CS 599: Formal Methods in Security and Privacy

Differential Privacy

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

(ε,δ)-Differential Privacy

Definition

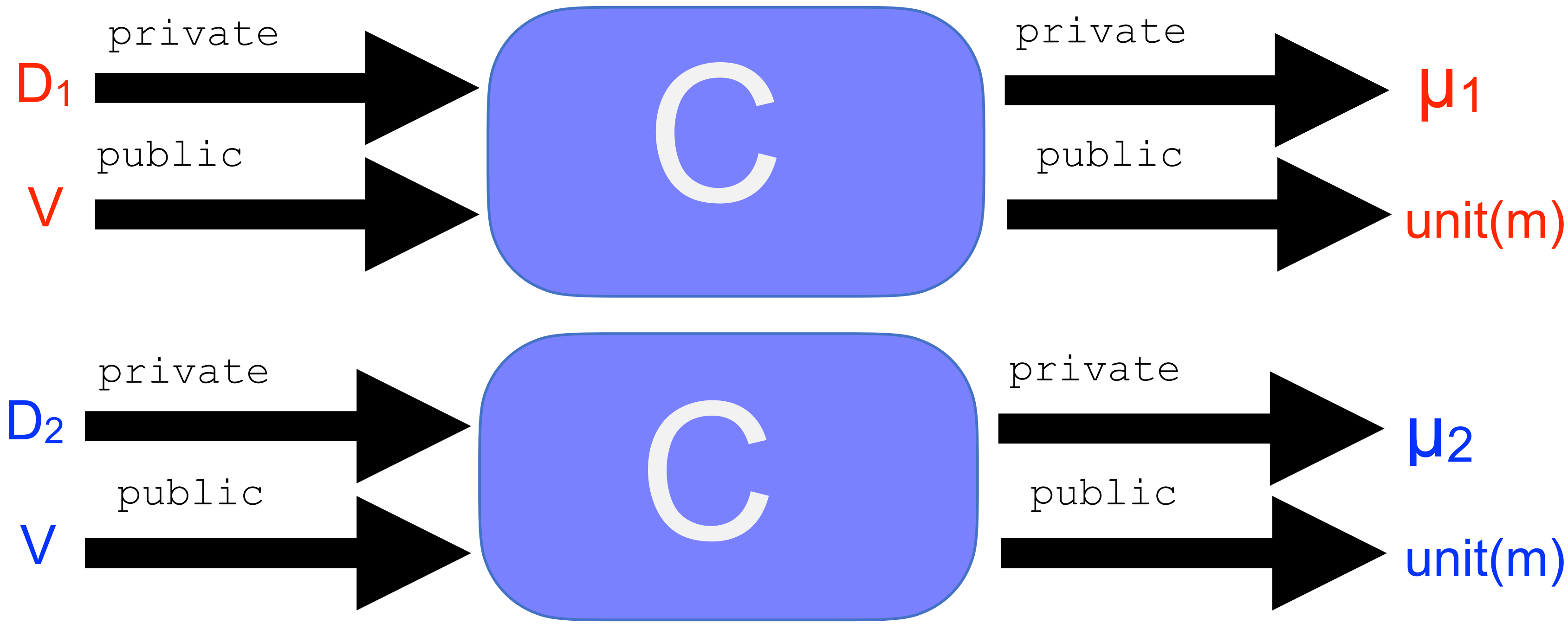
Given $\varepsilon,\delta \geq 0$, a probabilistic query $Q: X^n \rightarrow R$ is (ε,δ)-differentially private iff for all adjacent database b_1, b_2 and for every $S \subseteq R$:

$$\Pr[Q(b_1) \in S] \leq \exp(\varepsilon)\Pr[Q(b_2) \in S] + \delta$$

Differential Privacy as a Relational Property

c is differentially private if and only if for every $m_1 \sim m_2$ (extending the notion of adjacency to memories):

$\{c\}_{m1}=\mu_1$ and $\{c\}_{m2}=\mu_2$ implies $\Delta_\varepsilon(\mu_1,\mu_2) \leq \delta$



apRHL

Indistinguishability parameter

Precondition (a logical formula)

$$\vdash_{\epsilon,\delta} c_1 \sim c_2 : P \Rightarrow Q$$

Probabilistic Program

Probabilistic Program

Postcondition (a logical formula)

Validity of apRHL judgments

We say that the 6-tuple $\vdash_{\varepsilon,\delta}$ $c_1 \sim c_2 : P \Rightarrow Q$ is valid if and only if for every pair of memories m_1, m_2 such that $P(m_1, m_2)$ we have: $\{c_1\}_{m1} = \mu_1$ and $\{c_2\}_{m2} = \mu_2$ implies $Q_{\varepsilon,\delta}{}^*(\mu_1, \mu_2)$.

