Università degli Studi di Padova

DIFFERENTIAL PRIVACY: PART II

PRIVACY PRESERVING INFORMATION ACCESS

PhD in Information Engineering

A.Y. 2025/2026

GUGLIELMO FAGGIOLI
Intelligent Interactive Information Access (IIIA) Hub
Department of Information Engineering
University of Padua

Dipartimento di Ingegneria dell'Informazione

RANDOMIZED RESPONSE

We already know a differentially private algorithm: the randomized response or coin toss.

Flip a coin:

if “tail”, respond truthfully

if “head”, flip coin again:

if “tail”, respond “YES”

if “head”, respond “NO”

RANDOMIZED RESPONSE

We are also able to compute its privacy loss:

$$\frac{\Pr_x(Y)}{\Pr_y(Y)} = \frac{\Pr[R = Y \mid T = Y]}{\Pr[R = Y \mid T = N]} = \frac{3/4}{1/4} = 3$$

And thus we say that the randomized response is a (ln 3 - 0) differentially private algorithm.

We can do better than this...

ℓ_1-SENSITIVITY

remember that we are interested in queries that return **distributions** (functions).

We introduce the notion of **ℓ_1-sensitivity** of a function.

ℓ_1-SENSITIVITY

Given a function f: $\mathbb{N}^{|\mathcal{X}|} \rightarrow \mathbb{R}^k$ its ℓ_1-sensitivity is:

$$\Delta f = \max_{x,y \in \mathbb{N}^{|\mathcal{X}|} ||x-y||_1 = 1} ||f(x) - f(y)||_1$$

The ℓ_1-sensitivity describes the maximum change in the function induced by a single instance.

Intuitively, it also gives the magnitude of the “perturbation” required to hide the participation of a single individual.

THE LAPLACE MECHANISM

As its name suggests, the Laplace mechanism relies on the Laplace distribution and requires to perturb each data-point with noise drawn from it.

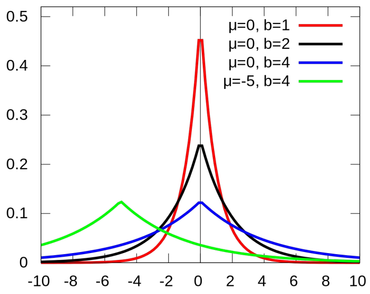
THE LAPLACE MECHANISM

Given a function f: $\mathbb{N}^{|\mathcal{X}|} \rightarrow \mathbb{R}^k$ the Laplace mechanism is defined as:

$$\mathcal{M}_L(x, f, \varepsilon) = f(x) + (Y_1, \ldots, Y_k)$$

Where $Y_1, \ldots, Y_k$ are drawn from Lap(0, $\Delta f/\varepsilon$), with Lap(x|μ, b) defined as:

$$Lap(x|\mu, b) = \frac{1}{2b} \cdot \exp\left(-\frac{|x-\mu|}{b}\right)$$



THE LAPLACE MECHANISM

The Laplace mechanism is (ε, 0)-differentially private:

$$
\begin{aligned}
\frac{\Pr_x(z)}{\Pr_y(z)} &= \prod_{i=1}^{k} \left(\frac{\exp\left(-\frac{\varepsilon|f(x)_i - z_i|}{\Delta f}\right)}{\exp\left(-\frac{\varepsilon|f(y)_i - z_i|}{\Delta f}\right)} \right) \\
&= \prod_{i=1}^{k} \exp\left(\frac{\varepsilon|f(x)_i - z_i| - |f(y)_i - z_i|}{\Delta f} \right) \\
&\leq \prod_{i=1}^{k} \exp\left(\frac{\varepsilon|f(x)_i - f(y)_i|}{\Delta f} \right) \\
&= \exp\left(\frac{\varepsilon||f(x) - f(y)||_1}{\Delta f} \right) \\
&= e^{\varepsilon}
\end{aligned}
$$

THE LAPLACE MECHANISM: ACCURACY

Let f: $\mathbb{N}^{|\mathcal{X}|} \rightarrow \mathbb{R}^k$ and y = $\mathcal{M}_L(x, f, \varepsilon)$. Then $\forall\ \delta \in (0, 1]$:

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right)\right] \leq \delta$$

This allows us to determine how “far” is our perturbation from the real value.

COUNTING QUERIES

Counting queries are the most common example of “statistical” queries on a dataset.

