



**TACTILENet**

**This work was supported in part by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 690893.**

# Distributed Hypothesis Testing With a Privacy Constraint

Sreejith Sreekumar

Information Processing and Communications Lab  
Department of Electrical and Electronic Engineering  
Imperial College London

Joint work with Deniz Gündüz and Asaf Cohen.

**Acknowledgement:** This work received support from the European Union's H2020 Research and Innovation Programme through project TACTILENet: Towards Agile, efficient, auTonomous and massIvely Large Network of things (agreement 690893).



# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint
- 3 Equivocation as a Privacy measure
- 4 Average distortion as a Privacy measure
- 5 Concluding Remarks and Open problems

# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint
- 3 Equivocation as a Privacy measure
- 4 Average distortion as a Privacy measure
- 5 Concluding Remarks and Open problems

# Problem Motivation

Distributed Statistical Inference problems- data indirectly available to the statistician.

Data may contain sensitive information irrelevant for given inference task.

Trade-off exists between performance and privacy.

# Problem Motivation

Distributed Statistical Inference problems- data indirectly available to the statistician.

Data may contain sensitive information irrelevant for given inference task.

Trade-off exists between performance and privacy.

# Problem Motivation

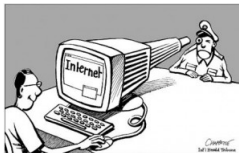
Distributed Statistical Inference problems- data indirectly available to the statistician.

Data may contain sensitive information irrelevant for given inference task.


Trade-off exists between performance and privacy.

# Examples

## Social Media



## Online shopping



More than **50%** of Android shopping apps send trackers to users

third-party domains by Android apps:

- name
- location
- email address
- phone number
- search terms



# Hypothesis Testing (HT)

Method of statistical inference to decide between different possible candidates based on available data.

## Simple Binary HT:

Null Hypothesis ( $H_0$ )

Alternate Hypothesis ( $H_1$ )

## Examples:

Weather prediction:

$H_0$  : Rain today,  $H_1$  : No rain today.

Testing probability distribution:

$H_0 : X \sim P_X, H_1 : X \sim Q_X.$

# Performance metrics:

$$H_0 : X \sim P_X, \quad H_1 : X \sim Q_X.$$

True hypothesis:  $H \in \{0, 1\}$ , Decision rule:  $g(x)$

Output of HT:  $\hat{H} \in \{0, 1\}$ .

Type 1 and Type 2 error probabilities:

$$\alpha(g(x)) = \mathbb{P}(\hat{H} = 1 | H = 0),$$

$$\beta(g(x)) = \mathbb{P}(\hat{H} = 0 | H = 1).$$

Bayesian Approach: Priors known.

$$\mathbb{P}(H = 0) = \mu_0, \quad \mathbb{P}(H = 1) = \mu_1, \quad \mu_0 + \mu_1 = 1,$$

$$\min_{\{g(x)\}} \mu_0 \alpha(g(x)) + \mu_1 \beta(g(x)).$$

Neyman-Pearson Approach: Priors unknown.

$$\min_{\{g(x)\}} \beta(g(x)) \text{ such that } \alpha(g(x)) \leq \epsilon.$$

# Optimal Test: Neyman-Pearson framework

## Neyman-Pearson Test:

Optimal Decision rule:  $g^*(x) = \mathbb{1} \left( \log \left( \frac{P_X(x)}{Q_X(x)} \right) > \tau \right)$ ,  $\tau \in \mathbb{R}$ .

## Large deviation regime:

$X^n = (X_1, \dots, X_n)$ -  $n$  i.i.d. samples of data available.

$$H_0 : X^n \sim \prod_{i=1}^n P_X, \quad H_1 : X^n \sim \prod_{i=1}^n Q_X.$$

Type 2 error exponent(T2EE):

$$\kappa(\epsilon) = \max_{g^{(n)}} \frac{-\log(\beta_n)}{n} \text{ s.t. } \alpha_n \leq \epsilon.$$

## Stein-Chernoff Lemma:

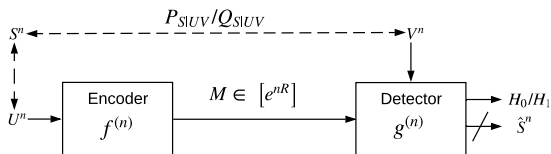
$$\kappa(\epsilon) = D(P_X \| Q_X), \quad \forall \epsilon \in (0, 1),$$

$$D(P_X \| Q_X) := \sum_{x \in \mathcal{X}} P_X(x) \log \left( \frac{P_X(x)}{Q_X(x)} \right).$$

# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint**
- 3 Equivocation as a Privacy measure
- 4 Average distortion as a Privacy measure
- 5 Concluding Remarks and Open problems

# Model:



Encoder observes  $U^n$  and sends  $M$  to the detector.

