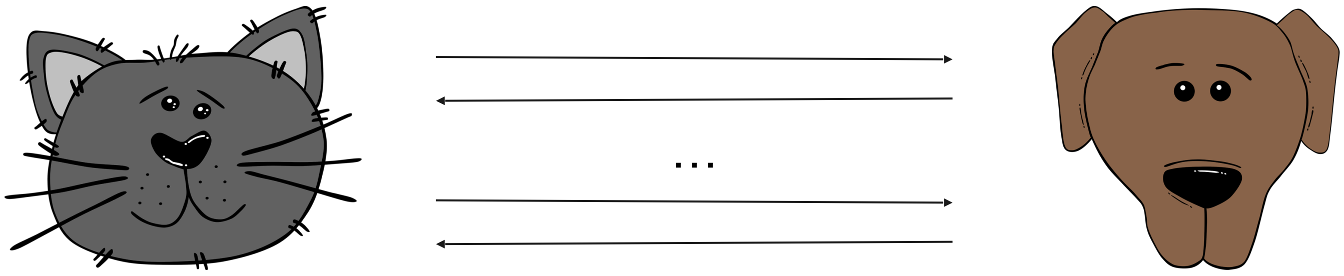
http://eprint.iacr.org/2022/660

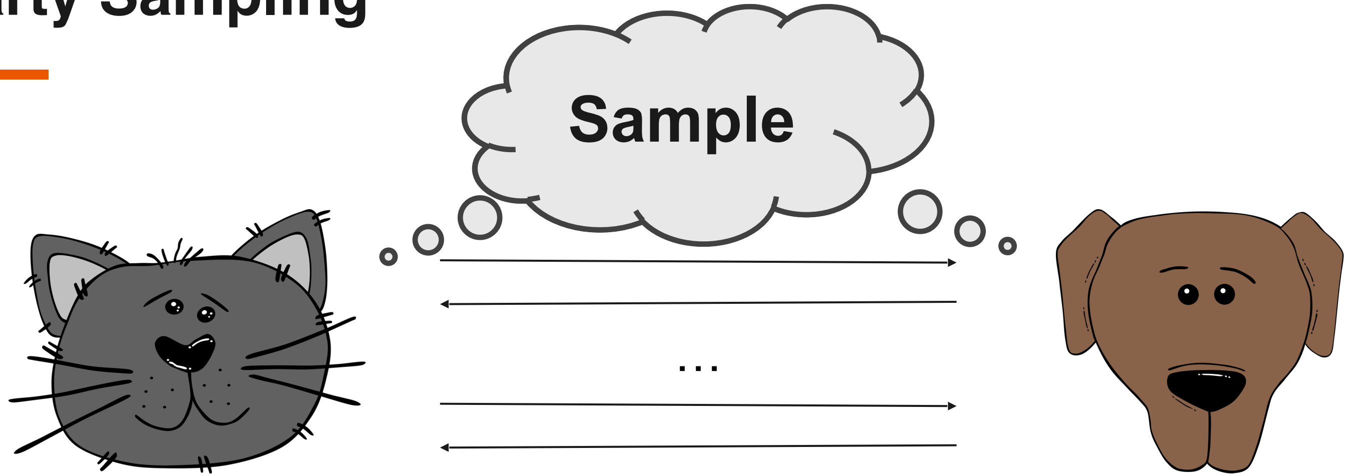
Secure Sampling with Sublinear Communication

Seung Geol Choi (US Naval Academy)
Dana Dachman-Soled (University of Maryland)
S. Dov Gordon (George Mason University)
Linsheng Liu (George Washington University)
Arkady Yerukhimovich (George Washington University)