“How many instances have this characteristic?”, “What is the proportion of instances satisfying a certain property?”

What is the sensitivity of a counting query?

COUNTING QUERIES

Counting queries are the most common example of “statistical” queries on a dataset.

“How many instances have this characteristic?”, “What is the proportion of instances satisfying a certain property?”

What is the sensitivity of a counting query?

$$\Delta f = \max_{x,y \in \mathbb{N}^{|\mathcal{X}|},\ ||x-y||_1 = 1} ||f(x) - f(y)||_1$$

How much changing a single instance changes the count?

COUNTING QUERIES

Counting queries are the most common example of "statistical" queries on a dataset.

"How many instances have this characteristic?", "What is the proportion of instances satisfying a certain property?"

What is the sensitivity of a counting query? **1**

COUNTING QUERIES

Counting queries are the most common example of “statistical” queries on a dataset.

“How many instances have this characteristic?”, “What is the proportion of instances satisfying a certain property?”

What is the sensitivity of a counting query? **1**

How much should we perturbate the result to make a counting query $(\varepsilon, 0)$-differentially private?

COUNTING QUERIES

Counting queries are the most common example of “statistical” queries on a dataset.

“How many instances have this characteristic?”, “What is the proportion of instances satisfying a certain property?”

What is the sensitivity of a counting query? **1**

How much should we perturbate the result to make a counting query (ε, 0)-differentially private? **Lap(1/ε)**

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

HISTOGRAM QUERIES

Histogram queries are (disjoint) count queries: we have n distinct ranges and we want to compute how many instances fall on each range.

How can we achieve (ε, 0)-differentially private queries?

- determine the sensitivity
- determine the perturbation distribution

HISTOGRAM QUERIES

Akin to count queries, also for histogram queries switching between neighbouring datasets changes only the count for a single range of 1: the sensitivity is 1.

Add to each column noise independently drawn from a Lap($1/\varepsilon$)

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right) \right] \leq \delta$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right) \right] \leq \delta$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right)\right] \leq \delta$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right)\right] \leq \delta$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right)\right] \leq \delta$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

$$\Pr\left[||f(x) - y||_\infty \geq \ln\left(\frac{k}{\delta}\right) \cdot \left(\frac{\Delta f}{\varepsilon}\right) \right] \leq \delta$$

$$\Pr\left[||f(x) - y||_\infty \geq \underbrace{\boxed{\ln\left(\frac{10000}{0.05}\right) \cdot \left(\frac{1}{1}\right)}}_{\approx 12.2} \right] \leq 0.05$$

FIRST NAMES

With probability 95%, how accurate is the (perturbed) histogram of the top 10000 names in the 2010 american census for a (1, 0)-differentially private Laplace mechanism?

The distance between the real and perturbed data will be, in most of the cases at most 12.2 (with over 300,000,000 people participating to the census).

REPORT NOISY MAX

Assume we have m independent count queries (not an histogram!) then the **report noisy max** that returns the index of the largest (Lap($1/\varepsilon$) perturbed) count, is (ε, 0) - differentially private.

Notice that **we do not release the counts**: they would be much more informative than ε: single user can appear in all the m count queries, thus $\boldsymbol{\Delta}$f=m.

The **noise is independent from the number of queries**.

GAUSSIAN NOISE

We can define a perturbation process based on a Gaussian noise which allows to have a differentially private mechanism.

$$\mathcal{M}_{\mathcal{G}}(x,\, \varepsilon, \delta) \sim \mathcal{N}\left(x,\, \frac{2\ln(1.25/\delta) \cdot (\Delta_2 f)^2}{\varepsilon^2} \right)$$

Where $\boldsymbol{\Delta}_2$ is the ℓ_2-sensitivity of the function.

Laplace mechanism can be used with δ=0 (ε-DP), Gaussian cannot (there is a risk of releasing more information than what we would like...).

Gaussian Mechanism is also less accurate (more noise).

GAUSSIAN NOISE

Why using it?

If the function f for which we are releasing the values returns a vector of size k and not a single value, its ℓ_2-sensitivity is smaller than its ℓ_1-sensitivity by a factor of sqrt(k).

Gaussian noise is particularly useful when you plan to release long vectors!

