* 1. 1. Imagine a hospital has a database of patients with a single column indicating whether or not the patient is HIV positive. The hospital wants to use an algorithm with 0.01-differential privacy (i.e., the simplest definition of differential privacy) to respond to the query - “How many patients are HIV positive?”.
  2. a) What is the sensitivity of this query function?

Sensitivity of function f= max |f(x1)-f(x2)| for neighbouring datasets x1 and x2. Used to measure how much one person can affect the output of the query.

Here the function is to compute the number of patients with HIV positive results. . The maximum difference should be 1 between the datasets. Since if the person who is …

b) Specify a query response algorithm with 0.01-differential privacy, i.e., provide a formula to generate the differentially private answer. [5 points]

add noise to make it diff private, pdf(z)= exp(-|z|/b)/2b, b=f/epsilon, As b gets larger less privacy

M(x.f(x),epsilon)= f(x)+ (Y1,Y2…YK). Here ,



(scale of laplace noise)Lambda=sensitivity/epsilon=1/epsilon=1/0.01=100

Pr(A=D)<exp(epsilon)\*Pr(A=D’)

\*Release the number + Laplace noise

=f(x)+lap(1/0.01)=f(x)+lap(100)

PDF(X)=exp(|x|/lambda)/2\*lambda.

=x+ exp(|x|/lambda)/2\*lambda=x+ exp(|x|/100)/2\*100

3)

Answer ! queries, each with sensitivity 1

• Use Laplace with "epsilon0 = epsilon/k” privacy per query

Epsilon no= 0.01/100=0.0001

2.

D is the dataset containing annual salaries of all NCSU employees. Let’s assume all salaries are in the range of [a, b. Let San be the standard Laplacian mechanism for -differential privacy. Given any function f, San generates random noise ξ from the Laplacian distribution with variance that depends on the sensitivity of function f and the privacy parameter ξ, and returns f(D) + ξ.

a. Assume f is mean(D) which returns the average salary in the dataset. What is the sensitivity of the mean function? State all assumptions you needed to calculate the answers. [10 points]

mean=salary\_sum/n,

mean(removal of b)= salary\_sum-b/n-1

diff=salary\_sum/n-salary\_sum/n-1+b/n-1

=salary\_sum(-1/n\*n-1+b/n-1)=

* 1. b)

. We view the database as a binary string x =x1 ... xn of length n. Identical copies of this string are stored by k >= 2 servers. The user has some index i, and he is interested in obtaining the value of the bit xi . To achieve this goal, the user queries each of the servers and gets replies from which the desired bit xi can be computed. The query to each server is distributed independently of i and therefore each server gains no information about i. A scheme with these properties is called a Private Information Retrieval (PIR) scheme.

We can’t reconstruct the data. • All servers have to respond properly • Which threat model is this?

Make the n-bit vector as a n1/2 \* n1/2 matrix • Consider each row as a n1/2 -bit database • Perform dot product with each row and xor result • Each server return one column DB • Take the xor of the j-th row across from all responses