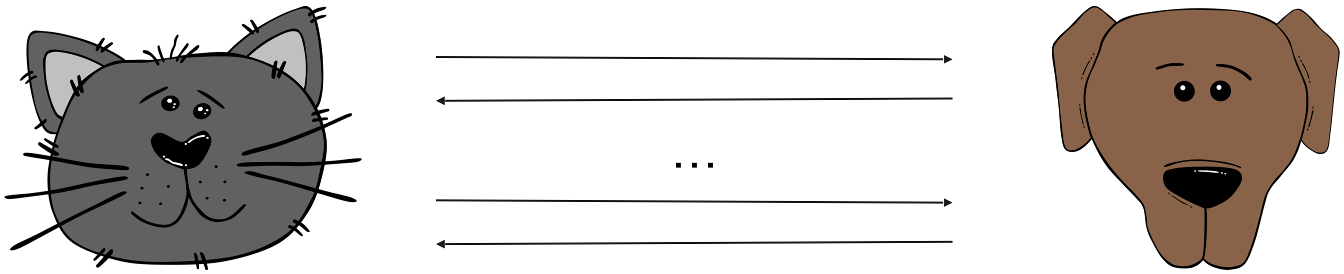
2-Party Sampling



2-Party Sampling

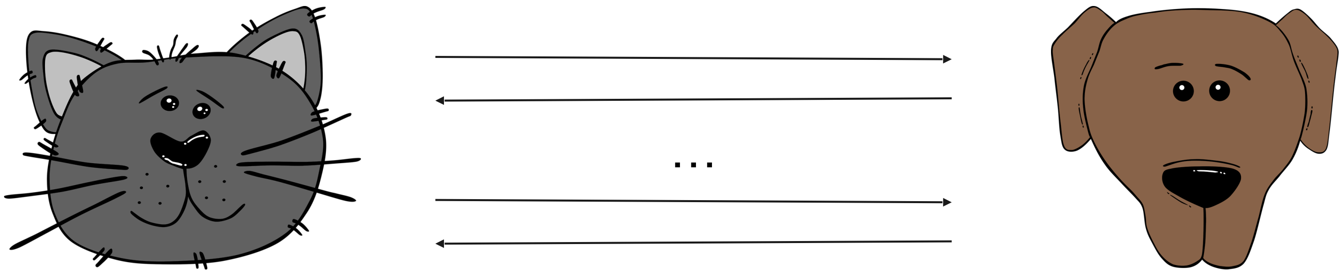


2-Party Sampling



2-Party Sampling

$W_1 = (w_{1,1}, w_{1,2}, ..., w_{1,n})$ $W_2 = (w_{2,1}, w_{2,2}, ..., w_{2,n})$



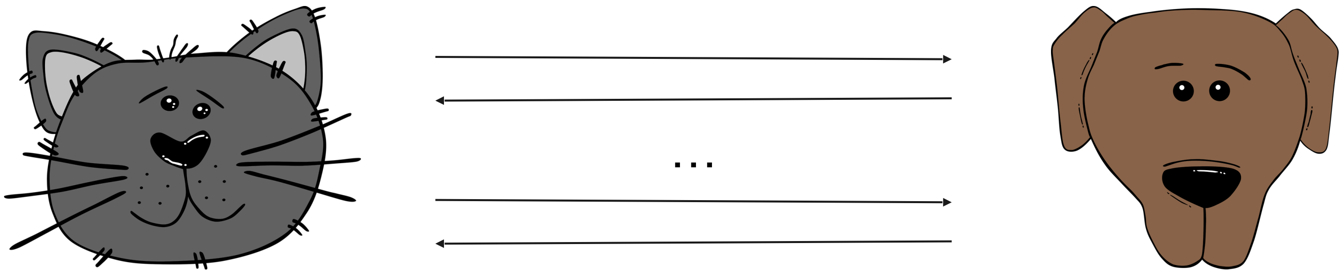
Private sampling based on W_1 and W_2

- Output i with $\Pr[i] \propto f(w_{1,i}, w_{2,i})$
- L_1 sampling; L_2 sampling; Product sampling

Distribution is private

2-Party Sampling

$W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n})$ $W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$



Private sampling based on W_1 and W_2

- Output i with $\Pr[i] \propto f(w_{1,i}, w_{2,i})$
- L_1 sampling; L_2 sampling; Product sampling

Distribution is private

Question: Sample with sublinear communication?