THE EXPONENTIAL MECHANISM

“How many people have blue eyes?” $\rightarrow$ Perturbing the answer with the Laplace mechanism does not “destroy” our answer: we introduce an error, but we will be “close” to the correct answer.

THE EXPONENTIAL MECHANISM

“What is the best value for a certain threshold?” → a small perturbation that brings the best value over the threshold, might make useless the answer!

THE EXPONENTIAL MECHANISM: THE AUCTION

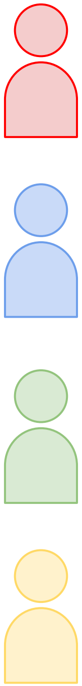
We are going to hold an auction to sell a certain product.

- Each (possible) buyer places their secret bid: they don't want the final price to be influenced by their bids, so the bids must remain secret also to the seller.

- If we set the price of the product below or equal to the bid, then the buyer will buy the item at the price we have chosen.

- If we set the price above the bid, then the buyer won't buy the product.

ON THE EXPONENTIAL MECHANISM

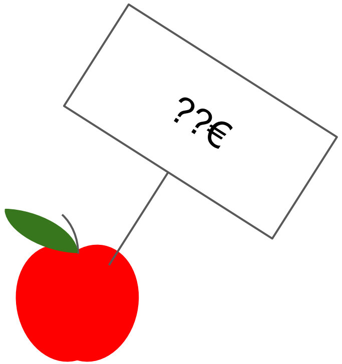


4.10€

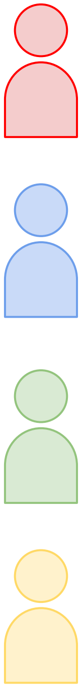
1.00€

1.00€

1.00€



