CS 591: Formal Methods in Security and Privacy

Differential Privacy

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

Where we were…

(ε,δ)-Differential Privacy

Definition

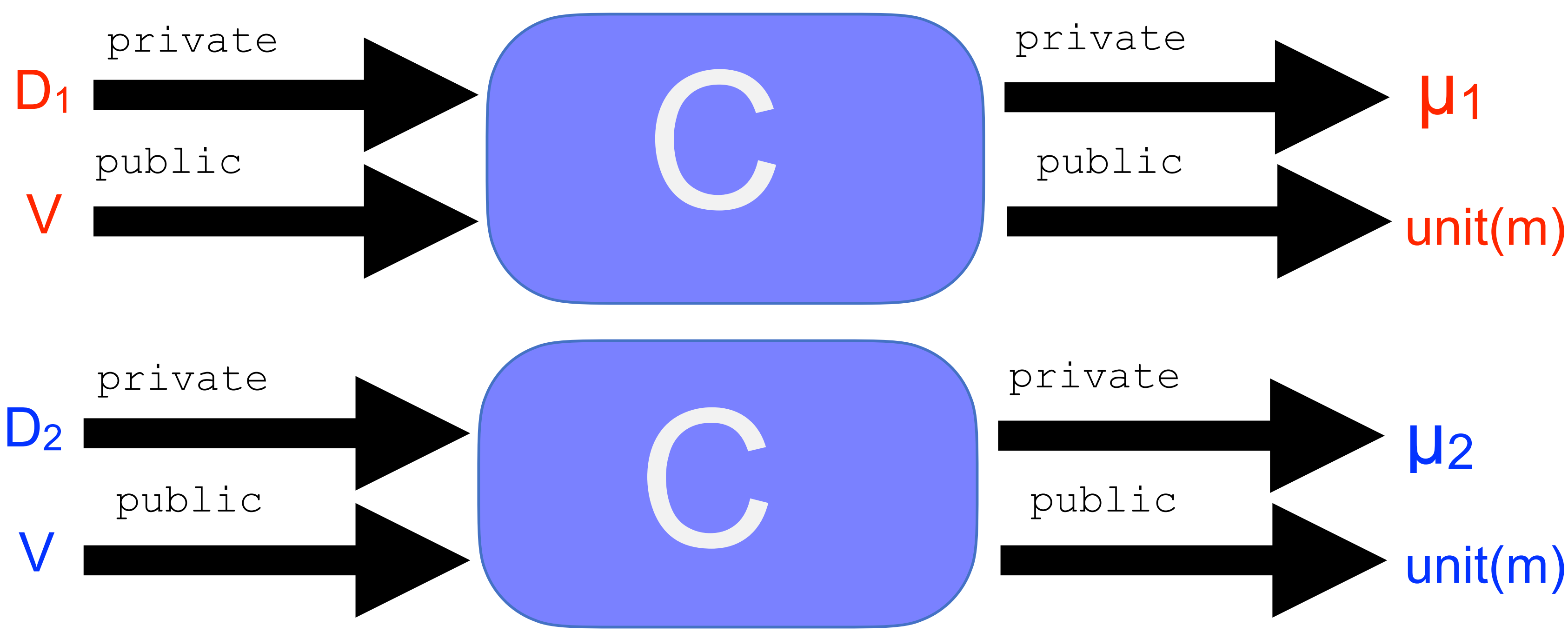
Given $\varepsilon,\delta \geq 0$, a probabilistic query $Q: X^n \rightarrow R$ is (ε,δ)-differentially private iff for all adjacent database b_1, b_2 and for every $S \subseteq R$:

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

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 $\vdash_{\epsilon,\delta} c_1 \sim c_2 : P \Rightarrow Q$ 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 $Q_{\epsilon,\delta}{*}(\mu_1, \mu_2)$.

$\mathcal{R}$-(ε,δ)-Coupling

Given two distributions $\mu_1 \in D(A)$, and $\mu_2 \in D(B)$, we have an $\mathcal{R}$-(ε,δ)-coupling between them, for $\mathcal{R} \subseteq A \times B$ and $0 \leq \delta \leq 1$, $\varepsilon \geq 0$, if there are two joint distributions $\mu_L, \mu_R \in D(A \times B)$ 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 $\mathcal{R}$. That is, if $\mu_L(a,b) > 0$, then $(a,b) \in \mathcal{R}$, and if $\mu_R(a,b) > 0$, then $(a,b) \in \mathcal{R}$.
3) $\Delta_\varepsilon(\mu_L, \mu_R) \leq \delta$

apRHL: skip rule

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

Correctness of Skip Rule

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

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

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

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

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

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
…	…	…	…	…	…

We need to show:

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

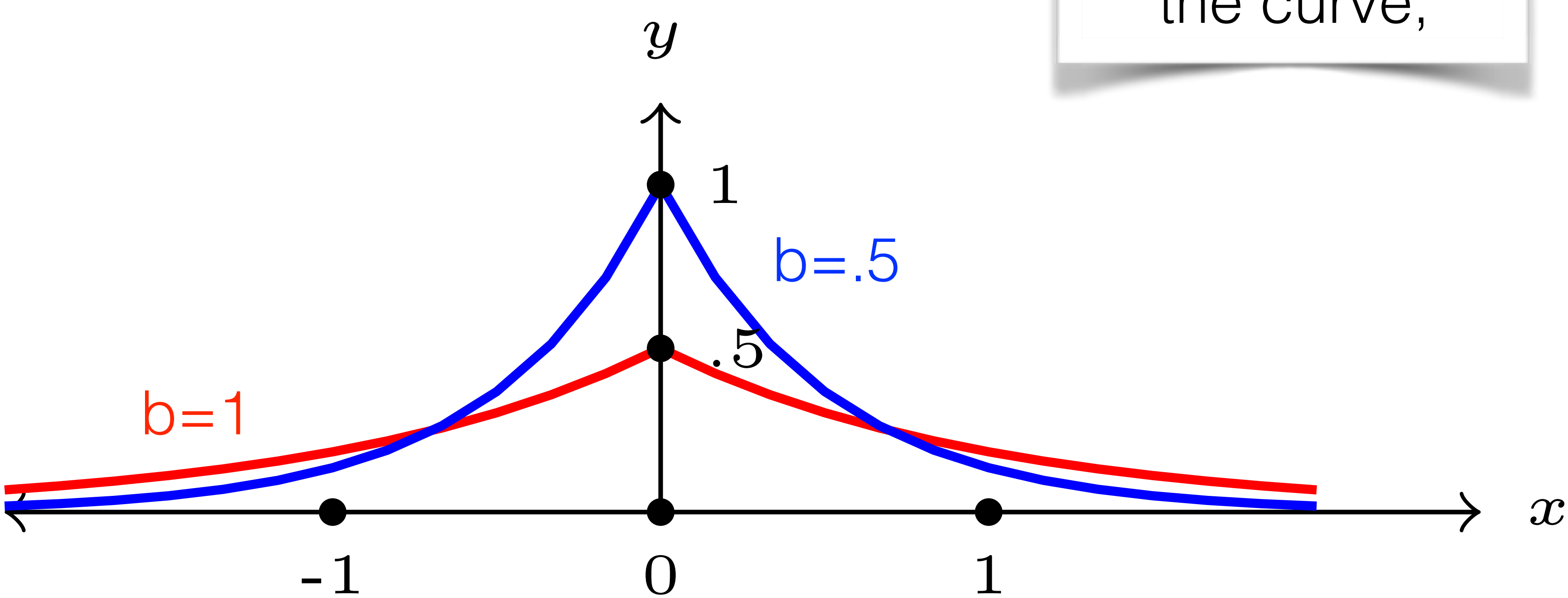
apRHL: Lap rule (simplified)

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

Laplace Distribution

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

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

$\vdash_{\varepsilon,0}$ `x`$_1$`:=$Lap(`$^{1/\varepsilon}$`,y`$_1$`)~x`$_2$`:=$Lap(`$^{1/\varepsilon}$`,y`$_2$`):`
`|y1-y2|≤1 ⇒ =`.

For every m_1,m_2 such that `P(m,m')` we have
`{x`$_1$`:=$Lap(`$^{1/\varepsilon}$`,y`$_1$`)}`$_m$`=let a={Lap(`$^{1/\varepsilon}$`,y`$_1$`)}m`
`in unit(m[x1←a])` and
`{x`$_1$`:=$Lap(`$^{1/\varepsilon}$`,y`$_1$`)}`$_m$`=let a={Lap(`$^{1/\varepsilon}$`,y`$_1$`)}m`
`in unit(m[x1←a])` we need to show that these two terms are in the (ε,0) lifting of =.

Correctness of Lap Rule

We can take:

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

and

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

Correctness of Lap Rule

We can take:

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

and

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

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) $\Delta_\varepsilon(\mu_L,\mu_R)\leq 0$

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:

$$\frac{\mathrm{Lap}(1/\varepsilon, \mathtt{m}(\mathtt{y}_1))(a)}{\mathrm{Lap}(1/\varepsilon, \mathtt{m}'(\mathtt{y}_2))(a)}$$

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:

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

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

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 $y1=y2+1$

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

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

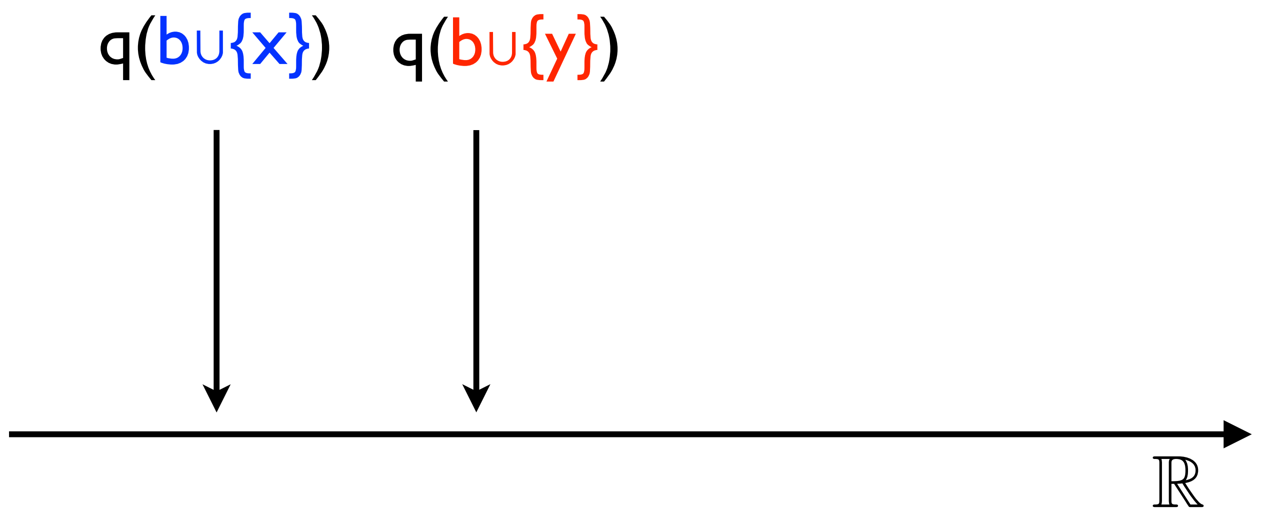
$$= \exp(\varepsilon)$$

Laplace Mechanism

```
Lap(d : priv data)(q: data -> real)
    (eps:real) : pub real
   z:= q(d)
   z:=$ Lap(GSq/eps,z)
   return z
```

Global Sensitivity

$$GS_q = \max\{\, |q(D) - q(D')| \text{ s.t. } D \sim D' \}$$



Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Proof:

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Proof:

Consider $D \sim_1 D' \in \mathcal{X}^n$, $q : \mathcal{X}^n \to \mathbb{R}$, and let p and p' denote the probability density function of $\mathsf{LapMech}(D, q, \epsilon)$ and $\mathsf{LapMech}(D', q, \epsilon)$ We compare them at an arbitrary point $z \in \mathbb{R}$.

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Proof:

Consider $D \sim_1 D' \in \mathcal{X}^n$, $q : \mathcal{X}^n \to \mathbb{R}$, and let p and p' denote the probability density function of $\mathsf{LapMech}(D, q, \epsilon)$ and $\mathsf{LapMech}(D', q, \epsilon)$ We compare them at an arbitrary point $z \in \mathbb{R}$.

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Continued proof:

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Continued proof:

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

$$= \exp\left(\frac{\epsilon(|q(D') - z| - |q(D) - z|)}{\Delta q}\right)$$

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Continued proof:

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

$$= \exp\left(\frac{\epsilon(|q(D') - z| - |q(D) - z|)}{\Delta q}\right)$$

$$\leq \exp\left(\frac{\epsilon(|q(D') - q(D)|)}{\Delta q}\right)$$

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Continued proof:

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

$$= \exp\left(\frac{\epsilon(|q(D') - z| - |q(D) - z|)}{\Delta q}\right)$$

$$\leq \exp\left(\frac{\epsilon(|q(D') - q(D)|)}{\Delta q}\right)$$

$$\leq \exp(\epsilon)$$

Laplace Mechanism

Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is ε-differentially private.

Continued proof:

$$\frac{p(z)}{p'(z)} = \frac{\exp\left(-\frac{\epsilon|q(D)-z|}{\Delta q}\right)}{\exp\left(-\frac{\epsilon|q(D')-z|}{\Delta q}\right)}$$

$$= \exp\left(\frac{\epsilon(|q(D')-z| - |q(D)-z|)}{\Delta q}\right)$$

$$\leq \exp\left(\frac{\epsilon(|q(D')-q(D)|)}{\Delta q}\right)$$

$$\leq \exp(\epsilon)$$

Similarly, we can prove that $\exp(-\epsilon) \leq \frac{p(z)}{p'(z)}$

Laplace Mechanism

```
Lap(d : priv data)(q: data -> real)
    (eps:real) : pub real
   z:= q(d)
   z:=$ Lap(GS_q/eps,z)
   return z
```

apRHL: More general Lap rule (still restricted)

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

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)~x_2:=\$Lap($^{1/\varepsilon}$,y_2):

|y1-y2|≤k ⇒ =.

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$`)~x`$_2$`:=$Lap(`$^{1/\varepsilon}$`,y`$_2$`):|y1-y2|`$\leq$`k ⇒ =`.

For every $\mathtt{m}_1,\mathtt{m}_2$ such that `P(m,m')` we have

`{x`$_1$`:=$Lap(`$^{1/\varepsilon}$`,y`$_1$`)}`$_{\mathtt{m}}$`=let a={Lap(`$^{1/\varepsilon}$`,y`$_1$`)}m in unit(m[x1←a])` and

`{x`$_1$`:=$Lap(`$^{1/\varepsilon}$`,y`$_1$`)}`$_{\mathtt{m}}$`=let a={Lap(`$^{1/\varepsilon}$`,y`$_1$`)}m in unit(m[x1←a])` we need to show that these two terms are in the ($k*\varepsilon$,0) lifting of =.

Correctness of Lap Rule

We can take:

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

and

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

Correctness of Lap Rule

We can take:

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

and

$\mu_R(m_1,m_2)=\mathbb{1}_{m1=m2}$*Lap($^{1}/_{\varepsilon}$, 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) $\Delta_{k^*\varepsilon}(\mu_L,\mu_R)\leq 0$

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:

$$\frac{\mathrm{Lap}(1/\varepsilon, \mathtt{m}(\mathtt{y}_1))(a)}{\mathrm{Lap}(1/\varepsilon, \mathtt{m}'(\mathtt{y}_2))(a)}$$

Correctness of Lap Rule

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

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

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:

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

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

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

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:

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

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

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

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

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

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 $y1=y2+k$

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

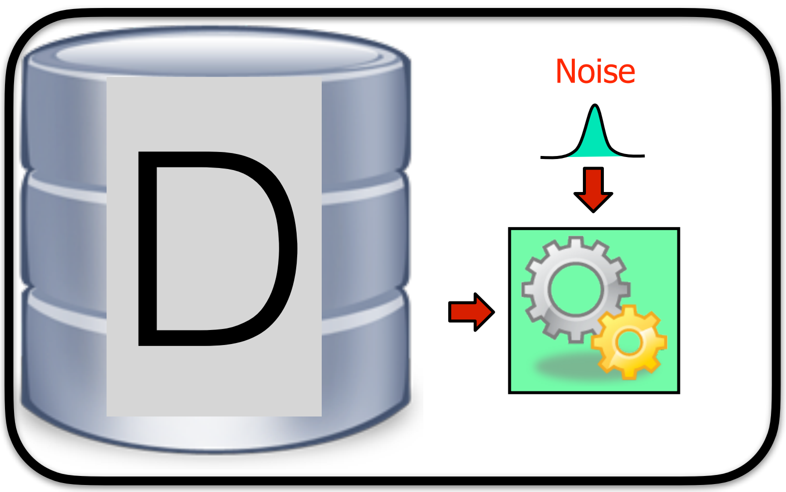
$$\leq \exp(\varepsilon|m(y2)-m(y2)+k|)$$

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

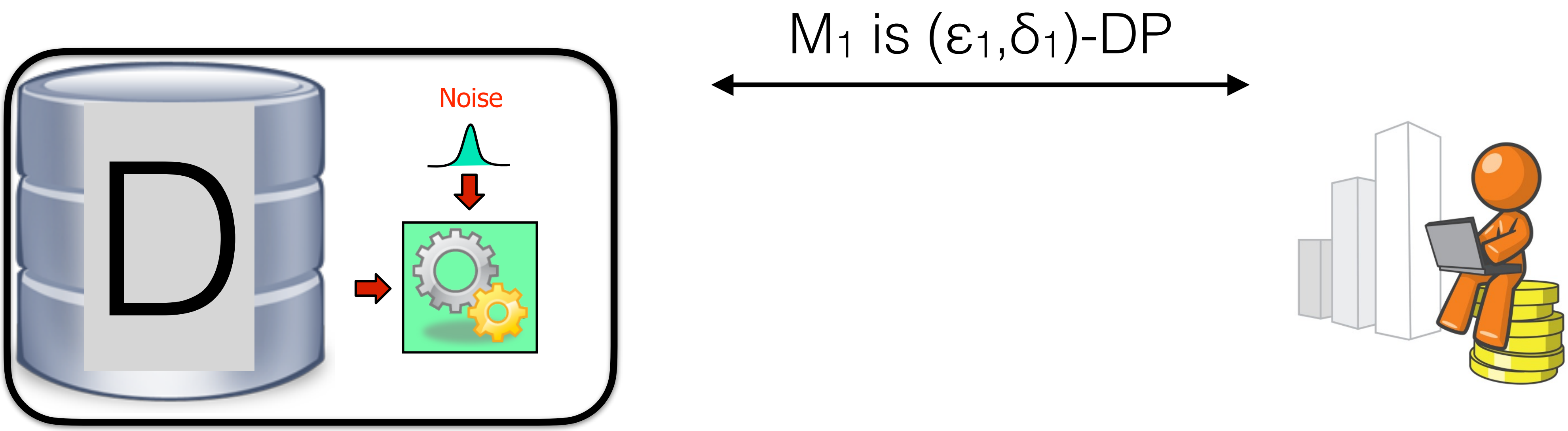
Releasing privately the mean of Some Data

```
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
```

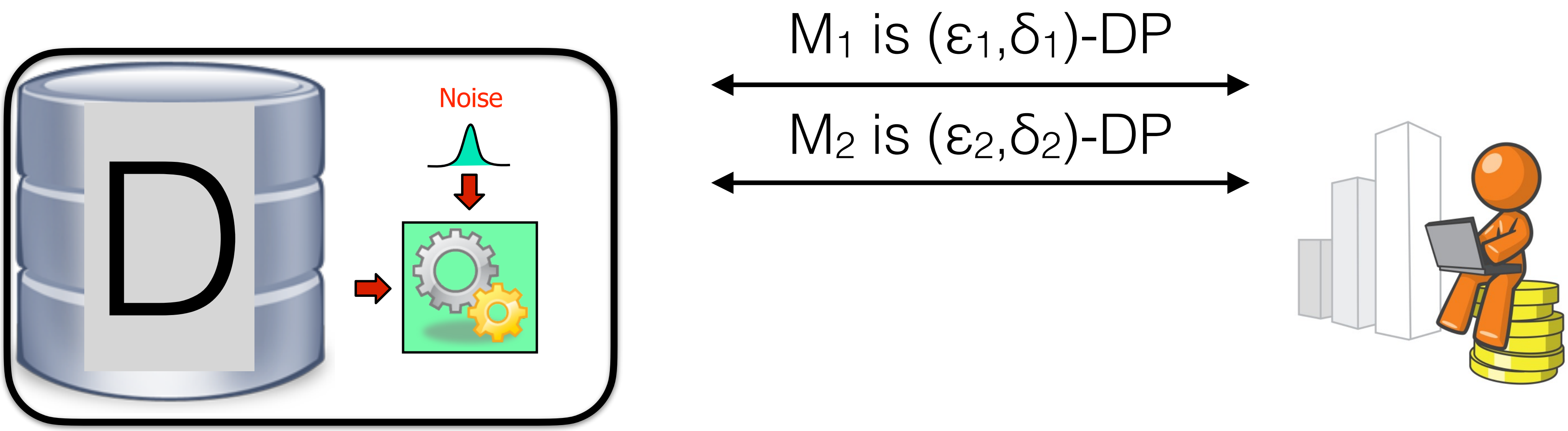
Composition



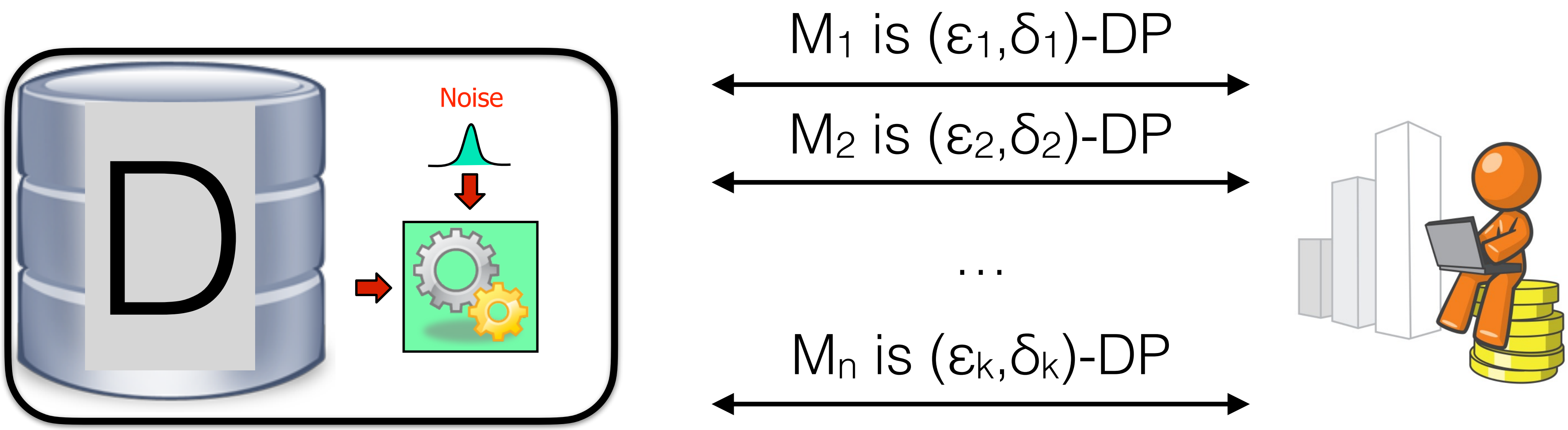
Composition



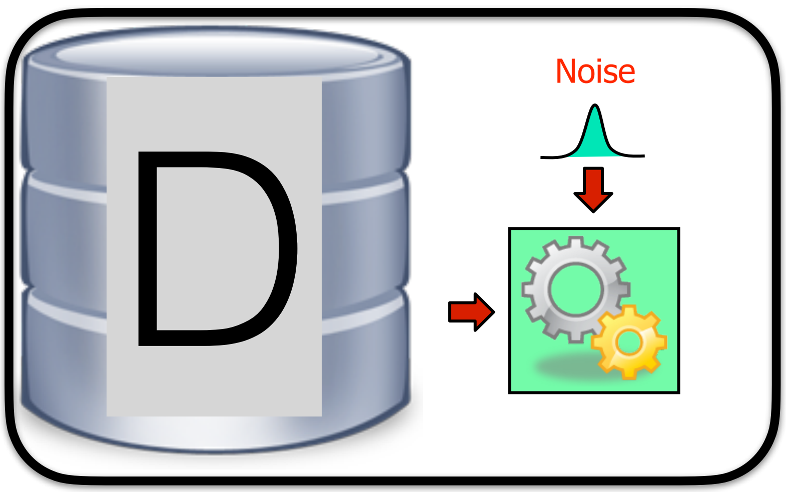
Composition



Composition



Composition



M_1 is (ε_1,δ_1)-DP

M_2 is (ε_2,δ_2)-DP

…

M_n is (ε_k,δ_k)-DP

The overall process is $(\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_k,\delta_1+\delta_2+\ldots+\delta_k)$-DP

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$\rightarrow R_1 x R_2$ 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`.

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
```

Parallel Composition

Let M_1:DB $\rightarrow$R be a (ε_1,δ_1)-differentially private program and M_2:DB $\rightarrow$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$\rightarrow$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

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

apRHL
awhile

$$P \wedge e\langle 1\rangle \leq 0 \Rightarrow \neg b1\langle 1\rangle$$

$$\frac{\vdash_{\varepsilon_k,\delta_k} c1 \sim c2 : P \wedge b1\langle 1\rangle \wedge b2\langle 2\rangle \wedge k = e\langle 1\rangle \wedge e\langle 1\rangle \leq n \Longrightarrow P \wedge b1\langle 1\rangle = b2\langle 2\rangle \wedge k < e\langle 1\rangle}{\vdash_{\sum\varepsilon_k,\sum\delta_k} \texttt{while } b1 \texttt{ do } c1 \sim \texttt{while } b2 \texttt{ do } c2 : P \wedge b1\langle 1\rangle = b2\langle 2\rangle \wedge e\langle 1\rangle \leq n \Longrightarrow P \wedge \neg b1\langle 1\rangle \wedge \neg b2\langle 2\rangle}$$

Properties of Differential Privacy

Some important properties

- Resilience to post-processing
- Group privacy
- Composition

Some important properties

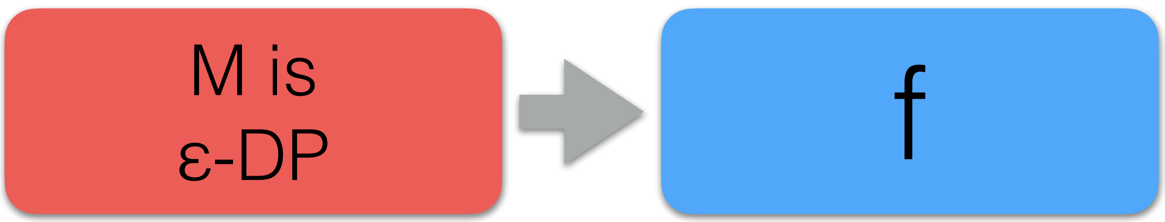
- Resilience to post-processing
- Group privacy
- Composition

We will look at them in the context of $(\varepsilon,0)$-differential privacy.

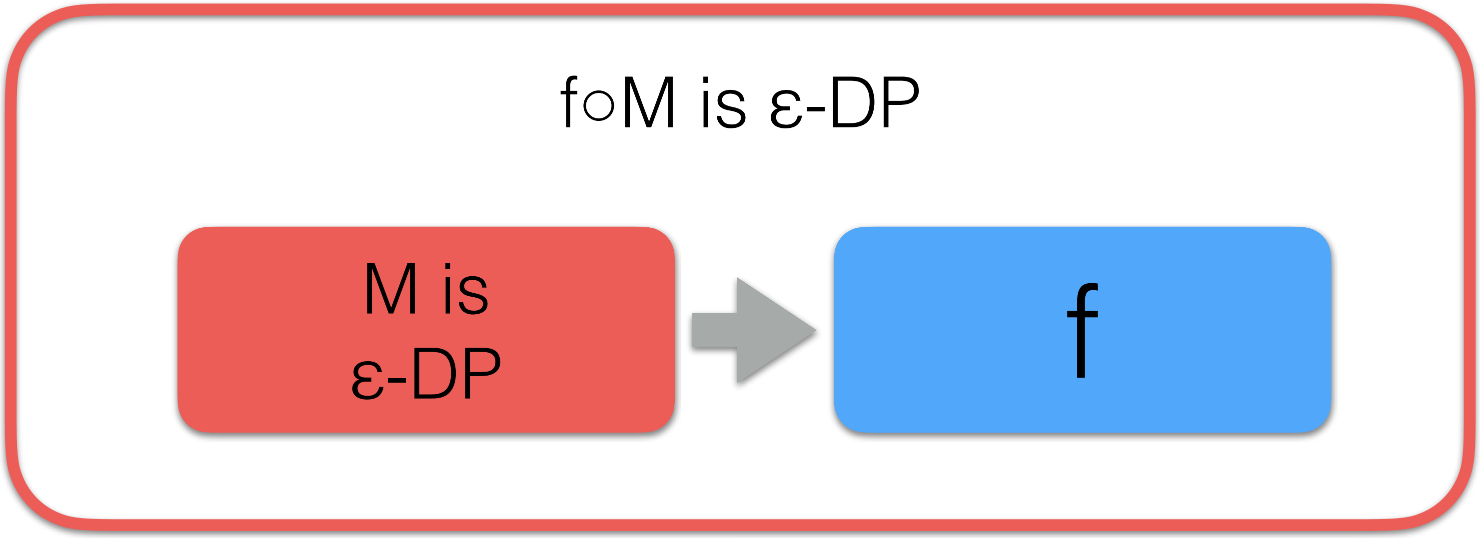
Resilience to Post-processing

M is
ε-DP

Resilience to Post-processing



Resilience to Post-processing



Resilience to Post-processing

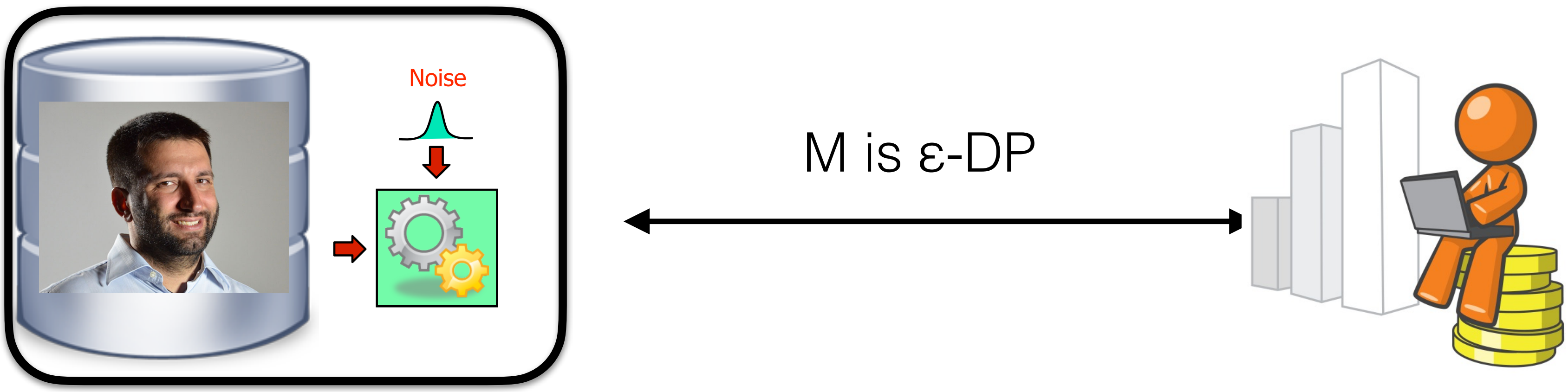
Question: Why is resilience to post-processing important?

Resilience to Post-processing

Question: Why is resilience to post-processing important?

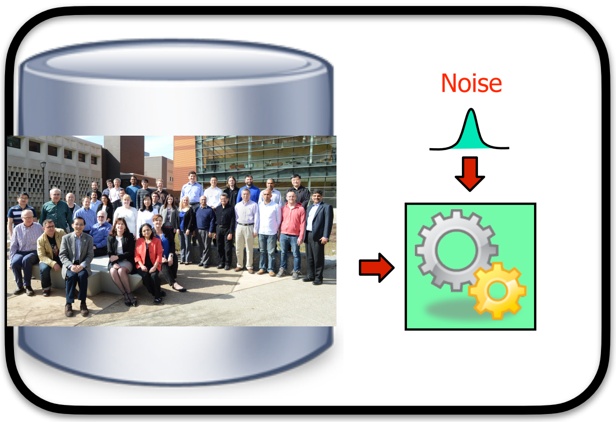
Answer: Because it is what allows us to publicly release the result of a differentially private analysis!

Group Privacy



$$\Pr[\mathcal{M}(D) = r] \leq e^{\epsilon} \Pr[\mathcal{M}(D') = r]$$

Group Privacy



M is kε-DP

$$\Pr[\mathcal{M}(D) \in S] \leq \exp(k\epsilon) \Pr[\mathcal{M}(D') \in S]$$

Group Privacy

Question: Why is group privacy important?

Group Privacy

Question: Why is group privacy important?

Answer: Because it allows to reason about privacy at different level of granularities!

Privacy Budget vs Epsilon

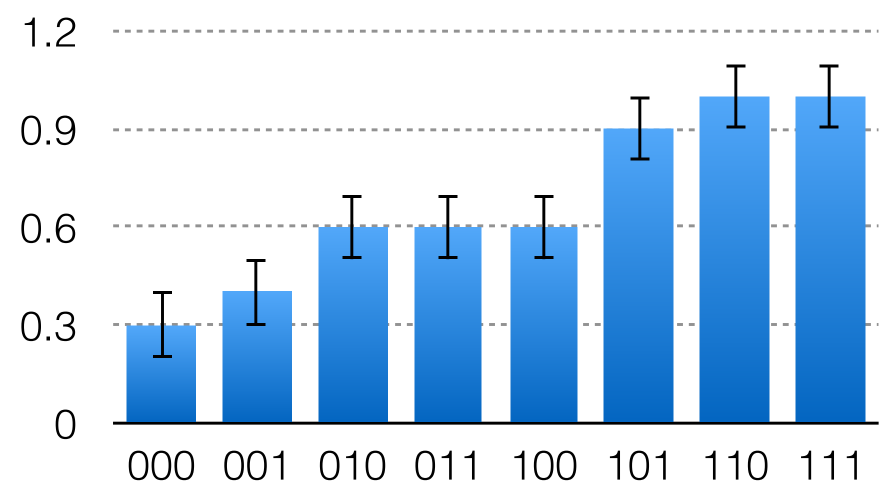
Sometimes is more convenient to think in terms of Privacy Budget: $\text{Budget} = \varepsilon_{global} - \sum \varepsilon_{local}$

Sometimes is more convenient to think in terms of epsilon: $\varepsilon_{global} = \sum \varepsilon_{local}$

Also making them uniforms is sometimes more informative.

$$\text{Budget} = \varepsilon_{global} - \varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4 - \varepsilon_5 - \varepsilon_6 - \varepsilon_7 - \varepsilon_8$$

$$\varepsilon_{global} = \varepsilon+\varepsilon+\varepsilon+\varepsilon+\varepsilon+\varepsilon+\varepsilon+\varepsilon=8\varepsilon$$



	D1	D2	D3
I1	0	0	0
I2	1	0	1
I3	0	1	0
I4	1	0	1
I5	0	0	0
I6	0	0	1
I7	1	1	0
I8	0	0	0
I9	0	1	0
I10	1	0	1
margin	$.4+Y_1$	$.3+Y_2$	$.4+Y_3$

$$\text{Budget} = \varepsilon_{global} - \varepsilon_1 - \varepsilon_2 - \varepsilon_3$$

$$\varepsilon_{global} = \varepsilon+\varepsilon+\varepsilon=3\varepsilon$$