Our results

- **Private sampling:**
  - L_1 sampling with sublinear communication
  - L_2 sampling with sublinear communication
- **Product sampling:**
  - Impossibility for arbitrary inputs
  - Sublinear communication with assumption on inputs

$$\langle \mathbf{W}_1, \mathbf{W}_2 \rangle \in \omega(\frac{\log n}{n})$$

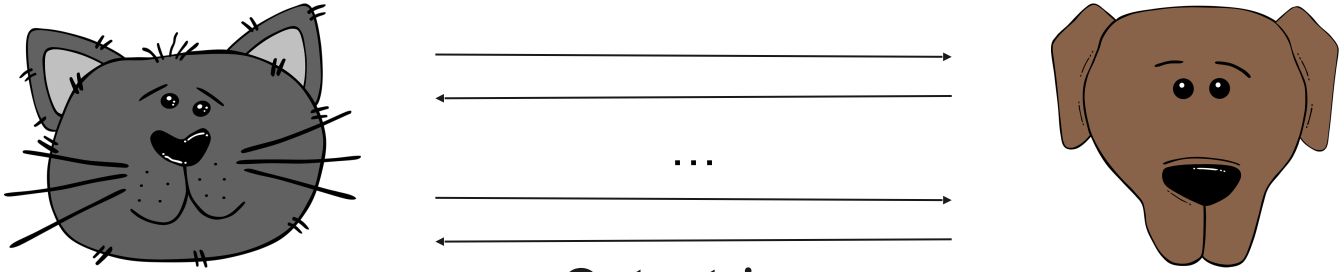
- **Exponential Mechanism**
  - 2-party Exponential Mechanism with sublinear communication

Outline

- Sublinear sampling
- Sampling from common distributions
  - L_1 sampling
  - L_2 sampling
  - Product sampling
- Exponential Mechanism

L_1 Sampling

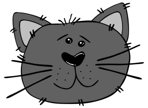
$$W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \qquad W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$$

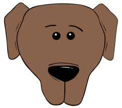


Output i

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\sum_j (w_{1,j} + w_{2,j})} = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1}$$

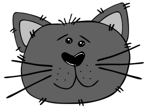
L_1 Sampling

 $W_1 = (w_{1,1}, w_{1,2}, ..., w_{1,n})$

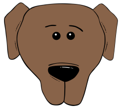
 $W_2 = (w_{2,1}, w_{2,2}, ..., w_{2,n})$

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto w_{1,i} + w_{2,i}$$

L_1 Sampling



$$W_1 = (w_{1,1}, w_{1,2}, \dots, w_{1,n})$$

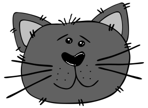


$$W_2 = (w_{2,1}, w_{2,2}, \dots, w_{2,n})$$

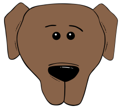
- **L_1 is linear!**

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto w_{1,i} + w_{2,i}$$

L_1 Sampling



$$W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n})$$

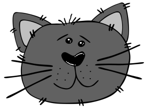


$$W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$$

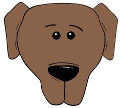
- **L_1 is linear!**

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto \boxed{w_{1,i}} + \boxed{w_{2,i}}$$

L_1 Sampling



$W_1 = (w_{1,1}, w_{1,2}, ..., w_{1,n})$

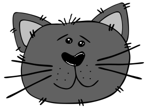


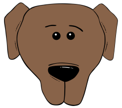
$W_2 = (w_{2,1}, w_{2,2}, ..., w_{2,n})$

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto \boxed{w_{1,i}} + \boxed{w_{2,i}}$$

- **L_1 is linear!**
- **First attempt:**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

L_1 Sampling

 $W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n})$

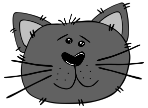
 $W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto \boxed{w_{1,i}} + \boxed{w_{2,i}}$$

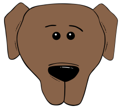
- **L_1 is linear!**
- **First attempt:**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

😄 **O(1) communication!**

L_1 Sampling



$W_1 = (w_{1,1}, w_{1,2}, \dots, w_{1,n})$



$W_2 = (w_{2,1}, w_{2,2}, \dots, w_{2,n})$

$$\Pr[i] = \frac{w_{1,i} + w_{2,i}}{\|W_1 + W_2\|_1} \propto \boxed{w_{1,i}} + \boxed{w_{2,i}}$$

- **L_1 is linear!**
- **First attempt:**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

😄 **O(1) communication!**

😔 **This is not private!**

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.
- **Fix for privacy**

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.
- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.
- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.
  3. Reconstruct i_1 or i_2 based on a oblivious coin flip.

L$_1$ Sampling — Fi

Party 1 doesn't know i_1

Party 2 doesn't know i_2

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.
  3. Reconstruct i_1 or i_2 based on a oblivious coin flip.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.
- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.
  3. Reconstruct i_1 or i_2 based on a oblivious coin flip.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

😄 **O(1) communication!**

- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.
  3. Reconstruct i_1 or i_2 based on a oblivious coin flip.