ON THE EXPONENTIAL MECHANISM

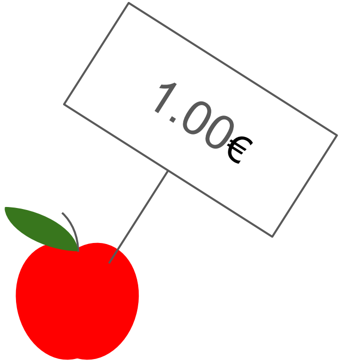


4.10€

1.00€

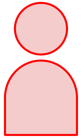
1.00€

1.00€

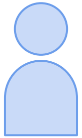


If the price is 1: everyone buys.
Total gain = price*buyers = 1*4 = 4.00

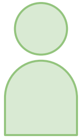
ON THE EXPONENTIAL MECHANISM



4.10€

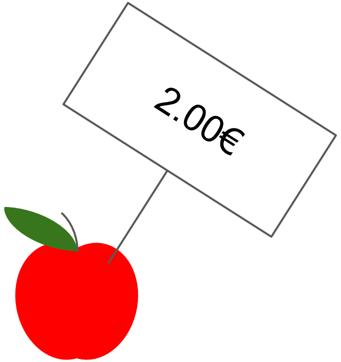


1.00€



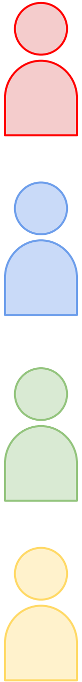
1.00€

1.00€



If the price is 2: only red buys.
Total gain = price*buyers = 2*1 = 2.00

ON THE EXPONENTIAL MECHANISM

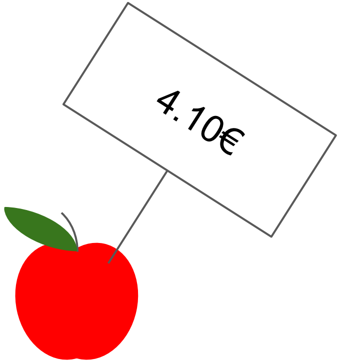


4.10€

1.00€

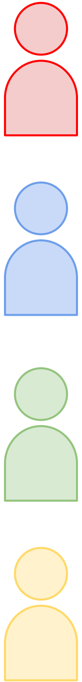
1.00€

1.00€



If the price is 4.10: only red buys.
Total gain = price*buyers = 4.10*1 = 4.10

ON THE EXPONENTIAL MECHANISM

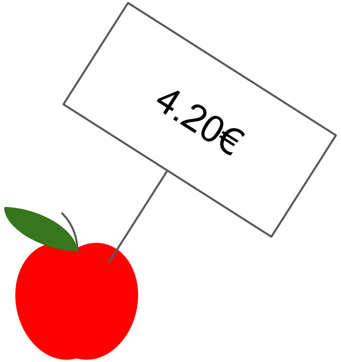


4.10€

1.00€

1.00€

1.00€

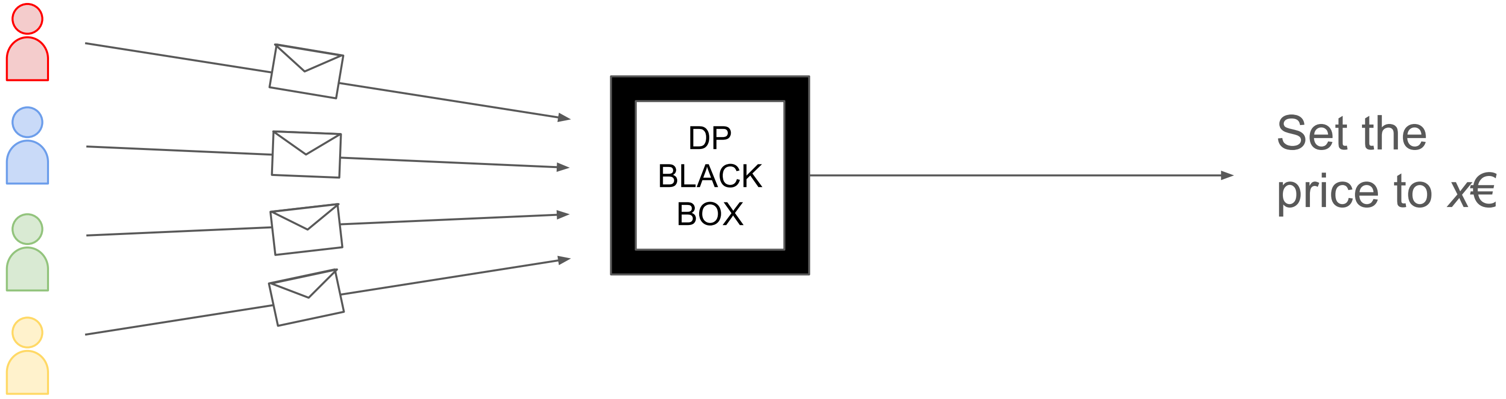


If the price is 4.20: nobody buys.
Total gain = price*buyers = 4.20*0 = 0

ON THE EXPONENTIAL MECHANISM

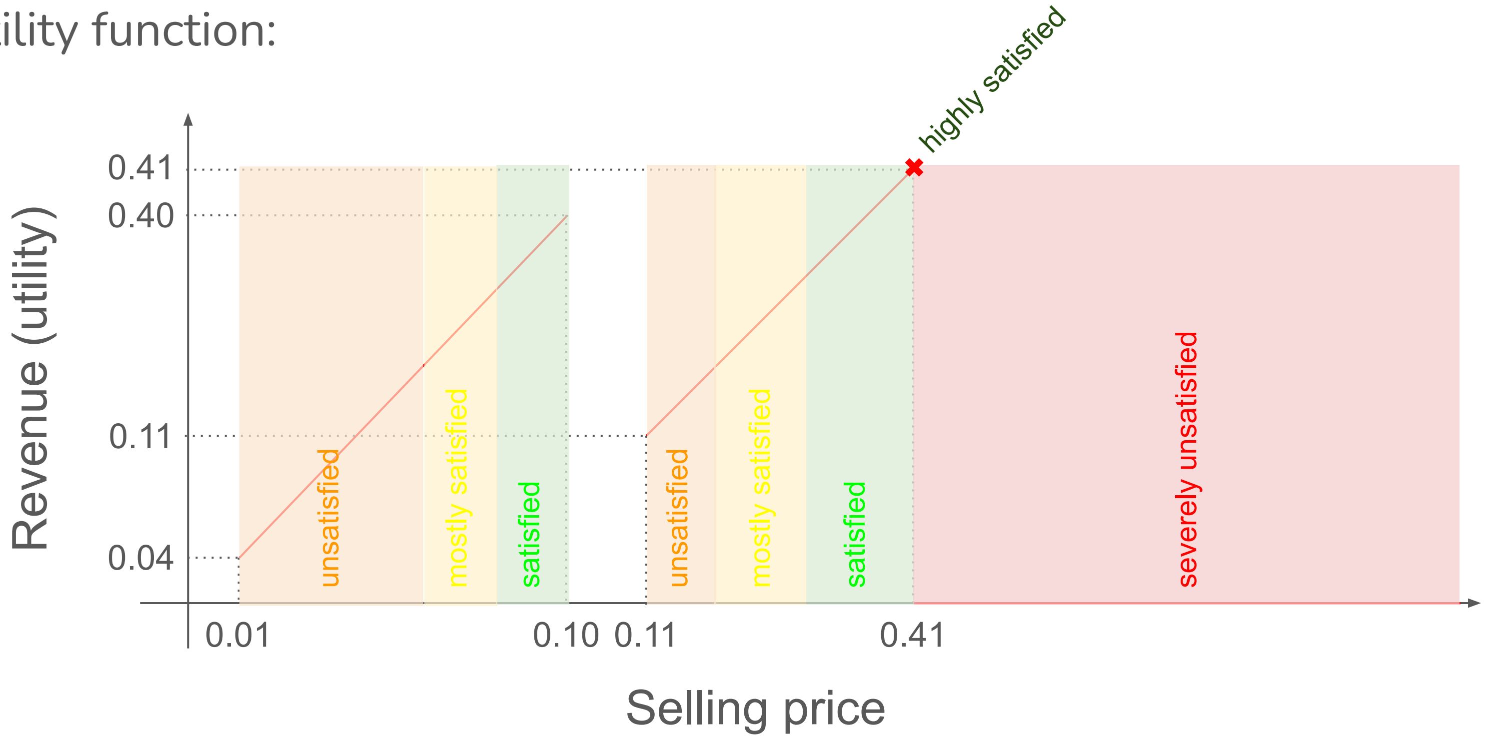
Challenges:

Red might not be happy with the selling price decided based on their bid. They will participate only if the bids remain private.

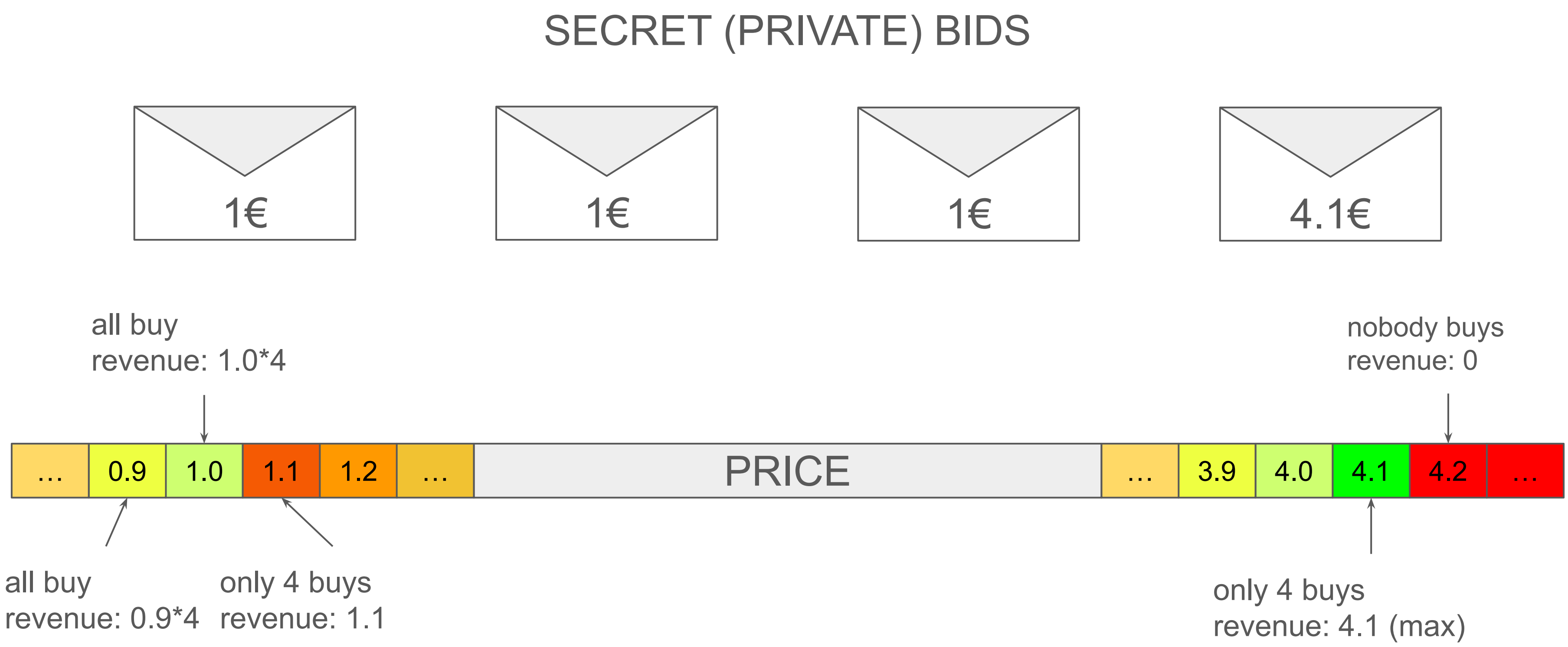


ON THE EXPONENTIAL MECHANISM

Utility function:



THE EXPONENTIAL MECHANISM: THE AUCTION



THE EXPONENTIAL MECHANISM: THE AUCTION

Perturbing from 1.0 to 1.1 or from 4.1 to 4.2 causes huge drops in terms of optimality of the price!

THE EXPONENTIAL MECHANISM: UTILITY

the revenue is the *utility* that we experience upon a realization of a certain future outcome ("if I will set the price to 1, my revenue will be 4").

we can then define a function *u* that, given a database, maps the set of possible future outcomes $\mathcal{R}$ (values from 0.1 to 4.2, with step 0.1) to a real value which represents the *utility* of the outcome:

$$u : \mathbb{N}^{|\mathcal{X}|}, \mathcal{R} \to \mathbb{R}$$

UTILITY

0.9	1.0	1.1	1.2	…	PRICE	…	3.9	4.0	4.1	4.2
3.6	4.0	1.1	1.2	…	UTILITY	…	3.9	4.0	4.1	0

THE EXPONENTIAL MECHANISM: SENSITIVITY

The sensitivity of a utility function *u* with respect to the future realizations is:

$$\Delta u = \max_{r \in \mathcal{R}} \max_{x,y; ||x-y||_1 \leq 1} |u(x, r) - u(y, r)|$$

It describes how much, with respect to two neighbouring datasets, the utility can change with respect to the same future outcome.

THE EXPONENTIAL MECHANISM: SENSITIVITY

0.9	1.0	1.1	1.2	…	PRICE	…	3.9	4.0	4.1	4.2
3.6	4.0	1.1	1.2	…	UTILITY	…	3.9	4.0	4.1	0
2.7	3.0	1.1	1.2	…	UTILITY (y_1)	…	3.9	4.0	4.1	0
2.7	3.0	1.1	1.2	…	UTILITY (y_2)	…	3.9	4.0	4.1	0
2.7	3.0	1.1	1.2	…	UTILITY(y_3)	…	3.9	4.0	4.1	0
2.7	3.0	0	0	…	UTILITY(y_4)	0	0	0	0	0
4.5	5	2.2	2.4	…	UTILITY(y_5)	…	7.8	8.0	8.2	4.2
2.8	2.0	2.2	2.4	…	SENSITIVITY	…	3.9	4.0	4.1	4.2

THE EXPONENTIAL MECHANISM: SENSITIVITY

0.9	1.0	1.1	1.2	…	PRICE	…	3.9	4.0	4.1	4.2
3.6	4.0	1.1	1.2	…	UTILITY	…	3.9	4.0	4.1	0
0.9	1.0	1.1	1.2	…	SENSITIVITY	…	3.9	4.0	4.1	4.2

THE EXPONENTIAL MECHANISM

The exponential mechanism $\mathcal{M}_E(x, u, \mathcal{R})$ selects and outputs an element r ∈ $\mathcal{R}$ with probability proportional to

$$\exp(\varepsilon u(x,r)/(2*\Delta u))$$

The exponential mechanism preserves (ε, 0)-differential privacy.

With the exponential mechanism we reduce the chances of outputting values in r where the utility is 0.