R-(ε,δ)-Coupling

Given two distributions $\mu_1 \in D(A)$, and $\mu_2 \in D(B)$, we have an R-(ε,δ)-coupling between them, for $R \subseteq AxB$ and $0 \le \delta \le 1$, $\varepsilon \ge 0$, if there are two joint distributions $\mu_L, \mu_R \in D(AxB)$ such that:

1) $\pi_1(\mu_L) = \mu_1$ and $\pi_2(\mu_R) = \mu_2$,
2) the support of μ_L and μ_R is contained in R. That is, if $\mu_L(a,b) > 0$, then $(a,b) \in R$, and if $\mu_R(a,b) > 0$, then $(a,b) \in R$.
3) $\Delta_\varepsilon(\mu_L, \mu_R) \le \delta$

Example of R-(ε,δ)-Coupling

μ_1

00	0.25
01	0.25
10	0.25
11	0.25

$R(a,b) = \{a=b\}$

μ_2

00	0.20
01	0.25
10	0.25
11	0.30

μ_L	00	01	10	11
00	0.25			
01		0.25		
10			0.25	
11				0.25

μ_R	00	01	10	11
00	0.20			
01		0.25		
10			0.25	
11				0.30

$$\Delta_{0.3}(\mu_L, \mu_R) = 0$$

apRHL: skip rule

$$\frac{}{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

Correctness of Skip Rule

$$\overline{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

To show this rule correct we need to show the validity of the $\vdash_{0,0}$ $\texttt{skip}\sim\texttt{skip}: P\Rightarrow P$.

Correctness of Skip Rule

$$\frac{}{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

To show this rule correct we need to show the validity of the $\vdash_{0,0}$ $\texttt{skip}\sim\texttt{skip}: P \Rightarrow P$.

For every m_1, m_2 such that $P(m,m')$ we have $\{\texttt{skip}\}_m = \texttt{unit}(m)$ and $\{\texttt{skip}\}_{m'} = \texttt{unit}(m')$ we need $P^*_{0,0}(\texttt{unit}(m), \texttt{unit}(m'))$.

Correctness of Skip Rule

$$\frac{}{\vdash_{0,0} \mathtt{skip} \sim \mathtt{skip} : P \Rightarrow P}$$

Correctness of Skip Rule

$$\overline{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

μ_L	m_1	m_2	…	m'	…
m_1	0	0	…	0	0
m_2	0	0	…	0	0
…	…	…	…	…	…
m	0	0	…	1	0
…	…	…	…	…	…

Correctness of Skip Rule

$$\overline{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

μ_L	m_1	m_2	…	m’	…
m_1	0	0	…	0	0
m_2	0	0	…	0	0
…	…	…	…	…	…
m	0	0	…	1	0
…	…	…	…	…	…

μ_R	m_1	m_2	…	m’	…
m_1	0	0	…	0	0
m_2	0	0	…	0	0
…	…	…	…	…	…
m	0	0	…	1	0
…	…	…	…	…	…

Correctness of Skip Rule

$$\frac{}{\vdash_{0,0} \texttt{skip} \sim \texttt{skip} : P \Rightarrow P}$$

μ_L	m_1	m_2	…	m'	…
m_1	0	0	…	0	0
m_2	0	0	…	0	0
…	…	…	…	…	…
m	0	0	…	1	0
…	…	…	…	…	…

μ_R	m_1	m_2	…	m'	…
m_1	0	0	…	0	0
m_2	0	0	…	0	0
…	…	…	…	…	…
m	0	0	…	1	0
…	…	…	…	…	…

We need to show:

1) $\pi_1(\mu_L)=\text{unit}(m)$ and $\pi_2(\mu_R)=\text{unit}(m')$
2) $(m,m') \in P$ 3) $\Delta_0(\mu_L,\mu_R) \leq 0$

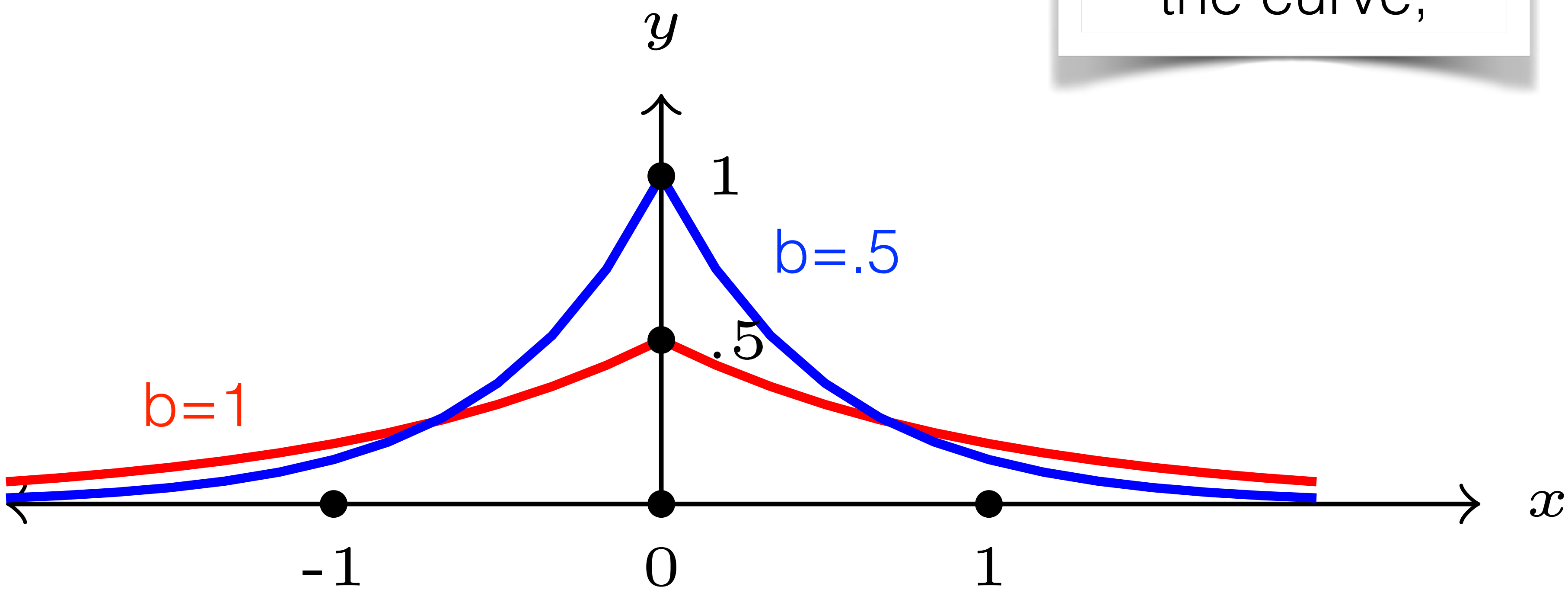
apRHL: Lap rule (simplified)

$$\frac{}{\vdash_{\varepsilon,0} \texttt{x}_1 \texttt{:=\$ Lap(1/}\varepsilon\texttt{,y}_1\texttt{)} \sim \texttt{x}_2 \texttt{:=\$ Lap(1/}\varepsilon\texttt{,y}_2\texttt{)} : |\texttt{y}_1 - \texttt{y}_2| \leq 1 \Rightarrow =}$$

Laplace Distribution

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

b regulates the skewness of the curve,



Correctness of Lap Rule

To show this rule correct we need to show the validity of

$\vdash_{\varepsilon,0}$ `x`$_1$`:=$Lap(`$^{1}/_{\varepsilon}$`, y`$_1$`)~x`$_2$`:=$Lap(`$^{1}/_{\varepsilon}$`, y`$_2$`):`

`|y1-y2|≤1 ⇒ =`.

Correctness of Lap Rule

To show this rule correct we need to show the validity of

$\vdash_{\varepsilon,0}$ x1:=\$Lap(1/ε, y1) ~ x2:=\$Lap(1/ε, y2): |y1-y2|≤1 ⇒ =.

For every m_1, m_2 such that P(m,m′) we have

{x1:=\$Lap(1/ε, y1)}m = let a={Lap(1/ε, y1)}m in unit(m[x1←a]) and

{x2:=\$Lap(1/ε, y2)}m′ = let a={Lap(1/ε, y2)} m′ in unit(m′[x2←a]) we need to show that these two terms are in the (ε,0) lifting of =.

Correctness of Lap Rule

We can take:

$\mu_L(m_1,m_2)=\mathbb{1}_{m1=m2}*\text{Lap}(1/\varepsilon, m(y_1))(a)*\mathbb{1}_{m1(x1)=a}$

and

$\mu_R(m_1,m_2)=\mathbb{1}_{m1=m2}*\text{Lap}(1/\varepsilon, m'(y_2))(a)*\mathbb{1}_{m1(x2)=a}$

Correctness of Lap Rule

We can take:

$\mu_L(m_1,m_2)=\mathbb{1}_{m1=m2}$*Lap(`1/ε, m(y₁)`)(a)*$\mathbb{1}_{m1(x1)=a}$

and

$\mu_R(m_1,m_2)=\mathbb{1}_{m1=m2}$*Lap(`1/ε, m'(y₂)`)(a)*$\mathbb{1}_{m1(x2)=a}$

We need to show:

1) $\pi_1(\mu_L)$=`let a={Lap(1/ε,y₁)}m in unit(m[x1←a])`

   and

   $\pi_2(\mu_R)$=`let a={Lap(1/ε,y₂)}m in unit(m[x2←a])`

2) $(m_1, m_2) \in =$ 3) $\Delta_\varepsilon(\mu_L,\mu_R)\leq 0$

Correctness of Lap Rule

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L,}\mu_{R}) \leq 0$ we can think about:

Correctness of Lap Rule

To prove $\Delta_\varepsilon(\mu_{L},\mu_R)\leq 0$ we can think about:

$$\frac{\text{Lap}(1/\varepsilon, m(y_1))(a)}{\text{Lap}(1/\varepsilon, m'(y_2))(a)}$$

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L}, \mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L}, \mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1) - a|)}{\exp(-\varepsilon|m(y_2) - a|)}$$

By the precondition we know $|y1 - y2| \leq 1$.

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L}, \mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon |m(y_1) - a|)}{\exp(-\varepsilon |m(y_2) - a|)}$$

By the precondition we know $|y1-y2| \leq 1$.

Let's consider for example the case $y1=y2+1$

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L}, \mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2| \leq 1$.

Let's consider for example the case $y1=y2+1$

$$\frac{\exp(-\varepsilon|m(y_2)+1-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_L, \mu_R) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2| \leq 1$.

Let's consider for example the case $y1=y2+1$

$$\frac{\exp(-\varepsilon|m(y_2)+1-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+1-a|)$$

Correctness of Lap Rule

To prove $\Delta_{\varepsilon}(\mu_{L},\mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2| \leq 1.$

Let's consider for example the case $y1=y2+1$

$$\frac{\exp(-\varepsilon|m(y_2)+1-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+1-a|)$$

$$\leq \exp(\varepsilon|m(y2)-m(y2)+1|)$$

Correctness of Lap Rule

To prove $\Delta_\varepsilon(\mu_{L},\mu_R)\leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2|\leq 1$.

Let's consider for example the case $y1=y2+1$

$$\frac{\exp(-\varepsilon|m(y_2)+1-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+1-a|)$$

$$\leq \exp(\varepsilon|m(y2)-m(y2)+1|)$$

$$= \exp(\varepsilon)$$

apRHL: More general Lap rule (still restricted)

$$\vdash_{k*\varepsilon,0} \frac{}{\texttt{x}_1 \texttt{:=\$ Lap(1/}\varepsilon\texttt{,y}_1\texttt{)} \sim \texttt{x}_2 \texttt{:=\$ Lap(1/}\varepsilon\texttt{,y}_2\texttt{)} : |\texttt{y}_1 - \texttt{y}_2| \le k \Rightarrow =}$$

Correctness of Lap Rule

To show this rule correct we need to show the validity of

$\vdash_{k*\varepsilon,0} x_1 := \$Lap(1/\varepsilon, y_1) \sim x_2 := \$Lap(1/\varepsilon, y_2) : |y1-y2| \leq k \Rightarrow =.$

Correctness of Lap Rule

To show this rule correct we need to show the validity of

$\vdash_{k^*\varepsilon,0}$ `x₁:=$Lap(1/ε,y₁)~x₂:=$Lap(1/ε,y₂):|y1-y2|≤k ⇒ =`.

For every m_1, m_2 such that `P(m,m')` we have

`{x₁:=$Lap(1/ε,y₁)}m=let a={Lap(1/ε,y₁)}m in unit(m[x1←a])` and

`{x₁:=$Lap(1/ε,y₁)}m=let a={Lap(1/ε,y₁)}m in unit(m[x1←a])` we need to show that these two terms are in the $(k^*\varepsilon, 0)$ lifting of =.

Correctness of Lap Rule

We can take:

$\mu_L(m_1,m_2)=\mathbb{1}_{m1=m2}$*$Lap(1/\varepsilon, m(y_1))(a)$*$\mathbb{1}_{m1(x1)=a}$

and

$\mu_R(m_1,m_2)=\mathbb{1}_{m1=m2}$*$Lap(1/\varepsilon, m'(y_2))(a)$*$\mathbb{1}_{m1(x2)=a}$

Correctness of Lap Rule

We can take:

$\mu_L(m_1,m_2)=\mathbb{1}_{m1=m2} * Lap(1/\varepsilon, m(y_1))(a) * \mathbb{1}_{m1(x1)=a}$

and

$\mu_R(m_1,m_2)=\mathbb{1}_{m1=m2} * Lap(1/\varepsilon, m'(y_2))(a) * \mathbb{1}_{m1(x2)=a}$

We need to show:

1) $\pi_1(\mu_L)=$ `let a={Lap(1/ε,y1)}m in unit(m[x1←a])`

   and

   $\pi_2(\mu_R)=$ `let a={Lap(1/ε,y2)}m in unit(m[x2←a])`

2) $(m_1, m_2) \in =$ 3) $\Delta_{k^*\varepsilon}(\mu_L, \mu_R) \le 0$

Correctness of Lap Rule

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_L, \mu_R) \leq 0$ we can think about:

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_L, \mu_R) \leq 0$ we can think about:

$$\frac{\text{Lap}(1/\varepsilon, m(y_1))(a)}{\text{Lap}(1/\varepsilon, m'(y_2))(a)}$$

Correctness of Lap Rule

To prove $\Delta_{k^* \varepsilon}(\mu_L, \mu_R) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_{L},\mu_{R}) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2| \leq k$.

Correctness of Lap Rule

To prove $\Delta_{k*\varepsilon}(\mu_{L},\mu_{R})\leq 0$ we can think about:

$$\frac{Lap(1/\varepsilon, m(y_1))(a)}{Lap(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2|\leq k$.

Let's consider for example the case $y1=y2+k$

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_L, \mu_R) \leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2| \leq k$.

Let's consider for example the case $y1=y2+k$

$$\frac{\exp(-\varepsilon|m(y_2)+k-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

Correctness of Lap Rule

To prove $\Delta_{k^{*}\varepsilon}(\mu_{L},\mu_{R}) \leq 0$ we can think about:

$$\frac{Lap(1/\varepsilon, m(y_1))(a)}{Lap(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2|\leq k$.

Let's consider for example the case $y1=y2+k$

$$\frac{\exp(-\varepsilon|m(y_2)+k-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+k-a|)$$

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_L,\mu_R)\leq 0$ we can think about:

$$\frac{Lap(1/\varepsilon, m(y_1))(a)}{Lap(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2|\leq k$.

Let's consider for example the case $y1=y2+k$

$$\frac{\exp(-\varepsilon|m(y_2)+k-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+k-a|)$$

$$\leq \exp(\varepsilon|m(y2)-m(y2)+k|)$$

Correctness of Lap Rule

To prove $\Delta_{k^*\varepsilon}(\mu_L,\mu_R)\leq 0$ we can think about:

$$\frac{\mathrm{Lap}(1/\varepsilon, m(y_1))(a)}{\mathrm{Lap}(1/\varepsilon, m'(y_2))(a)} = \frac{\exp(-\varepsilon|m(y_1)-a|)}{\exp(-\varepsilon|m(y_2)-a|)}$$

By the precondition we know $|y1-y2|\leq k$.

Let's consider for example the case $y1=y2+k$

$$\frac{\exp(-\varepsilon|m(y_2)+k-a|)}{\exp(-\varepsilon|m(y_2)-a|)} = \exp(\varepsilon|m(y2)-a|-\varepsilon|m(y2)+k-a|)$$

$$\leq \exp(\varepsilon|m(y2)-m(y2)+k|)$$

$$= \exp(k^*\varepsilon)$$

Releasing privately the mean of Some Data

```
Mean(d : private data) : public real
    i:=0;
    s:=0;
    while (i<size(d))
        s:=s + d[i]
        i:=i+1;
    z:=$ Lap(sens/eps,(s/i))
    return z
```

Composition

Let M_1:DB $\rightarrow R_1$ be a (ε_1,δ_1)-differentially private program and M_2:DB $\rightarrow R_2$ be a (ε_2,δ_1)-differentially private program. Then, their composition $M_{1,2}$:DB$\rightarrow R_1$xR_2 defined as

$$M_{1,2}(D)=(M_1(D),M_2(D))$$

is $(\varepsilon_1+\varepsilon_2,\delta_1+\delta_2)$-differentially private.

Probabilistic Relational Hoare Logic
Composition

$$\frac{\vdash_{\varepsilon 1,\delta 1} c_1 \sim c_2 : P \Rightarrow R \quad \vdash_{\varepsilon 2,\delta 2} c_1' \sim c_2' : R \Rightarrow S}{\vdash_{\varepsilon 1+\varepsilon 2,\delta 1+\delta 2} c_1; c_1' \sim c_2; c_2' : P \Rightarrow S}$$

Releasing partial sums

```
DummySum(d : {0,1} list) : real list
   i:= 0;
   s:= 0;
   r:= [];
   while (i<size d)
      s:= s + d[i]
      z:=$ Lap(eps,s)
      r:= r ++ [z];
      i:= i+1;
   return r
```

I am using the easycrypt notation here where `Lap(eps,a)` corresponds to adding to the value `a` noise from the Laplace distribution with `b=1/eps` and mean `mu=0`.

Parallel Composition

Let M_1:DB →R be a (ε_1,δ_1)-differentially private program and M_2:DB →R be a (ε_2,δ_2)-differentially private program. Suppose that we partition D in a data-independent way into two datasets D_1 and D_2. Then, the composition $M_{1,2}$:DB→R defined as

$$MP_{1,2}(D)=(M_1(D_1),M_2(D_2))$$

is $(\max(\varepsilon_1,\varepsilon_2),\max(\delta_1,\delta_2))$-differentially private.

Probabilistic Relational Hoare Logic

Composition

$$\frac{\vdash_{\varepsilon 1,\delta 1} c_1 \sim c_2 : P \Rightarrow R \quad \vdash_{\varepsilon 2,\delta 2} c_1' \sim c_2' : R \Rightarrow S}{\vdash_{\varepsilon 1+\varepsilon 2,\delta 1+\delta 2} c_1 ; c_1' \sim c_2 ; c_2' : P \Rightarrow S}$$

Releasing partial sums

```
DummySum(d : {0,1} list) : real list
   i:=0;
   s:=0;
   r:=[];
   while (i<size d)
      z:=$ Lap(eps,d[i])
      s:= s + z
      r:= r ++ [s];
      i:= i+1;
   return r
```

apRHL
awhile

```
P/\ e<1>≤0 => ¬b1<1>

⊢ε_k,δ_k c1~c2:P/\b1<1>/\b2<2>/\k=e<1> /\ e<1>≤n
        ==> P /\ b1<1>=b2<2> /\k < e<1>
────────────────────────────────────────────────────
              while b1 do c1~while b2 do c2
⊢∑ε_k,∑δ_k    :P/\ b1<1>=b2<2>/\ e<1> ≤ n
               ==> P /\ ¬b1<1>/\ ¬b2<2>
```