L_1 Sampling — Fix privacy issue

- **Initial attempt**
  1. Party 1 samples i_1 locally.
  2. Party 2 samples i_2 locally.
  3. Flip a coin and output i_1 or i_2.

😄 **O(1) communication!**

- **Fix for privacy**
  1. The parties obliviously sample and secret share i_1.
  2. The parties obliviously sample and secret share i_2.
  3. Reconstruct i_1 or i_2 based on a oblivious coin flip.

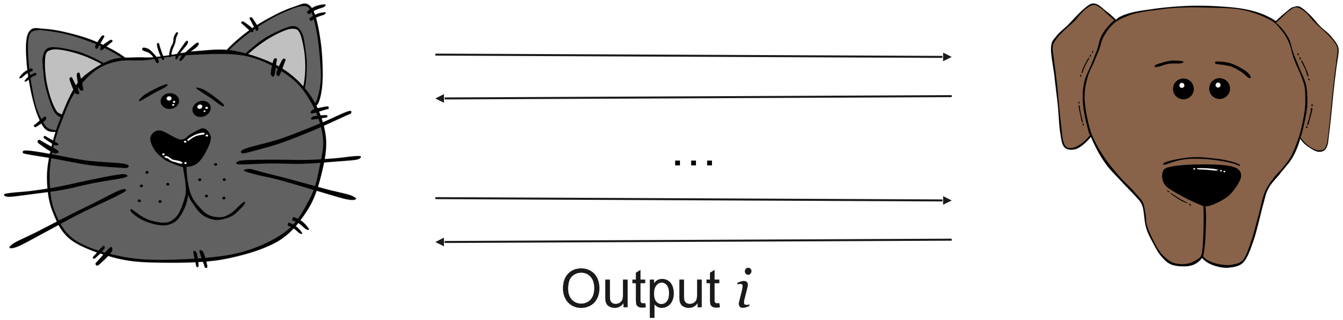
😄 **This is private!**

Outline

- Sublinear sampling
- Sampling from common distributions
    - L_1 sampling
    - L_2 sampling
    - Product sampling
- Exponential Mechanism

L_2 Sampling

$$W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \qquad W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$$



$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\sum_j (w_{1,j} + w_{2,j})^2} = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Why is L_2 Sampling hard?

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 + 2w_{1,i} \cdot w_{2,i}}{\|W_1\|_2^2 + \|W_2\|_2^2 + 2\sum_j (w_{1,j} \cdot w_{2,j})}$$

Why is L_2 Sampling hard?

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 + 2w_{1,i} \cdot w_{2,i}}{\|W_1\|_2^2 + \|W_2\|_2^2 + 2\sum_j (w_{1,j} \cdot w_{2,j})}$$

- **Apply the linearity trick like L_1?**

Why is L_2 Sampling hard?

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 + \boxed{2w_{1,i} \cdot w_{2,i}}}{\|W_1\|_2^2 + \|W_2\|_2^2 + \boxed{2\sum_j (w_{1,j} \cdot w_{2,j})}}$$

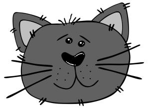
- **Apply the linearity trick like L_1?**

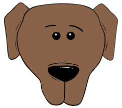
Why is L_2 Sampling hard?

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 + 2w_{1,i} \cdot w_{2,i}}{\|W_1\|_2^2 + \|W_2\|_2^2 + 2\sum_j (w_{1,j} \cdot w_{2,j})}$$

- **Apply the linearity trick like L_1?**
  - No longer linear
  - Cross terms. (Inner product)
  - Impossible to compute with sublinear communication

New trick

 $W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n})$

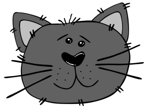
 $W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$

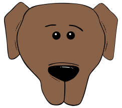
- **Corrective sampling**

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 + 2w_{1,i} \cdot w_{2,i}}{\|W_1\|_2^2 + \|W_2\|_2^2 + 2\sum_j (w_{1,j} \cdot w_{2,j})}$$

Goal: Output i with Pr[L_2 = i]

