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 ε, δ ≥ 0, a probabilistic query Q: X^n → R is (ε, δ)-differentially private iff for all adjacent database b_1, b_2 and for every S ⊆ R:

\[
\Pr[Q(b_1) ∈ S] ≤ \exp(ε)\Pr[Q(b_2) ∈ S] + δ
\]
c is differentially private if and only if for every \( m_1 \sim m_2 \) (extending the notion of adjacency to memories):

\[
\{c\}_{m_1} = \mu_1 \text{ and } \{c\}_{m_2} = \mu_2 \text{ implies } \Delta_{\varepsilon}(\mu_1, \mu_2) \leq \delta
\]
apRHL

Indistinguishability parameter

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

Precondition (a logical formula)

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:

$\{c_1\}_{m_1} = \mu_1$ and $\{c_2\}_{m_2} = \mu_2$ implies $Q_{\varepsilon, \delta^*}(\mu_1, \mu_2)$. 
**R- ( \( \epsilon, \delta \) ) -Coupling**

Given two distributions \( \mu_1 \in D(A) \), and \( \mu_2 \in D(B) \), we have an \( R-(\epsilon,\delta)\)-coupling between them, for \( R \subseteq A \times B \) and \( 0 \leq \delta \leq 1 \), \( \epsilon \geq 0 \), 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 \( \mu_L \) and \( \mu_R \) 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) \( \Delta_\epsilon(\mu_L, \mu_R) \leq \delta \)
Example of $R-(\varepsilon, \delta)$-Coupling

\[ R(a, b) = \{ a=b \} \]

\begin{align*}
\mu_1 & \\
00 & 0.25 \\
01 & 0.25 \\
10 & 0.25 \\
11 & 0.25 \\
\mu_2 & \\
00 & 0.20 \\
01 & 0.25 \\
10 & 0.25 \\
11 & 0.30 \\
\end{align*}

\begin{align*}
\mu_L & \\
00 & 0.25 \\
01 & 0.25 \\
10 & 0.25 \\
11 & 0.25 \\
\mu_R & \\
00 & 0.20 \\
01 & 0.25 \\
10 & 0.25 \\
11 & 0.30 \\
\end{align*}

\[ \Delta_{0.3}(\mu_L, \mu_R) = 0 \]
apRHL: skip rule

\[ \vdash_{0,0} \text{skip} \Rightarrow \text{skip} : P \Rightarrow P \]
Correctness of Skip Rule

To show this rule correct we need to show the validity of the \( \vdash_{0,0} \text{skip} \sim \text{skip}: P \Rightarrow P \).
Correctness of Skip Rule

\[ \vdash_{0,0} \text{skip} \rightarrow \text{skip} : P \Rightarrow P \]

To show this rule correct we need to show the validity of the \[ \vdash_{0,0} \text{skip} \rightarrow \text{skip} : P \Rightarrow P \].

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

\[ \vdash_{0,0} \text{skip \sim skip} : P \Rightarrow P \]
Correctness of Skip Rule

$$\vdash 0,0 \text{skip}\sim\text{skip}: P \Rightarrow P$$

<table>
<thead>
<tr>
<th>$\mu_L$</th>
<th>$m_1$</th>
<th>$m_2$</th>
<th>...</th>
<th>$m'$</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_1$</td>
<td>0</td>
<td>0</td>
<td>...</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$m_2$</td>
<td>0</td>
<td>0</td>
<td>...</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$m$</td>
<td>0</td>
<td>0</td>
<td>...</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Correctness of Skip Rule

\[ 0, 0 \vdash \text{skip} \sim \text{skip} : P \Rightarrow P \]

\[
\begin{array}{cccccc}
\mu_L & m_1 & m_2 & \ldots & m' & \ldots \\
m_1 & 0 & 0 & \ldots & 0 & 0 \\
m_2 & 0 & 0 & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
m & 0 & 0 & \ldots & 1 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{array}
\]

\[
\begin{array}{cccccc}
\mu_R & m_1 & m_2 & \ldots & m' & \ldots \\
m_1 & 0 & 0 & \ldots & 0 & 0 \\
m_2 & 0 & 0 & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
m & 0 & 0 & \ldots & 1 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{array}
\]
Correctness of Skip Rule

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

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) $\Delta_0(\mu_L, \mu_R) \leq 0$
\textbf{apRHL: Lap rule (simplified)}

\[ x_1 := \text{Lap}(1/\varepsilon, y_1) \]
\[ \sim \]
\[ \vdash \varepsilon, 0 \quad x_2 := \text{Lap}(1/\varepsilon, y_2) \]
\[ : \quad |y_1 - y_2| \leq 1 \quad \Rightarrow \quad = \]
The variance of the Laplace distribution is $\sigma^2 = \frac{b^2}{2}$.

The Laplace distribution centered in $0$ has the symmetric shape of two exponential distributions with symmetry axis in $0$. The parameter $b$ describes how "concentrated" the distribution is, see Figure 1.1 for two examples.

To ensure a bound on the privacy loss we need to calibrate the additive noise to the possible influence that a single individual can have on the result of the numeric query. This influence is captured by the notion of global sensitivity.

Definition 1.8 (Global sensitivity). The global sensitivity of a function $q : X^n \rightarrow \mathbb{R}$ is:

$$\text{gs}(q) = \max_{D, D' : D \neq D', |D| \leq 1} |q(D) - q(D')|$$

Intuitively, smaller the global sensitivity of a function is and less impact a single individual has on the result of the function. So, when the global sensitivity is small we can add less noise to provide the same protection. This is the intuition behind the Laplace mechanism.

We use the notation $\exp(c)$ for $e^c$ for making the formulas easier to read.

Following the literature on differential privacy we use here the term "mechanism", there this is used as a synonym of algorithm, program, etc. It doesn't have any other special meaning.

$b$ regulates the skewness of the curve,
Correctness of Lap Rule

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

\[ \vdash_{\varepsilon, 0} x_1 \triangleq \text{Lap} \left( \frac{1}{\varepsilon}, y_1 \right) \sim x_2 \triangleq \text{Lap} \left( \frac{1}{\varepsilon}, y_2 \right) : |y_1 - y_2| \leq 1 \Rightarrow =. \]
Correctness of Lap Rule

To show this rule correct we need to show the validity of
\[ \varepsilon, 0 x_1 := \text{Lap}(1/\varepsilon, y_1) \sim x_2 := \text{Lap}(1/\varepsilon, y_2) : |y_1 - y_2| \leq 1 \Rightarrow =. \]

For every \( m_1, m_2 \) such that \( P(m, m') \) we have
\[ \{ x_1 := \text{Lap}(1/\varepsilon, y_1) \}_m = \text{let } a = \{ \text{Lap}(1/\varepsilon, y_1) \}_m \text{ in unit}(m[x_1 \leftarrow a]) \text{ and} \]
\[ \{ x_2 := \text{Lap}(1/\varepsilon, y_2) \}_m' = \text{let } a = \{ \text{Lap}(1/\varepsilon, y_2) \}_m' \text{ in unit}(m'[x_2 \leftarrow a]) \] we need to show that these two terms are in the \((\varepsilon, 0)\) lifting of \( =. \)
Correctness of Lap Rule

We can take:
\[ \mu_L(m_1,m_2) = 1_{m_1=m_2} \ast \text{Lap}(1/\varepsilon, m(y_1))(a) \ast 1_{m_1(x_1)=a} \]
and
\[ \mu_R(m_1,m_2) = 1_{m_1=m_2} \ast \text{Lap}(1/\varepsilon, m'(y_2))(a) \ast 1_{m_1(x_2)=a} \]
Correctness of Lap Rule

We can take:
\[ \mu_L(m_1,m_2) = \mathbb{1}_{m_1=m_2} \cdot \text{Lap}\left(\frac{1}{\varepsilon}, m(y_1)\right)(a) \cdot \mathbb{1}_{m_1(x_1)=a} \]
and
\[ \mu_R(m_1,m_2) = \mathbb{1}_{m_1=m_2} \cdot \text{Lap}\left(\frac{1}{\varepsilon}, m'(y_2)\right)(a) \cdot \mathbb{1}_{m_1(x_2)=a} \]

We need to show:
1) \( \pi_1(\mu_L) = \text{let } a = \{ \text{Lap}\left(\frac{1}{\varepsilon}, y_1\right) \} m \text{ in unit}(m[x_1\leftarrow a]) \)
   and
   \( \pi_2(\mu_R) = \text{let } a = \{ \text{Lap}\left(\frac{1}{\varepsilon}, y_2\right) \} m \text{ in unit}(m[x_2\leftarrow a]) \)
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:

\[
\text{Lap}\left(\frac{1}{\varepsilon}, m(y_1)\right)(a) \\
\underline{\text{Lap}\left(\frac{1}{\varepsilon}, m'(y_2)\right)(a)}
\]
Correctness of Lap Rule

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

$$\frac{\text{Lap}\left(\frac{1}{\varepsilon}, m(y_1)\right)(a)}{\text{Lap}\left(\frac{1}{\varepsilon}, m'(y_2)\right)(a)} = \frac{\exp(-\varepsilon |m(y_1) - a|)}{\exp(-\varepsilon |m(y_2) - a|)}$$
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq 1$. 
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq 1$.

Let’s consider for example the case $y_1 = y_2 + 1$. 
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq 1$. Let's consider for example the case $y_1 = y_2 + 1$.

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

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

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

By the precondition we know $|y_1 - y_2| \leq 1$.

Let's consider for example the case $y_1 = y_2 + 1$

\[
\frac{\exp(-\varepsilon|m(y_2) + 1 - a|)}{\exp(-\varepsilon|m(y_2) - a|)} = \exp(\varepsilon|m(y_2) - a| - \varepsilon|m(y_2) + 1 - a|)
\]
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq 1$.

Let's consider for example the case $y_1 = y_2 + 1$

$$\frac{\exp(-\varepsilon |m(y_2) + 1 - a|)}{\exp(-\varepsilon |m(y_2) - a|)} = \exp(\varepsilon |m(y_2) - a| - \varepsilon |m(y_2) + 1 - a|) \leq \exp(\varepsilon |m(y_2) - m(y_2) + 1|)$$
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq 1$.

Let's consider for example the case $y_1 = y_2 + 1$

$$\frac{\exp(-\varepsilon \left| m(y_2) + 1 - a \right|)}{\exp(-\varepsilon \left| m(y_2) - a \right|)} = \exp(\varepsilon \left| m(y_2) - a \right| - \varepsilon \left| m(y_2) + 1 - a \right|) \leq \exp(\varepsilon \left| m(y_2) - m(y_2) + 1 \right|) = \exp(\varepsilon)$$
apRHL: More general Lap rule
(still restricted)

\[ x_1 := \$ \text{Lap}(1/\varepsilon, y_1) \]

\[ \vdash k^* \varepsilon, 0 \sim \]

\[ x_2 := \$ \text{Lap}(1/\varepsilon, y_2) \]

\[ : \ |y_1 - y_2| \leq k \Rightarrow = \]
Correctness of Lap Rule

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

\[ \vdash k^* \varepsilon, 0 \ x_1 := \text{Lap}(1/\varepsilon, y_1) \sim x_2 := \text{Lap}(1/\varepsilon, y_2) : \]

\[ |y_1 - y_2| \leq k \Rightarrow =. \]
Correctness of Lap Rule

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

$$\vdash k^* \varepsilon, 0 \ x_1 := \text{Lap}(\frac{1}{\varepsilon}, y_1) \sim x_2 := \text{Lap}(\frac{1}{\varepsilon}, y_2): \ |y_1 - y_2| \leq k \Rightarrow =.$$

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

$$\{x_1 := \text{Lap}(\frac{1}{\varepsilon}, y_1)\}_m = \text{let } a = \{\text{Lap}(\frac{1}{\varepsilon}, y_1)\}_m \text{ in unit}(m[x_1 \leftarrow a]) \text{ and }$$

$$\{x_1 := \text{Lap}(\frac{1}{\varepsilon}, y_1)\}_m = \text{let } a = \{\text{Lap}(\frac{1}{\varepsilon}, y_1)\}_m \text{ in unit}(m[x_1 \leftarrow a])$$

we need to show that these two terms are in the $(k^* \varepsilon, 0)$ lifting of $\Rightarrow$. 
Correctness of Lap Rule

We can take:

\[ \mu_L(m_1, m_2) = 1_{m_1 = m_2} * \text{Lap}(\frac{1}{\varepsilon}, m(y_1))(a) * 1_{m_1(x_1) = a} \]

and

\[ \mu_R(m_1, m_2) = 1_{m_1 = m_2} * \text{Lap}(\frac{1}{\varepsilon}, m'(y_2))(a) * 1_{m_1(x_2) = a} \]
We need to show:

1) \( \pi_1(\mu_L) = \text{let } a=\{\text{Lap}(1/\varepsilon, y_1)\}m \text{ in unit}(m[x_1 \leftarrow a]) \)
   and
   \( \pi_2(\mu_R) = \text{let } a=\{\text{Lap}(1/\varepsilon, y_2)\}m \text{ in unit}(m[x_2 \leftarrow a]) \)

2) \( (m_1, m_2) \in \Delta_k^* \varepsilon(\mu_L, \mu_R) \leq 0 \)
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:

\[
\text{Lap}\left(\frac{1}{\varepsilon}, m(y_1)\right)(a) \\
\text{Lap}\left(\frac{1}{\varepsilon}, m'(y_2)\right)(a)
\]
Correctness of Lap Rule

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

\[
\frac{\text{Lap}(\frac{1}{\varepsilon}, m(y_1))(a)}{\text{Lap}(\frac{1}{\varepsilon}, m'(y_2))(a)} = \frac{\exp(-\varepsilon |m(y_1) - a|)}{\exp(-\varepsilon |m(y_2) - a|)}
\]
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq k$. 
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq k$.

Let's consider for example the case $y_1 = y_2 + k$. 
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq k$.

Let’s consider for example the case $y_1 = y_2 + k$

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

To prove $\Delta_k^* \epsilon (\mu_L, \mu_R) \leq 0$ we can think about:

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

By the precondition we know $|y_1 - y_2| \leq k$.

Let’s consider for example the case $y_1 = y_2 + k$

$$\frac{\exp(-\epsilon |m(y_2) + k - a|)}{\exp(-\epsilon |m(y_2) - a|)} = \exp(\epsilon |m(y_2) - a| - \epsilon |m(y_2) + k - a|)$$
Correctness of Lap Rule

To prove $\Delta_k^\epsilon (\mu_L, \mu_R) \leq 0$ we can think about:

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

By the precondition we know $|y_1 - y_2| \leq k$.

Let's consider for example the case $y_1 = y_2 + k$

$$\frac{\exp(-\epsilon |m(y_2) + k - a|)}{\exp(-\epsilon |m(y_2) - a|)} = \exp(\epsilon |m(y_2) - a| - \epsilon |m(y_2) + k - a|) \leq \exp(\epsilon |m(y_2) - m(y_2) + k|)$$
Correctness of Lap Rule

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

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

By the precondition we know $|y_1 - y_2| \leq k$.

Let's consider for example the case $y_1 = y_2 + k$

\[
\frac{\exp(-\varepsilon |m(y_2) + k - a|)}{\exp(-\varepsilon |m(y_2) - a|)} = \frac{\exp(\varepsilon |m(y_2) - a|)}{\exp(\varepsilon |m(y_2) + k - a|)} \leq \exp(\varepsilon |m(y_2) - m(y_2) + k|) = \exp(k^* \varepsilon)
\]
Releasing privately the mean of Some Data

\[ \text{Mean}(d : \text{private data}) : \text{public real} \]

\[
i := 0;
\]

\[
s := 0;
\]

\[
\text{while } (i < \text{size}(d))
\]

\[
s := s + d[i]
\]

\[
i := i + 1;
\]

\[
z := \text{Lap}(\text{sens/eps}, (s/i))
\]

return z
Let $M_1: DB \rightarrow R_1$ be a $(\varepsilon_1, \delta_1)$-differentially private program and $M_2: DB \rightarrow R_2$ be a $(\varepsilon_2, \delta_1)$-differentially private program. Then, their composition $M_{1,2}: DB \rightarrow R_1 \times R_2$ 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

\[ \frac{\vdash \epsilon_1, \delta_1 c_1 \sim c_2 : P \Rightarrow R \quad \vdash \epsilon_2, \delta_2 c_1' \sim c_2' : R \Rightarrow S}{\vdash \epsilon_1 + \epsilon_2, \delta_1 + \delta_2 c_1 ; c_1' \sim c_2 ; c_2' : P \Rightarrow S} \]
Releasing partial sums

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

I am using the easycrypt notation here where $\text{Lap}(\text{eps},a)$ corresponds to adding to the value $a$ noise from the Laplace distribution with $b=1/\text{eps}$ and mean $\mu=0$. 
Let \( M_1 : DB \rightarrow R \) be a \((\varepsilon_1, \delta_1)\)-differentially private program and \( M_2 : DB \rightarrow R \) be a \((\varepsilon_2, \delta_2)\)-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

\[
M_{1,2}(D) = (M_1(D_1), M_2(D_2))
\]

is \((\max(\varepsilon_1, \varepsilon_2), \max(\delta_1, \delta_2))\)-differentially private.
Probabilistic Relational Hoare Logic
Composition

\[ \vdash \varepsilon_1, \delta_1 c_1 \sim c_2 : P \Rightarrow R \quad \vdash \varepsilon_2, \delta_2 c_1' \sim c_2' : R \Rightarrow S \]

\[ \vdash \varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2 c_1 ; c_1' \sim c_2 ; c_2' : P \Rightarrow S \]
Releasing partial sums

\textbf{DummySum}(d : \{0,1\} list) : real list

\begin{verbatim}
  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
\end{verbatim}
apRHL

awhile

\[ P \land e<1> \leq 0 \Rightarrow \neg b1<1> \]

\[ \vdash \sum_{\varepsilon_k, \delta_k} c1 \sim c2 : P \land b1<1> \land b2<2> \land k = e<1> \land e<1> \leq n \Rightarrow P \land b1<1> = b2<2> \land k < e<1> \]

while b1 do c1 \sim while b2 do c2

\[ \vdash \sum_{\varepsilon_k, \delta_k} : P \land b1<1> = b2<2> \land e<1> \leq n \Rightarrow P \land \neg b1<1> \land \neg b2<2> \]