Detector observes  $V^n$  and performs following HT using  $M$  and  $V^n$ .

$$H_0 : (U^n, V^n) \sim \prod_{i=1}^n P_{UV}$$

$$H_1 : (U^n, V^n) \sim \prod_{i=1}^n Q_{UV}$$

Private data  $S^n$  correlated with  $(U^n, V^n)$  needs to be protected.

# Metrics of Privacy

- Equivocation or Information Leakage:

$$\frac{1}{n}H(S^n|M, V^n, H = i) \text{ or } \frac{1}{n}I(S^n; M|V^n, H = i), i \in \{0, 1\}.$$

- Average distortion:

Given distortion measure  $d : \mathcal{S} \times \hat{\mathcal{S}} \rightarrow [0, D_m]$ ,

$$\inf_{P_{\hat{S}^n|M, V^n}} \mathbb{E} \left( d(S^n, \hat{S}^n) \right),$$

$$d(s^n, \hat{s}^n) := \frac{1}{n} \sum_{i=1}^n d(s_i, \hat{s}_i)$$

# Metrics of Privacy

- Equivocation or Information Leakage:

$$\frac{1}{n}H(S^n|M, V^n, H = i) \text{ or } \frac{1}{n}I(S^n; M|V^n, H = i), i \in \{0, 1\}.$$

- Average distortion:

Given distortion measure  $d : \mathcal{S} \times \hat{\mathcal{S}} \rightarrow [0, D_m]$ ,

$$\inf_{P_{\hat{S}^n|M, V^n}} \mathbb{E} \left( d(S^n, \hat{S}^n) \right),$$

$$d(s^n, \hat{s}^n) := \frac{1}{n} \sum_{i=1}^n d(s_i, \hat{s}_i)$$

### Distributed HT in rate-limited settings

- Error exponent- Ahlswede and Csiszár [1986] and Han [1987].
- Testing and lossy data compression-Katz, Piantinada and Debbah [2017].
- Noisy Channel-Sreekumar and Gündüz [2017].
- Multiple detectors and Multi-hop relay setting- Salehkaleiber and Wigger [2017].
- Error exponents via Channel detection codes- Weinberger and Kochman [2017].



## Related work: HT under privacy constraints

- Direct HT under mutual information leakage constraint- Liao, Sankar, Tan and Calmon [2016].
- Distributed HT under mutual information leakage constraint- Amor, Gilani, Salehkalaibar and Tan [2018].

Data is processed through a privacy mechanism before it is observed by the encoder.

Privacy mechanism adds noise to increase privacy of sensitive information.

Information leakage measured as mutual information between input (data) and output of privacy mechanism.

Results restricted to memoryless privacy mechanisms.

# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint
- 3 Equivocation as a Privacy measure**
- 4 Average distortion as a Privacy measure
- 5 Concluding Remarks and Open problems

# Rate- Error Exponent- Equivocation Trade-off

## Definition

$\mathcal{R}_e(\epsilon)$  : Closure of the set of all  $(R, \kappa, \Omega_0, \Omega_1)$  tuples such that

$$\begin{aligned} \exists f^{(n)} : \mathcal{U}^n &\rightarrow \{P_{M|U^n}\}, \mathcal{M} = [e^{nR}], \\ g^{(n)} : [e^{nR}] \times \mathcal{V}^n &\rightarrow \{P_{\hat{H}|M, V^n}\}, \end{aligned}$$

such that

$$\begin{aligned} \liminf_{n \rightarrow \infty} -\frac{\log(\beta(f^{(n)}, g^{(n)}))}{n} &\geq \kappa, \alpha(f^{(n)}, g^{(n)}) \leq \epsilon, \\ \liminf_{n \rightarrow \infty} \frac{1}{n} H(S^n | M, V^n, H = H_i) &\geq \Omega_i, i = 0, 1. \end{aligned}$$