New trick

 $W_1 = (w_{1,1}, w_{1,2}, ..., w_{1,n})$

 $W_2 = (w_{2,1}, w_{2,2}, ..., w_{2,n})$

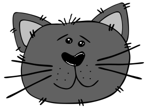
- **Corrective sampling**

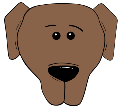
$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 \cancel{+ 2w_{1,i} \cdot w_{2,i}}}{\|W_1\|_2^2 + \|W_2\|_2^2 \cancel{+ 2\sum_j (w_{1,j} \cdot w_{2,j})}}$$

Goal: Output *i* with Pr[L_2 = *i*]

  - Sample from a related distribution — "Drop the cross terms"

New trick

 $W_1 = (w_{1,1}, w_{1,2}, ..., w_{1,n})$

 $W_2 = (w_{2,1}, w_{2,2}, ..., w_{2,n})$

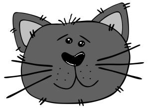
- **Corrective sampling**

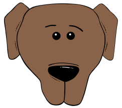
$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 \cancel{+ 2w_{1,i} \cdot w_{2,i}}}{\|W_1\|_2^2 + \|W_2\|_2^2 \cancel{+ 2\sum_j (w_{1,j} \cdot w_{2,j})}}$$

Goal: Output i with $\Pr[L_2 = i]$

  - Sample from a related distribution — "Drop the cross terms"
  - Correct it by "rejection sampling"
    - Output i with some probability p_i

New trick

 $W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n})$

 $W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$

- **Corrective sampling**

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 \cancel{+ 2w_{1,i} \cdot w_{2,i}}}{\|W_1\|_2^2 + \|W_2\|_2^2 \cancel{+ 2\sum_j (w_{1,j} \cdot w_{2,j})}}$$

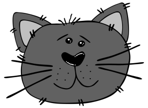
Goal: Output i with Pr[L$_2$ = i]

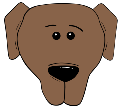
- Sample from a related distribution — "Drop the cross terms"

Avoid computing "Inner Product"

- Correct it by "rejection sampling"
  - Output i with some probability p_i

New trick

 $W_1 = (w_{1,1}, w_{1,2}, \dots, w_{1,n})$

 $W_2 = (w_{2,1}, w_{2,2}, \dots, w_{2,n})$

- **Corrective sampling**

$$\Pr[i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2} = \frac{w_{1,i}^2 + w_{2,i}^2 \cancel{+ 2w_{1,i} \cdot w_{2,i}}}{\|W_1\|_2^2 + \|W_2\|_2^2 \cancel{+ 2\sum_j (w_{1,j} \cdot w_{2,j})}}$$

Goal: Output i with Pr[$L_2 = i$]

- Sample from a related distribution — “Drop the cross terms”

Avoid computing “Inner Product”

- Correct it by “rejection sampling”
  - Output i with some probability p_i

Depends only on $w_{1,i}$ and $w_{2,i}$

Our protocol

Our protocol

- **The simple distribution A**

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Our protocol

- **The simple distribution A**

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Simply using our L1 sampling

$$V_1 = (w_{1,1}^2, w_{1,2}^2, \ldots, w_{1,n}^2)$$
$$V_2 = (w_{2,1}^2, w_{2,2}^2, \ldots, w_{2,n}^2)$$

Our protocol

- **The simple distribution A**

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Simply using our L1 sampling

$$V_1 = (w_{1,1}^2, w_{1,2}^2, \ldots, w_{1,n}^2)$$
$$V_2 = (w_{2,1}^2, w_{2,2}^2, \ldots, w_{2,n}^2)$$

- **Acceptance probability p_i**

Goal for acceptance rate: $\dfrac{\Pr[L_2 = i]}{\Pr[A = i]}$

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2} \cdot \frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}$$

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}$$

- Only depend on w_i
- easy to compute

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \boxed{\frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}}$$

Hard to compute

- Only depend on w_i
- easy to compute

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \boxed{\frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}}$$

- Only depend on w_i
- easy to compute

Hard to compute

Constant

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \boxed{\frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}}$$

Hard to compute

Constant

- Only depend on w_i
- easy to compute

p_i

Computing p_i

Correctness

O(1) communication

$\Downarrow$

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \boxed{\frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}}$$

