closed if for all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$, $\mathcal{P}_{X_2,Y_2|X_1} \cup \mathcal{P}_{X_1,Y_1|X_2} \subseteq \mathcal{P}_{X_1,Y_1,X_2,Y_2}$.

Lemma: Relationship between $(k-1)$-Round and k-Round Interactive Mechanism

Lemma

1. For all $k \in \mathbb{Z}^+$ and $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$ we have

$$\eta_k^A(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) =$$

$$\max_{P(U_1|X_1)} \left\{ \max_{\substack{\forall u_1 \in \mathcal{U}_1, (D_1', D_2)_{u_1} \in \mathcal{D}^2 \\ (D_1', D_2)_{u_1} : E((D_1', D_2)_{u_1}) \leq (D_1, D_2)}} \left\{ \sum_{u_1 \in \mathcal{U}_1} g(u_1) \right\} \right\}.$$

   where $g(u_1) = P(u_1)\eta_{k-1}^B(P_{X_1,Y_1,X_2,Y_2|u_1}, (D_1', D_2)_{u_1})$.

2. For all $k \in \mathbb{Z}^+$ and all $(q_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \in \mathcal{P}_{X_1,Y_1,X_2,Y_2} \times \mathcal{D}^2$, η_k^A is concave on $\mathcal{P}_{X_2,Y_2|X_1} \times \mathcal{D}^2$.

3. For all $k \in \mathbb{Z}^+$ and all $(q_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \in \mathcal{P}_{X_1,Y_1,X_2,Y_2} \times \mathcal{D}^2$, if $\eta : \mathcal{P}_{X_1,Y_1,X_2,Y_2} \times \mathcal{D}^2 \to \mathbb{R}$ is concave on $\mathcal{P}_{X_2,Y_2|X_1} \times \mathcal{D}^2$ and if for all $(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \in \mathcal{P}_{X_2,Y_2|X_1}(q_{X_1,Y_1,X_2,Y_2}) \times \mathcal{D}^2$, $\eta_{k-1}^B(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \leq \eta(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$, then for all $(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \in \mathcal{P}_{X_2,Y_2|X_1}(q_{X_1,Y_1,X_2,Y_2}) \times \mathcal{D}^2$, $\eta_k^A(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \leq \eta(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$.

Sketch of Proof.

- part 1[10]
  - To construct a k-round interactive mechanism, we first pick U_1.
  - For each realization of $U_1 = u_1$, construct the remaining by considering $(k-1)$-round initiated at agent B but with different data distribution $P_{X_1,Y_1,X_2,Y_2|U_1=u_1} \in \mathcal{P}_{X_2,Y_2|X_1}(P_{X_1,Y_1,X_2,Y_2})$.
  - Distortion vector $(D_1', D_2)_{u_1}$ for each realization $U_1 = u_1$ in $(k-1)$-round interactive subproblem could be different from the original distortion vector (D_1, D_2).
  - $\sum_{u_1}(D_1', D_2)_{u_1} P_{U_1}(u_1) = (D_1, D_2)$.
- part 2
  - By using the relationship between $(k-1)$-round and k-round interactive mechanism and definition of concave function, η_k^A is concave on $\mathcal{P}_{X_2,Y_2|X_1} \times \mathcal{D}^2$.
- part 3
  - Using the relationship between $(k-1)$-round and k-round interactive mechanism and $\eta_{k-1}^B \leq \eta$ imply $\eta_k^A \leq \eta$.

- By reversing the roles of agent A and B in Lemma, we can prove the same lemma for agent B.

[10] N. Ma, P. Ishwar. "The infinite message limit of two terminal interactive source coding" Information theory, IEEE Transaction on, vol 31, no. 6.