# Optimal Trade-off: Single-letter characterization

Testing Against Independence:

$$P_{SUV} = P_{S|UV}P_{UV}, \quad Q_{SUV} = Q_{S|UV}P_U P_V.$$

## Theorem

$(R, \kappa, \Omega_0, \Omega_{min}) \in \mathcal{R}_e(0)$  iff  $\exists$  an auxiliary r.v.  $W$  such that the Markov chain  $(S, V) - U - W$  is satisfied and

$$R \geq I_P(W; U),$$

$$\kappa \leq I_P(W; V),$$

$$\Omega_0 \leq H_P(S|W, V),$$

where  $P_{SUVW} := P_{S|UV}P_{UV}P_{W|U}$  and  $\Omega_{min} := H_Q(S|U, V)$ .

# An Example: Perfect Privacy

$$\mathcal{S} = \mathcal{U} = \{0, 1, 2, 3\}, \mathcal{V} = \{0, 1\},$$

$$P_{SU} = 0.125 * \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, P_{V|U} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$P_{SUV} = P_{SU}P_{V|U}, Q_{SUV} = P_{SU}P_V.$$

$$H_P(U) = H_Q(U) = H_P(S) = H_Q(S) = 2 \text{ bits.}$$

Hypothesis test:

$$H_0 : (U^n, V^n) \sim \prod_{i=1}^n P_{UV} \quad H_1 : (U^n, V^n) \sim \prod_{i=1}^n P_U P_V.$$

$$W = U \bmod 2 \Rightarrow H_P(S|W, V) = 2 \text{ bits,}$$

$$I_P(U; W) = 1, I_P(V; W) = 1 \text{ bit,}$$

$$\text{i.e., } (1, 1, 2, 1) \in \mathcal{R}_e(0).$$

# Proof: Achievability

## Coding scheme:

- 1 Quantize  $U^n$  to  $\mathcal{C}_w := \{W^n(k), k \in [1 : 2^{nR}]\}$ .  
Encoder  $f^{(n)}$  looks for index  $M$  in the codebook such that  $(U^n, W^n(M))$  is typical.
- 2 Encoder sends index  $M$  if step 1 succeeds, else sends error message  $M = 0$ .
- 3 If  $M \neq 0$  and  $(W^n(M), V^n)$  is typical, detector declares  $H_0$ , else  $H_1$ .

# Analysis of Type 1 and Type 2 error probabilities:

Type 1 error probability:

$\alpha_n \rightarrow 0$  by Covering lemma (if  $R > I_P(U; W)$ ) and Markov Lemma.

Type 2 error exponent (T2EE):

$$\begin{aligned}\beta_n &\leq e^{-n\theta + o(n)}, \\ \theta &:= \min_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}}: \\ P_{\tilde{U}\tilde{W}}=P_{UW}, \\ P_{\tilde{V}\tilde{W}}=P_{VW}}} D(P_{\tilde{U}\tilde{V}\tilde{W}} \| P_{UW} P_V) \\ &\geq \min_{P_{\tilde{V}\tilde{W}}: P_{\tilde{V}\tilde{W}}=P_{VW}} D(P_{\tilde{V}\tilde{W}} \| P_W P_V) := I_P(V; W). \\ \frac{1}{n} H(S^n | M, V^n, H = 0) &\geq \frac{1}{n} H(S^n | W^n(M), V^n, H = 0) \\ &\geq H_P(S | W, V) - o(n) \\ \frac{1}{n} H(S^n | M, V^n, H = 1) &\geq \frac{1}{n} H(S^n | U^n, V^n, H = 1) \\ &\geq H_Q(S | U, V) - o(n)\end{aligned}$$

## Proof: Weak Converse ( $\epsilon \rightarrow 0$ )

Given decision region  $\mathcal{A}_n$  for  $H_0$  such that  $\epsilon_n \rightarrow 0$ ,

$$\begin{aligned} & D(P_{MV^n} \| Q_{MV^n}) \\ & \geq P_{MV^n}(\mathcal{A}_n) \log \left( \frac{P_{MV^n}(\mathcal{A}_n)}{Q_{MV^n}(\mathcal{A}_n)} \right) + P_{MV^n}(\mathcal{A}_n^c) \log \left( \frac{P_{MV^n}(\mathcal{A}_n^c)}{Q_{MV^n}(\mathcal{A}_n^c)} \right) \quad (DPI) \\ & \geq -H(\epsilon_n) - (1 - \epsilon_n) \log(\beta(n, \epsilon_n)) \end{aligned}$$

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{-\log(\beta(n, 0))}{n} & \leq \limsup_{n \rightarrow \infty} \sup_{f(n)} \frac{1}{n} D(P_{MV^n} \| Q_{MV^n}) \\ & = \limsup_{n \rightarrow \infty} \sup_{f(n)} \frac{1}{n} I_P(M; V^n) \quad (\text{since } Q_{MV^n} = P_M P_{V^n}) \\ & = H_P(V) - \liminf_{n \rightarrow \infty} \inf_{f(n)} \frac{1}{n} H_P(V^n | M) \end{aligned}$$



## Proof: Weak Converse ( $\epsilon \rightarrow 0$ )

$$\begin{aligned}\frac{1}{n} H_P(V^n | M) &= \frac{1}{n} \sum_{i=1}^n H_P(V_i | M, V^{i-1}) \\ &= H_P(V_T | W_T, T) \quad (T \sim \text{Unif}[1 : n], W_i = (M, V^{i-1})) \\ &= H_P(V | W) \quad (W = (W_T, T)).\end{aligned}$$

Also,

$$\begin{aligned}nR &\geq H_P(M) \geq I_P(M; U^n) = \sum_{i=1}^n I_P(M, U^{i-1}; U_i) \\ &\geq \sum_{i=1}^n I_P(M, V^{i-1}; U_i) \quad (\text{since } (M, V^{i-1}) - (M, U^{i-1}) - U_i) \\ &= nI_P(W_T, T; U_T) = nI_P(W; U).\end{aligned}$$

## Proof: Converse

$$\begin{aligned}\frac{1}{n}H(S^n|M, V^n, H=0) &= \frac{1}{n}\sum_{i=1}^n H(S_i|M, V^n, S^{i-1}, H=0) \\ &\leq \frac{1}{n}\sum_{i=1}^n H(S_i|M, V^{i-1}, V_i, H=0) \\ &= H(S_T|W_T, V_T, T, H=0) \\ &= H_P(S|W, V).\end{aligned}$$

Note that Markov chain  $V - U - W$  holds.

# Optimal Trade-off: Single-letter characterization

Zero-rate case:

$$\lim_{n \rightarrow \infty} \frac{\log(|\mathcal{M}|)}{n} = 0.$$

Motivated by low bandwidth and low power applications like IoT and sensor networks.

$$H_0 : (U^n, V^n) \sim \prod_{i=1}^n P_{UV}, \quad H_1 : (U^n, V^n) \sim \prod_{i=1}^n Q_{UV}$$

## Proposition

For  $\epsilon \in (0, 1)$ ,  $(0, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$  iff

$$\kappa \leq \min_{P_{\tilde{U}\tilde{V}} \in \mathcal{T}_1(P_U, P_V)} D(P_{\tilde{U}\tilde{V}} \| Q_{UV}),$$

$$\Omega_0 \leq H_P(S|V),$$

$$\Omega_1 \leq H_Q(S|V),$$

where  $\mathcal{T}_1(P_U, P_V) := \{P_{\tilde{U}\tilde{V}} \in \mathcal{T}(\mathcal{U} \times \mathcal{V}) : P_{\tilde{U}} = P_U, P_{\tilde{V}} = P_V\}$ .

# Coding scheme: Achievability

- 1 Encoder sends  $M = 1$  if  $U^n$  is typical, else it sends  $M = 0$ .
- 2 If  $M = 1$  and  $V^n$  is typical, detector declares  $H_0$ , else  $H_1$ .

Type 1 error probability:

$\alpha_n \rightarrow 0$  by Weak law of large numbers.

Type 2 error exponent:

$$\beta_n \leq e^{-n\theta_0 + o(n)},$$
$$\theta_0 := \min_{\substack{P_{\tilde{U}\tilde{V}}: \\ P_{\tilde{U}}=P_U, \\ P_{\tilde{V}}=P_V}} D(P_{\tilde{U}\tilde{V}} \| Q_{UV}).$$

## Proof:

$$\lim_{n \rightarrow \infty} \frac{\log(|\mathcal{M}|)}{n} = 0 \Rightarrow \lim_{n \rightarrow \infty} \frac{1}{n} H_P(M) = 0.$$

$$\begin{aligned} \frac{1}{n} H(S^n | M, V^n, H = H_i) &\geq \frac{1}{n} H(S^n | V^n, H = H_i) - \frac{1}{n} H(M) \\ &\geq H(S | V, H = H_i) - \gamma_n, \end{aligned}$$

## Converse:

$$\frac{1}{n} H(S^n | M, V^n, H = H_i) \leq \frac{1}{n} H(S^n | V^n, H = H_i) = H(S | V, H = H_i).$$

Converse follows from existing results on distributed HT without privacy constraint.