- Only depend on w_i
- easy to compute

p_i

Hard to compute

Constant

Computing p_i

Correctness

L_2 distribution

$$\Pr[L_2 = i] = \frac{(w_{1,i} + w_{2,i})^2}{\|W_1 + W_2\|_2^2}$$

O(1) communication

$\Downarrow$

Easy distribution A

$$\Pr[A = i] = \frac{w_{1,i}^2 + w_{2,i}^2}{\|W_1\|_2^2 + \|W_2\|_2^2}$$

Probability for i being accepted

$$\frac{\Pr[L_2 = i]}{\Pr[A = i]} = \boxed{\frac{(w_{1,i} + w_{2,i})^2}{w_{1,i}^2 + w_{2,i}^2}} \cdot \boxed{\frac{\|W_1\|_2^2 + \|W_2\|_2^2}{\|W_1 + W_2\|_2^2}}$$

Hard to compute

Constant

- Only depend on w_i
- easy to compute

p_i

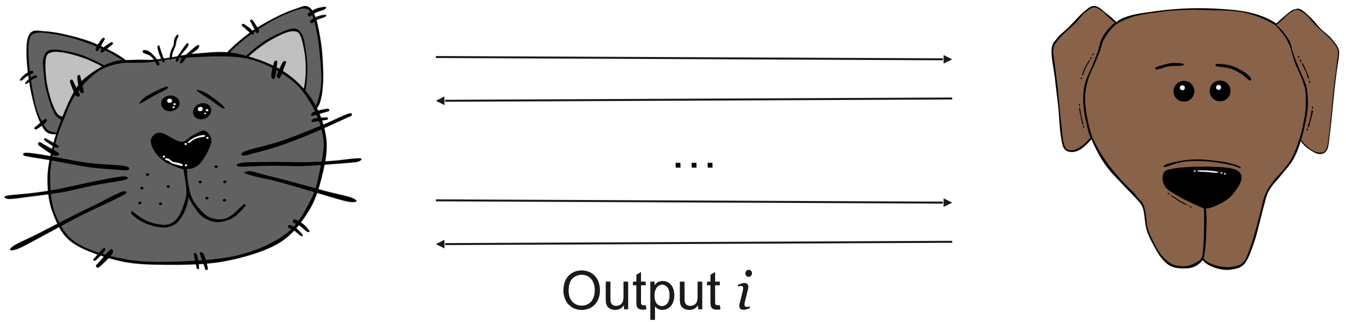
Expected constant round

Outline

- Sublinear sampling
- Sampling from common distributions
  - L_1 sampling
  - L_2 sampling
  - Product sampling
- Exponential Mechanism

Product Sampling

$$W_1 = (w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \qquad W_2 = (w_{2,1}, w_{2,2}, \ldots, w_{2,n})$$



$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle}$$

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto w_{1,i} \cdot w_{2,i}$$

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

1. The parties obliviously sample and secret share i_1.
2. The parties obliviously sample and secret share i_2.
3. Equality check:
   a. if $i_1 = i_2$, output i_1
   b. else $i_1 \neq i_2$, go to 1

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

1. The parties obliviously sample and secret share i_1.
2. The parties obliviously sample and secret share i_2.
3. Equality check:
   a. if $i_1 = i_2$, output i_1
   b. else $i_1 \neq i_2$, go to 1

Expected # of iterations:

$$\frac{1}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle}$$

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

1. The parties obliviously sample and secret share i_1.
2. The parties obliviously sample and secret share i_2.
3. Equality check:
   a. if $i_1 = i_2$, output i_1
   b. else $i_1 \neq i_2$, go to 1

Expected # of iterations:

$$\frac{1}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle}$$

- **Need sufficiently large inner product** $\langle \mathbf{W}_1, \mathbf{W}_2 \rangle = \omega(\frac{\log n}{n})$

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

1. The parties obliviously sample and secret share i_1.
2. The parties obliviously sample and secret share i_2.
3. Equality check:
   a. if $i_1 = i_2$, output i_1
   b. else $i_1 \neq i_2$, go to 1

Expected # of iterations:

$$\frac{1}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle}$$

- **Need sufficiently large inner product** $\langle \mathbf{W}_1, \mathbf{W}_2 \rangle = \omega(\frac{\log n}{n})$
- **Leakage: (at most) inner product**