η_0-Majorizing Family of Functionals

- Interaction does not help if $\eta_k^A = \eta_{k+1}^B$.
- η_{k+1}^B is concave on $\mathcal{P}_{X_1,Y_1|X_2}$ (previous lemma).
- Interaction does not help if η_k^A is concave on $\mathcal{P}_{X_1,Y_1|X_2}$.
- To characterize η_∞, introduce a set of functionals as follows:

Definition

η_0-majorizing family of functionals $\mathcal{F}_D(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$ is the set of all functionals $\eta : \mathcal{P}_{X_1,Y_1,X_2,Y_2} \times \mathcal{D}^2 \to \mathbb{R}$ satisfying

1. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$ and $(D_1, D_2) \in \mathcal{D}^2$, $\eta(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \geq \eta_0(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$.
2. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$, η is concave on $\mathcal{P}_{X_2,Y_2|X_1}$.
3. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$, η is concave on $\mathcal{P}_{X_1,Y_1|X_2}$.

Properties of η_∞

Theorem

$\eta_\infty(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2) \in \mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$ and η_∞ is the least element of the set $\mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$.

Proof.

- η_∞ is in η_0-majorizing family of functionals $\mathcal{F}_D(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$ since:
  - Condition 1 in definition of η_0-majorizing family of functionals is satisfied since $L_{sum,\infty} \leq L_{sum,0}$.
  - Condition 2 in definition of η_0-majorizing family of functionals is satisfied since $\eta_\infty = lim_{k\to\infty}\eta_k^A$ and η_k^A is concave on $\mathcal{P}_{X_2,Y_2|X_1}$.
  - Condition 3 in definition of η_0-majorizing family of functionals is satisfied since $\eta_\infty = lim_{k\to\infty}\eta_k^B$ and η_k^B is concave on $\mathcal{P}_{X_1,Y_1|X_2}$.
- Proof that η_∞ is the smallest element of $\mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$:
  - By using induction on k in addition to part 3 of Lemma , if $\eta_{k-1}^B \leq \eta$, then $\eta_k^A \leq \eta$, η_∞ is the least element of $\mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$.

□

Conditions under which Interaction Does Not Help

Theorem

The following equivalent conditions establish when interaction does not help.

1. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$ and $D = (D_1, D_2) \in \mathcal{D}^2$, $\eta_k^A(P_{X_1,Y_1,X_2,Y_2}, D) = \eta_\infty(P_{X_1,Y_1,X_2,Y_2}, D)$.
2. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$ and $D = (D_1, D_2) \in \mathcal{D}^2$, $\eta_k^A(P_{X_1,Y_1,X_2,Y_2}, D) = \eta_{k+1}^B(P_{X_1,Y_1,X_2,Y_2}, D)$.
3. For all $P_{X_1,Y_1,X_2,Y_2} \in \mathcal{P}_{X_1,Y_1,X_2,Y_2}$ and $D = (D_1, D_2) \in \mathcal{D}^2$, η_k^A is concave on $\mathcal{P}_{X_1,Y_1|X_2}(P_{X_1,Y_1,X_2,Y_2}) \times \mathcal{D}^2$.

Proof.

- Condition 1 implies condition 2 since $\eta_k^A \leq \eta_{k+1}^B \leq \eta_\infty$. This inequality holds due to $L_{sum,k}^A \geq L_{sum,k+1}^B$.
- Condition 2 implies condition 3 since $\eta_{k+1}^B(P_{X_1,Y_1,X_2,Y_2}, D_1, D_2)$ is concave on $\mathcal{P}_{X_1,Y_1|X_2}(P_{X_1,Y_1,X_2,Y_2}) \times \mathcal{D}^2$.
- Condition 3 implies condition 1 since concavity of η_k^A on $\mathcal{P}_{X_2,Y_2|X_1}$ in addition to the fact that $\eta_k^A \geq \eta_0$ lead $\eta_k^A \in \mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$. According to theorem, η_∞ is the least element of $\mathcal{F}_\mathcal{D}(\mathcal{P}_{X_1,Y_1,X_2,Y_2})$, thus $\eta_k^A \geq \eta_\infty$. Therefore, $\eta_k^A = \eta_\infty$.

□

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

Theorem

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

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

Proof.