# General result: Single letter Inner bound

## Theorem

For  $\epsilon \in (0, 1)$ ,  $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$  if  $\exists$  an auxiliary r.v.  $W$  such that  $(V, S) - U - W$  and

$$R \geq I_P(W; U|V),$$

$$\kappa \leq \kappa^*(P_{W|U}, R),$$

$$\Omega_0 \leq H_P(S|W, V),$$

$$\Omega_1 \leq \mathbb{1}(P_U = Q_U) H_{Q'}(S|W, V) + \mathbb{1}(P_U \neq Q_U) H_Q(S|V),$$

where  $\kappa^*(P_{W|U}, R) = \min(E_1(P_{W|U}), E_2(R, P_{W|U}))$ ,

$$P_{SUVW} = P_{SUV}P_{W|U}, \quad Q_{SUVW} = Q_{SUV}P_{W|U}, \quad Q'_{SUVW} = Q_{SV|U}P_U P_{W|U}.$$

## Remarks about Inner bound :

- Tight for Testing Against Independence and Zero-rate case.
- Compression rate is reduced using binning at the encoder and using  $V^n$  as side-information.
- Extra factor  $E_2(R, P_{W|U})$  in T2EE (due to binning).
- Privacy achieved under alternate hypothesis depends on whether  $P_U = Q_U$  or  $P_U \neq Q_U$ .

# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint
- 3 Equivocation as a Privacy measure
- 4 Average distortion as a Privacy measure**
- 5 Concluding Remarks and Open problems



# Average distortion as a Privacy measure

Average distortion:

$$\mathbb{E} \left( d(S^n, \hat{S}^n) \right),$$
$$d(s^n, \hat{s}^n) := \frac{1}{n} \sum_{i=1}^n d(s_i, \hat{s}_i)$$

An additive measure as opposed to equivocation.

Information-theoretic security:

Rate distortion problem for communication system with a secondary decoder to be hindered- Yamamoto [1989].

Rate-distortion theory of secrecy systems- Schieler and Cuff [2014].

# Rate- Error Exponent-Distortion Trade-off

## Definition

$\mathcal{R}_d(\epsilon)$  : Closure of the set of all  $(R, \kappa, \Delta_0, \Delta_1)$  tuples such that

$$\begin{aligned} \exists f^{(n)} : \mathcal{U}^n &\rightarrow \{P_{M|U^n}\}, \mathcal{M} = [e^{nR}], \\ g^{(n)} : [e^{nR}] \times \mathcal{V}^n &\rightarrow \{P_{\hat{H}|M, V^n}\} \end{aligned}$$

such that

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{\log(\beta(f^{(n)}, g^{(n)}))}{n} &\leq -\kappa, \alpha(f^{(n)}, g^{(n)}) \leq \epsilon, \\ \liminf_{n \rightarrow \infty} \inf_{g_r^{(n)}} \mathbb{E} \left[ d(S^n, \hat{S}^n) \mid H = H_i \right] &\geq \Delta_i, \quad i = 0, 1. \end{aligned}$$

where  $g_r^{(n)} : [e^{nR}] \times \mathcal{V}^n \rightarrow \{P_{\hat{S}^n|M, V^n}\}$  and  $P_{\hat{S}^n|M, V^n}$  denotes an arbitrary conditional probability distribution.