Product Sampling

$$\Pr[i] = \frac{w_{1,i} \cdot w_{2,i}}{\sum_j w_{1,j} \cdot w_{2,j}} = \frac{w_{1,i} \cdot w_{2,i}}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle} \propto w_{1,i} \cdot w_{2,i}$$

$$\Pr[i] \propto \boxed{w_{1,i}} \cdot \boxed{w_{2,i}}$$

1. The parties obliviously sample and secret share i_1.
2. The parties obliviously sample and secret share i_2.
3. Equality check:
   a. if $i_1 = i_2$, output i_1
   b. else $i_1 \neq i_2$, go to 1

Expected # of iterations:

$$\frac{1}{\langle \mathbf{W_1}, \mathbf{W_2} \rangle}$$

- **Need sufficiently large inner product** $\langle \mathbf{W}_1, \mathbf{W}_2 \rangle = \omega(\frac{\log n}{n})$
- **Leakage: (at most) inner product**
- **Impossible for sublinear communication**
  - Reduction from Set Disjointness Problem

Requires at least linear communication[R92]

Outline

- Sublinear sampling
- Sampling from common distributions
  - L_1 sampling
  - L_2 sampling
  - Product sampling
- Exponential Mechanism

Exponential Mechanism for Differential Privacy

- **Exponential Mechanism (simplified)**
  - A list of items h_i
  - Goal: output h_i with probability $\propto e^{s(h_i)}$

Exponential Mechanism for Differential Privacy

- **Exponential Mechanism (simplified)**
  - A list of items h_i
  - Goal: output h_i with probability $\propto e^{s(h_i)}$
- **2 party sublinear Exponential Mechanism**
  - Additive score function $s(h_i) = s_1(h_i) + s_2(h_i)$
  - Party j computes $s_j(h_i)$ privately
  - Goal: output h_i with probability

$$\propto e^{s(h_i)} = e^{s_1(h_i)+s_2(h_i)} = e^{s_1(h_i)} \cdot e^{s_2(h_i)}$$

Exponential Mechanism for Differential Privacy

- **Exponential Mechanism (simplified)**
  - A list of items h_i
  - Goal: output h_i with probability $\propto e^{s(h_i)}$
- **2 party sublinear Exponential Mechanism**
  - Additive score function $s(h_i) = s_1(h_i) + s_2(h_i)$
  - Party j computes $s_j(h_i)$ privately
  - Goal: output h_i with probability

$$\propto e^{s(h_i)} = e^{s_1(h_i)+s_2(h_i)} = \boxed{e^{s_1(h_i)}} \cdot \boxed{e^{s_2(h_i)}}$$

Exponential Mechanism for Differential Privacy

- **Exponential Mechanism (simplified)**
  - A list of items h_i
  - Goal: output h_i with probability $\propto e^{s(h_i)}$
- **2 party sublinear Exponential Mechanism**
  - Additive score function $s(h_i) = s_1(h_i) + s_2(h_i)$
  - Party j computes $s_j(h_i)$ privately
  - Goal: output h_i with probability $\propto e^{s(h_i)} = e^{s_1(h_i)+s_2(h_i)} = \boxed{e^{s_1(h_i)}} \cdot \boxed{e^{s_2(h_i)}}$

Product Sampling!

Exponential Mechanism for Differential Privacy

- **Exponential Mechanism (simplified)**
  - A list of items h_i
  - Goal: output h_i with probability $\propto e^{s(h_i)}$
- **2 party sublinear Exponential Mechanism**
  - Additive score function $s(h_i) = s_1(h_i) + s_2(h_i)$
  - Party j computes $s_j(h_i)$ privately
  - Goal: output h_i with probability $\propto e^{s(h_i)} = e^{s_1(h_i)+s_2(h_i)} = \boxed{e^{s_1(h_i)}} \cdot \boxed{e^{s_2(h_i)}}$

Product Sampling!

- **We have a problem — leaking inner product is not DP!**

✓ Solution: estimate Inner Product by DP version of Johnson-Lindenstrauss Transform[JL84, IM98]

Conclusion

- **Introduce a new problem of distributed sublinear sampling**
- **Achieve**
  - 2-party L_1, L_2, $L_p$sublinear sampling
  - Impossibility of sublinear product sampling in general
  - Sublinear product sampling protocol
    - for inputs w/ sufficient large inner product
  - 2-party exponential mechanism for differential privacy

Thank You!

http://eprint.iacr.org/2022/660

Thanks!

http://eprint.iacr.org/2022/660