- $L^{A}_{sum,1}(0, D_2) = \min_{P_{U_1|X_1}} [I(X_1; Y_2) + I(Y_1; U_1, X_2)]$
- $L^{A}_{sum,1}(0, D_2) = 2 - H(2p(1-p)) - \max_{P(U_1|X_1)} H(Y_1|U_1, X_2)$ where $\mathcal{U} = \{0, e, 1\}$ and

$$P(U_1|X_1) = \begin{cases} \alpha_0, & \text{if } x = 0 \text{ and } u = e \\ 1 - \alpha_0, & \text{if } x = 0 \text{ and } u = 0 \\ \alpha_1, & \text{if } x = 1 \text{ and } u = e \\ 1 - \alpha_1, & \text{if } x = 1 \text{ and } u = 1 \\ 0, & \text{otherwise} \end{cases}$$

Proof.

- $E(d_B(X_1, U_1)) = P_{X_1}(0)\alpha_0 + P_{X_1}(1)\alpha_1 \leq D_2$.
- $P(X_1 = 0, U_1 = 1) = P(X_1 = 1, U_1 = 0) = 0$ since otherwise $E(d_B(X_1, U_1)) = \infty$.
- Simplify $L^A_{sum,1}(0, D_2)$

$$\begin{aligned} H(Y_1|U_1, X_2) =& \frac{1}{2}(1-\alpha_0)H(p) + \frac{1}{2}(1-\alpha_1)H(p) \\ &+ [\frac{\alpha_0}{2}(1-p) + \frac{\alpha_1}{2}p]H(\frac{(1-p)^2\alpha_0 + p^2\alpha_1}{(1-p)\alpha_0 + p\alpha_1}) \\ &+ [\frac{\alpha_0}{2}p + \frac{\alpha_1}{2}(1-p)]H(\frac{p(1-p)\alpha_0 + p(1-p)\alpha_1}{p\alpha_0 + (1-p)\alpha_1}) \end{aligned}$$

- $H(Y_1|U_1, X_2)$ is maximized if $\alpha_0 = \alpha_1 = \alpha$, then the result is attained.

□

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* $\beta = \frac{cov(X_2,Y_2)}{\sigma^2_{Y_2}}$.

Proof: Converse.

If (X_1, Y_1) is jointly Gaussian, we can write $Y_1 = \alpha X_1 + Z_1$, where Z_1 is a zero mean Gaussian random variable independent of X_1.

$$
\begin{aligned}
L_1 + \epsilon \geq & \frac{1}{n} I(Y_1^n; U_1^n, \dots, U_K^n, X_2^n) \\
=& \frac{1}{n}[nh(Y_1) - \sum_{i=1}^{n} h(Y_{1i}|U_1^n, \dots, U_K^n, X_2^n, Y_1^{i-1})] \\
\geq & h(Y_1) - \frac{1}{n}\sum_{i=1}^{n} h(Y_{1i}|U_1^n, \dots, U_K^n, X_2^n) \\
\geq & h(Y_1) - \frac{1}{n}\sum_{i=1}^{n} \frac{1}{2}\log(2\pi e(Var(Y_{1i}|U_1^n, \dots, U_K^n, X_2^n))) \\
\geq & h(Y_1) - \frac{1}{2}\log(2\pi e \frac{1}{n}\sum_{i=1}^{n}(Var(Y_{1i}|U_1^n, \dots, U_K^n, X_2^n))) \\
\geq & h(Y_1) - \frac{1}{2}\log(2\pi e \frac{1}{n}\sum_{i=1}^{n}(Var(\alpha X_{1i} + Z_{1i}|U_1^n, \dots, U_K^n, X_2^n))) \\
\geq & \frac{1}{2}\log(\frac{\sigma_{Y_1}^2}{\alpha^2 D_1 + \sigma_{Y_1|X_1,X_2}^2})
\end{aligned}
$$

Similarly, we can prove $L_2 \geq \frac{1}{2}\log(\frac{\sigma_{Y_2}^2}{\beta^2 D_2 + \sigma_{Y_2|X_1,X_2}^2})$.

Proof: Achievability.

- The sequence U_1^n is chosen such that the 'test channel' from U_1 to X_1 yields $U_1 = X_1 + V_1$, where V_1 is Gaussian and independent of the rest of random variables, with variance Q chosen to satisfy distortion condition D_1 and $\hat{X}_1 = E[X_1|U_1, X_2]$.
- For such a system, the achievable distortion is $D_1 = E(Var(X_1|U_1, X_2))$ (no interaction is required).

□

Log-Loss Distortion

Definition

For a random variable $X \in \mathcal{X}$ and its reproduction alphabet $\hat{\mathcal{X}}$ as the set of probability measures on $\mathcal{X}$, the log-loss distortion is defined as

$$d(x, \hat{x}) = \log\left(\frac{1}{\hat{x}(x)}\right).$$

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:

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

Proof.

The distortion bounds result from applying $\hat{X}_i = P(X_i = x_i|U_1, \ldots, U_K, X_j)$ $i = 1, 2$, $j \neq i$

$$\begin{aligned}&D_i \geq E(d(X_i, \hat{X}_i)) \\ &= \sum_{x_i, u_1, \ldots, u_K} P(x_i, u_1, \ldots, u_K) \log\left(\frac{1}{P(x_i|u_1, \ldots, u_K, x_j)}\right) = H(X_i|U_1, \ldots, U_K, X_j),\end{aligned}$$

□

Sum-Leakage vs. Distortion under Log-loss

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

$$I(X_1; U_1, \ldots, U_K, X_2) \geq \tau_1$$
$$I(X_2; U_1, \ldots, U_K, X_1) \geq \tau_2.$$

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

$$\min_{\{P_{1k}, P_{2k}\}_{k=1}^{K/2}} \sum_{i,j=1, i \neq j}^{2} I(Y_i; U_1, ..., U_K, X_j)$$

such that for all $i, j = 1, 2, i \neq j$,

$$I(X_i; U_1, ... U_K, X_j) \geq \tau_i.$$

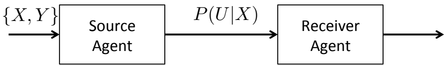
- The optimization problem is not convex because of the non-convexity of the feasible region.
- Problem closely related (an interactive version) to the information bottleneck problem.

- 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 $X_2 = Y_2 = \emptyset$.

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



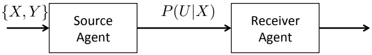
- Makhdoumi *et. al.* refer to the optimization problem as *privacy funnel*.[11]

[11] 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 ".

- Privacy funnel is dual of information bottleneck problem.
- Information bottleneck problem is a well-studied problem introduced by Tishby.[12]
- Can Information bottleneck problem be generalized to interactive setting and applied?

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

- 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

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

- Tishby *et. al.* characterized a locally optimal solution to information bottleneck problem by minimizing the Lagrangian of the problem and using KKT conditions.[13]
- They introduced an iterative algorithm to construct a locally optimal solution by applying the fixed-point equations.
- Agglomerative Information bottleneck algorithm is another method to construct a locally optimal solution. In this method, compression rate is minimized by reducing the cardinality of $\mathcal{U}$.

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

Sum-Leakage under Log-loss: Iterative Algorithm

- Sum leakage optimization under log-loss:

Theorem

Consider the two agent K-round leakage-distortion region and their Markov conditions. The conditional distribution $P_{U_j|U^{j-1},X_{(.)}}(u_j|u^{j-1},x_{(.)})$, for all j, with Lagrange mutipliers β_1 and β_2 is the stationary point of

$$\mathcal{L} = I(Y_1;U^K,X_2) + I(Y_2;U^K,X_1) - \beta_1 I(X_1;U^K,X_2) - \beta_2 I(X_2;U^K,X_1)$$

if and only if

$$P(u_j|u^{j-1},x_s) = \frac{P(u^j)}{\mathcal{Z}(x_1,x_2,u^{j-1},\beta_1,\beta_2)} exp\{-\beta_1^{-1}[E_{X_t|X_s,u^{j-1}}\{D(P(y_1|x_1,x_2,u^{j-1})||P(y_1|u^j,x_t))\}$$
$$+D(P(y_2|x_s,u^{j-1})||P(y_2|x_s,u^j))] - D(P(x_t|x_s,u^{j-1})||P(x_t|u^j))\}$$

for $\{s,t\} \in \{1,2\}$ and $s \neq t$ and for some β_1 and β_2, where $\mathcal{Z}(x_1,x_2,u^{j-1},\beta_1,\beta_2)$ is a normalization function.

- For each round j, a fixed point equation that can be solved by extending the iterative algorithm of Tishby. Repeat procedure for each j.

- Recall: Information bottleneck problem is

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

  and $Y \leftrightarrow X \leftrightarrow U$ forms a Markov chain
- Slonim *et. al.*[14] propose an *agglomerative* algorithm.
- The goal is to iteratively find the optimal U.
- It begins with $\mathcal{U} = \mathcal{X}$ and reduces the cardinality of U until the constraints on both X and Y are satisfied.
- They 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.

[14] 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 $P_{X,Y}$

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

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

those i', j', let

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

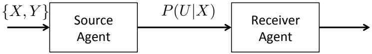
Merge $\{u_i, u_j\} \to u_{ij}$

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

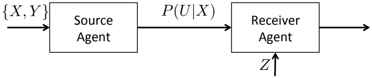
Output $P_{U|X}$

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

- 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?

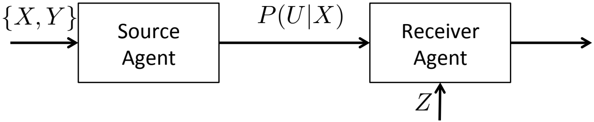


- How can agglomerative algorithm be applied?
- This is the first step to develop an algorithm for an interactive setting.
- Recall: The iterative setting involves multiple rounds and in each round we transmit to a receiver agent with correlated side information.

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:

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



- 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 $I(X;U_{ij}^k, Z) \geq \tau_1$ where U_{ij}^k is the resulting from merging u_i and u_j while maximizing $I(Y;U^{k-1}|Z) - I(Y;U_{ij}^k|Z)$ where U^{k-1} is the output of the algorithm in round $(k-1)$.

- 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.

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): $P(X_1, Y_1)$, $P(U_{2k-2}, \ldots, U_1, X_1, X_2)$, τ_{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): $P(X_2, Y_2)$, $P(U_{2k-1}, \ldots, U_1, X_1, X_2)$, τ_{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 : $P(U_1|X_1), \ldots, P(U_K|U_1, \ldots, U_{K-1}, X_2)$

- Tishby *et. al.* proved the mapping $P_{U|X}$ that minimizes the information bottleneck problem for jointly Gaussian sources is Gaussian.[15]

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

- 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.

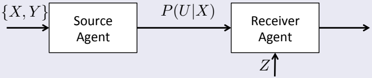
$$\begin{aligned} \min_{\substack{P_{U|X} \\ Y \leftrightarrow X \leftrightarrow U}} \quad & I(Y;U) \\ \text{subject to} \quad & I(X;U) \geq \tau. \end{aligned}$$

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

Non-Interactive Private Mechanism with Correlated Side Information Under Log-loss Distortion

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.



Proof.

- Define $V = (U, Z)$. Now, consider the following optimization problem

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

.

- The optimizing mechanism $P_{V|X}$, and therefore, the output V are Gaussian.
- Since V and Z are Gaussian, U is Gaussian.

□

Optimality of a One-Round Gaussian Private Interactive Mechanism

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.

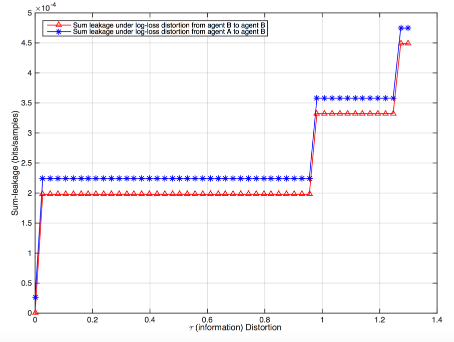
Proof.

- According to previous lemma, the optimal mechanism for non-interactive setting with side information is Gaussian.
- Since the interactive setting involves a set of K such mechanisms, the tuple $(U_1, \ldots, U_K)$ should also be Gaussian, i.e., one round of interaction suffices.

□

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.
- Conditions under which interaction reduces leakage was introduced, and it was illustrated through an example.
- 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.
- Benefit of using interaction under log-loss distortion was discussed.

Future Work

- Evaluating leakage for different classes of statistical inference attacks.
- Extension to the multi-agent ($K > 2$) case.