# Optimal Trade-off: Single-letter characterization

Testing Against Independence:

$$P_{SUV} = P_{S|UV}P_{UV}, \quad Q_{SUV} = Q_{S|UV}P_U P_V.$$

## Theorem

$(R, \kappa, \Delta_0, \Delta_{min}) \in \mathcal{R}_d(0)$  iff  $\exists$  an auxiliary r.v.  $W$  such that

$$\begin{aligned} R &\geq I_P(W; U), \\ \kappa &\leq I_P(W; V), \\ \Delta_0 &\leq \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_P [d(S, \phi(W, V))], \end{aligned}$$

for some deterministic function  $\phi : \mathcal{W} \times \mathcal{V} \rightarrow \hat{\mathcal{S}}$ ,  
 $P_{SUVW} := P_{S|UV}P_{UV}P_{W|U}$  and  $\Delta_{min} := \min_{\phi} \mathbb{E}_Q [d(S, \phi(U, V))].$

# Coding scheme: Achievability

- Channel Resolvability [Han-Verdu] or Soft-covering Lemma [Cuff]

## Lemma

Given a joint distribution  $P_{UW}$ , let  $\mathcal{C}_W^n$  be a random codebook of sequences  $W^n(m)$ ,  $m \in [1 : 2^{nR}]$  each drawn independently according to  $\prod_{i=1}^n P_W$ . Let

$$P_{MU^n}(m, u^n) \triangleq \frac{1}{2^{nR}} \prod_{i=1}^n P_{U|W}(u_i | W_i(m)).$$

If  $R > I(U; W)$ , then,

$$\mathbb{E} \left[ \left\| P_{U^n} - \prod_{i=1}^n P_U \right\| \right] \xrightarrow{(n)} 0$$

# Achievability:

- 1 Choose codebook  $\mathcal{C}_w = \{w^n(k), k \in [1 : 2^{nR}]\}$  satisfying Soft-covering lemma.
- 2 Stochastic encoding: If  $U^n$  is typical, encoder chooses  $M = m$  with probability

$$P_{E_u}(m|U^n, \mathcal{C}_u^n) \triangleq \frac{\prod_{i=1}^n P_{U|W}(u_i|w_i(m))}{\sum_{m'} \prod_{i=1}^n P_{U|W}(u_i|w_i(m'))},$$

else sends  $M = 0$ .

- 3 If  $M \neq 0$  and  $(W^n(M), V^n)$  is typical, detector declares  $H_0$ , else  $H_1$ .

## Converse:

$$\begin{aligned} & \min_{g_r^{(n)}} \mathbb{E} \left[ d \left( S^n, \hat{S}^n \right) \mid H = H_0 \right] \\ &= \min_{\{\phi(m, v^n, i)\}} \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^n d \left( S_i, \phi(M, V^n, i) \right) \mid H = H_0 \right] \\ &= \min_{\{\phi(\cdot, \cdot, \cdot)\}} \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^n d \left( S_i, \phi(W_i, V_i, V_{i+1}^n, i) \right) \mid H = H_0 \right] \\ &\leq \min_{\{\phi(w_i, v_i, i)\}} \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^n d \left( S_i, \phi(W_i, V_i, i) \right) \mid H = H_0 \right] \\ &= \min_{\{\phi(\cdot, \cdot, \cdot)\}} \mathbb{E} \left[ d \left( S_T, \phi(W_T, V_T, T) \right) \mid H = H_0 \right] \\ &= \min_{\{\phi(w, v)\}} \mathbb{E}_P \left[ d \left( S, \phi(W, V) \right) \right]. \end{aligned}$$

# Optimal Trade-off: Single-letter characterization

Zero-rate case:

## Theorem

For  $\epsilon \in (0, 1)$ ,  $(0, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$  iff,

$$\kappa \leq \min_{P_{\tilde{U}\tilde{V}} \in \mathcal{T}_1(P_U, P_V)} D(P_{\tilde{U}\tilde{V}} \| Q_{UV}),$$

$$\Delta_0 \leq \min_{\phi'(\cdot)} \mathbb{E}_P [d(S, \phi'(V))],$$

$$\Delta_1 \leq \min_{\phi'(\cdot)} \mathbb{E}_Q [d(S, \phi'(V))],$$

where,  $\phi' : \mathcal{V} \rightarrow \hat{\mathcal{S}}$  is a deterministic function and

$$\mathcal{T}_1(P_U, P_V) = \{P_{\tilde{U}\tilde{V}} \in \mathcal{T}(\mathcal{U} \times \mathcal{V}) : P_{\tilde{U}} = P_U, P_{\tilde{V}} = P_V\}.$$

# Coding scheme: Achievability

## Lemma

Let  $P_{XY}$  and  $Q_{XY}$  denote two probability distributions on r.v.'s  $X$  and  $Y$ . Let  $P_{X^n Y^n} = \prod_{i=1}^n P_{XY}$  and  $Q_{X^n Y^n} = \prod_{i=1}^n Q_{XY}$ . For  $\delta > 0$ , define

$$I_X(x^n, \delta) \triangleq \mathbb{1} \left( x^n \notin T_{[P_X]_\delta}^n \right).$$

If  $P_X \neq Q_X$ , then for  $\delta > 0$  sufficiently small,

$$\|Q_{Y^n} - Q_{Y^n|I_X(X^n, \delta)=1}\| \xrightarrow{(n)} 0,$$

If  $P_X = Q_X$ , then the following holds for any  $\delta > 0$ ,

$$\|Q_{Y^n} - Q_{Y^n|I_X(X^n, \delta)=0}\| \xrightarrow{(n)} 0,$$

$$\|P_{Y^n} - P_{Y^n|I_X(X^n, \delta)=0}\| \xrightarrow{(n)} 0.$$



# Coding scheme: Converse

$$\begin{aligned} & \min_{g_r^{(n)}} \mathbb{E} \left[ d \left( S^n, \hat{S}^n \right) \mid H = H_0 \right] \\ & \leq \min_{\{\phi'_i(v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{P_{S^n V^n}} \left[ d \left( S_i, \phi'_i(V^n) \right) \right] \quad (\text{neglect } M) \\ & = \min_{\{\phi'(v)\}} \mathbb{E}_P \left[ d(S, \phi'(V)) \right]. \end{aligned}$$

# General result: Single letter Inner bound

## Theorem

For  $\epsilon \in (0, 1)$ ,  $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$  if  $\exists W, (V, S) - U - W$ ,

$$R \geq I_P(W; U|V),$$

$$\kappa \leq \kappa^*(P_{W|U}, R),$$

$$\Delta_0 \leq \min_{\phi(\cdot, \cdot)} \mathbb{E}_P [d(S, \phi(W, V))],$$

$$\begin{aligned} \Delta_1 \leq & \mathbb{1}(P_U = Q_U) \min_{\phi(\cdot, \cdot)} \mathbb{E}_{Q'} [d(S, \phi(W, V))] \\ & + \mathbb{1}(P_U \neq Q_U) \min_{\phi'(\cdot)} \mathbb{E}_Q [d(S, \phi'(V))], \end{aligned}$$

$$P_{SUVW} = P_{SUV}P_{W|U}, \quad Q_{SUVW} = Q_{SUV}P_{W|U}, \quad Q'_{SUVW} = Q_{SV|U}P_U P_{W|U}.$$

# Outline

- 1 Introduction
- 2 Distributed Hypothesis Testing With a Privacy Constraint
- 3 Equivocation as a Privacy measure
- 4 Average distortion as a Privacy measure
- 5 Concluding Remarks and Open problems**

# Concluding Remarks and Open Problems

- Distributed HT under a privacy constraint studied with equivocation and average distortion as privacy measures.
- Admits single-letter characterization for special cases.
- Open problems

Single-letter outer bound for rate-error exponent-privacy trade-off in the general HT case ?

Strong Converse holds?

Generalization to more general data sets ?

Exact distributions under the null and alternate hypothesis unknown- tools in machine learning tools applicable ?

# Concluding Remarks and Open Problems

- Distributed HT under a privacy constraint studied with equivocation and average distortion as privacy measures.
- Admits single-letter characterization for special cases.
- Open problems

Single-letter outer bound for rate-error exponent-privacy trade-off in the general HT case ?

Strong Converse holds?

Generalization to more general data sets ?

Exact distributions under the null and alternate hypothesis unknown- tools in machine learning tools applicable ?

# References

- 1 R. Ahlswede and I. Csiszar- Hypothesis testing with communication constraints, IEEE Trans. Inf. Theory, vol. 32, no. 4, pp. 533-542, Jul. 1986.
- 2 T. S. Han, Hypothesis testing with multiterminal data compression, IEEE Trans. Inf. Theory, vol. 33, no. 6, pp. 759-792, Nov. 1987.
- 3 J. Liao, L. Sankar, V. Tan, and F. Calmon, Hypothesis testing under mutual information privacy constraints in the high privacy regime, IEEE Trans.on Inf. Forensics and Security, vol. 13, no. 4, pp. 1058-1071, Apr. 2018.
- 4 A. Gilani, S. B. Amor, S. Salehkalaibar, and V. Y. F. Tan, Distributed hypothesis testing with privacy constraints, arXiv:1806.02015

THANK YOU!