THE EXPONENTIAL MECHANISM: SENSITIVITY

0.9	1.0	1.1	1.2	…	PRICE	…	3.9	4.0	4.1	4.2
3.6	4.0	1.1	1.2	…	UTILITY	…	3.9	4.0	4.1	0
0.9	1.0	1.1	1.2	…	SENSITIVITY	…	3.9	4.0	4.1	4.2
1.02	1.02	1.02	1.03	…	PROBABILITY* (ε=0.1)	…	1.10	1.10	1.11	0

* This is not the probability, but a value which is proportional to it.

ACCURACY

if u is the utility achieved by the exponential mechanism, opt_u the optimal utility, and R_{opt} the set of optimal values (those that achieve the best utility), the following inequality bounds our errors:

$$\Pr\left[u(\mathcal{M}_E(x,\, u,\, \mathcal{R})) \leq opt_u(x) - \frac{2\Delta u}{\varepsilon}\left(\ln\left(\frac{|\mathcal{R}|}{|\mathcal{R}_{opt}|}\right) + t\right)\right] \leq e^{-t}$$

COMBINATION

Remember what we said last time about group privacy?

“Any (ε, 0)-differentially private mechanism $\mathcal{M}$ is (kε, 0)-differentially private for groups of size k”

And what about the report noisy max algorithm?

“We cannot release all the noisy counts to avoid increasing the sensitivity (and thus the privacy loss).”

COMBINATION

$\mathcal{M}_1$ ε_1-differentially private

$\mathcal{M}_2$ ε_2-differentially private

...

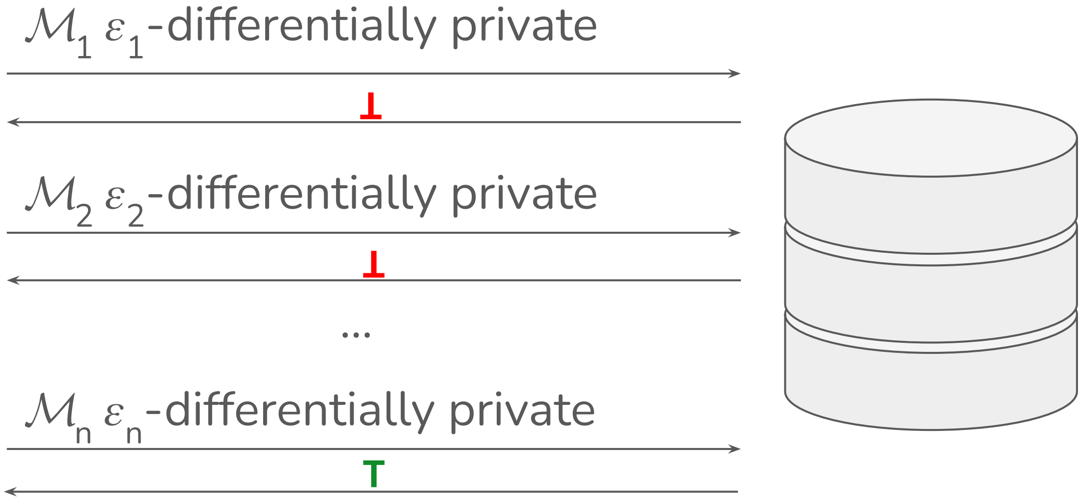
$\mathcal{M}_n$ ε_n-differentially private

The whole process is $(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)$-differentially private: each time we query our database we increase the privacy loss.

SPARSE VECTOR: ABOVE THRESHOLD

Let say that, instead of answering with the “correct” (perturbed) answer, we simply say if it is above a certain threshold.

SPARSE VECTOR: ABOVE THRESHOLD



More precisely, we continue answering as long as our results are below the threshold: once we get the first “above threshold” result, we stop.

SPARSE VECTOR: ABOVE THRESHOLD

Above-Threshold(D, Q, T, ε):

Let $T_p = T + \text{Lap}(2/\varepsilon)$;

for q_i in Q:

Let $v_i = \text{Lap}(4/\varepsilon)$;

if $q_i(D) + v_i \geq T_p$:

output $\top$

break

else:

output $\perp$

Where D is a dataset while Q is a stream of queries

SPARSE VECTOR - OTHER APPROACHES

By properly adapting the parameter of the Laplace and the threshold we can also expand our above threshold algorithm and remain ε differentially private. In particular:

- "Sparse" allows to output up to "c" above threshold results
- "NumericSparse" allows to output up to "c" above threshold results and their numerical value

Obviously, to achieve such result, we increase the noise and lose accuracy.

pseudocode here: https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf