Karlsruhe Institute of Technology

PRIVACY AND SECURITY

¿Como pueden las matemáticas proteger tu privacidad?

PEREGRINANDO: Traxectorias internacionais nas matemáticas e na física

Patricia Guerra-Balboa | 20 de Diciembre 2024

Primeros pasos

Matemáticas en la USC

- Grado & Máster en Matemáticas
- Especialización en Geometría Algebraica
- ¿Y ahora qué?

Primeros pasos

Matemáticas en la USC

- Grado & Máster en Matemáticas
- Especialización en Geometría Algebraica
- ¿Y ahora qué?

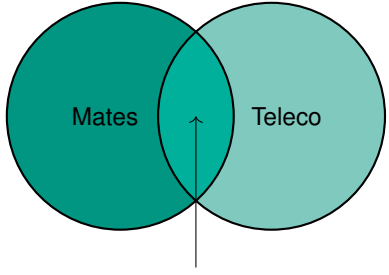
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Departamento de Ingeniería Telemática

Primeros pasos

Matemáticas en la USC

- Grado & Máster en Matemáticas
- Especialización en Geometría Algebraica
- ¿Y ahora qué?

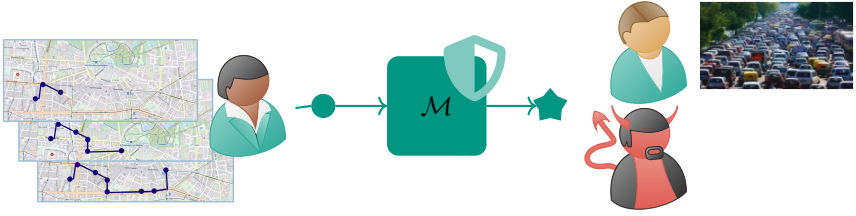


CRIPTOGRAFÍA

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

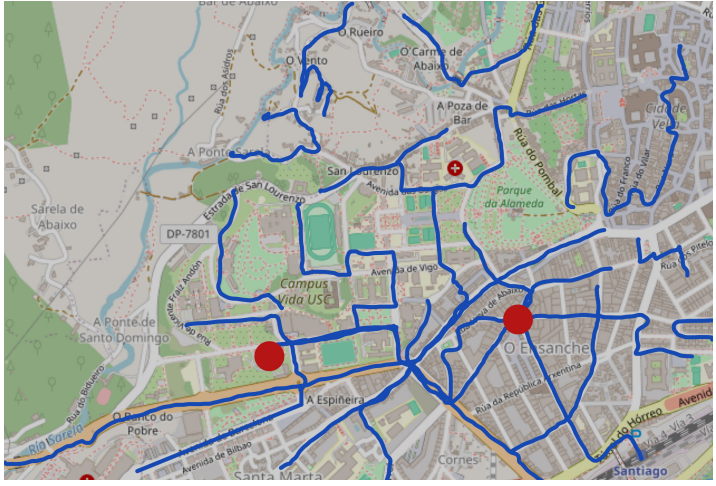
Departamento de Ingeniería Telemática

Predecir un atasco sin saber dónde está la gente

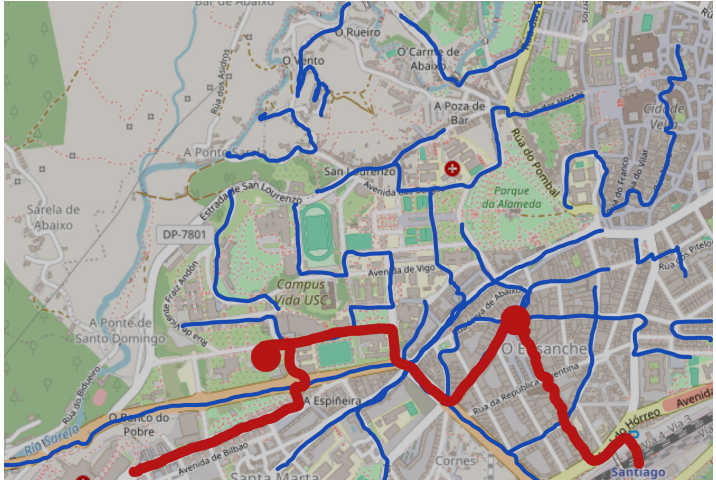


Pseudoanonimización

Pseudoanonimización



Pseudoanonimización

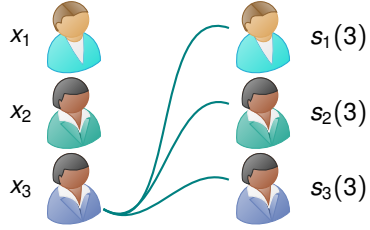


Multiparty Computation y la distribución de secretos

Multiparty Computation y la distribución de secretos

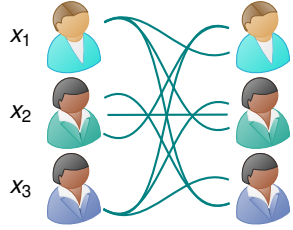
$$x_3 = s_1(3) + s_2(3) + s_3(3)$$

Multiparty Computation y la distribución de secretos



$$x_3 = s_1(3) + s_2(3) + s_3(3)$$

Multiparty Computation y la distribución de secretos



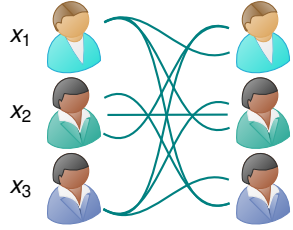
$$s_1(3) + s_1(2) + s_1(1) = S_1$$

$$s_2(3) + s_2(2) + s_2(1) = S_2$$

$$s_3(3) + s_3(2) + s_3(1) = S_3$$

$$x_3 = s_1(3) + s_2(3) + s_3(3)$$

Multiparty Computation y la distribución de secretos



$$s_1(3) + s_1(2) + s_1(1) = S_1$$

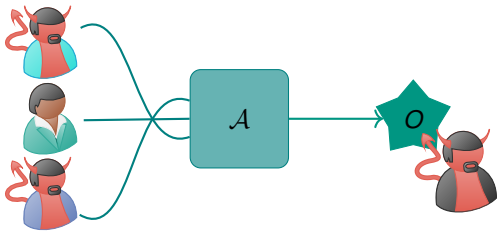
$$s_2(3) + s_2(2) + s_2(1) = S_2$$

$$s_3(3) + s_3(2) + s_3(1) = S_3$$

$$x_3 = s_1(3) + s_2(3) + s_3(3)$$

x_3 x_2 x_1 X

Pero . . . ¿y si hay usuarios corruptos?



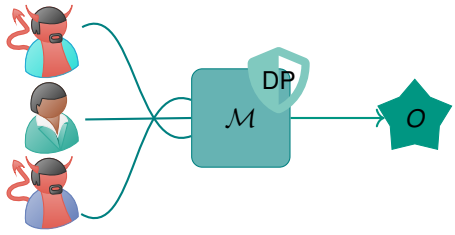
Si $O = 1 \Rightarrow$ Alice está en Rúa Romero Donallo

Si $O = 0 \Rightarrow$ Alice no está ahí

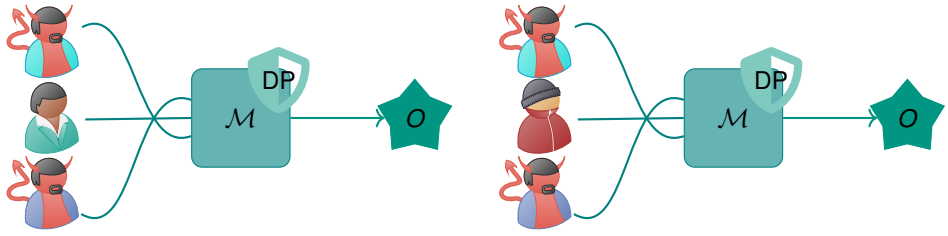
Empieza mi doctorado

Mathematical Foundations of Differential Privacy with Applications to Trajectory Data

Privacidad diferencial

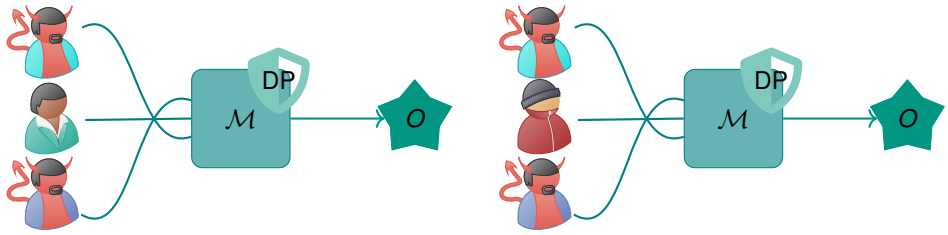


Privacidad diferencial



Privacidad diferencial

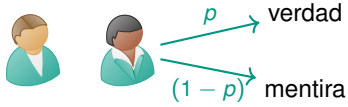
$$\Pr(O|\mathit{Alice}) \leq e^{\varepsilon} \Pr(O|\mathit{Bob})$$



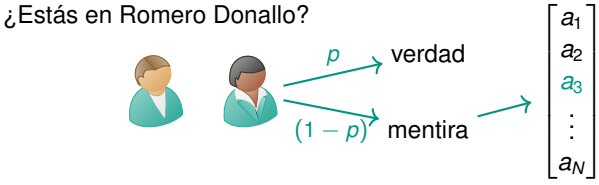
- $\Pr(\mathcal{M}(D, z_1) = O) \leq e^{\varepsilon} \Pr(\mathcal{M}(D, z_2) = O)$ (o función de densidad)
- El presupuesto de privacidad ε controla la indistinguibilidad entre cualquier par de entradas z_1, z_2

Ejemplo de protocolo DP: Randomized Response

¿Estás en Romero Donallo?

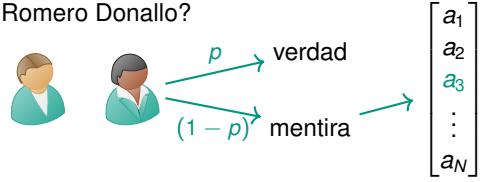


Ejemplo de protocolo DP: Randomized Response



Ejemplo de protocolo DP: Randomized Response

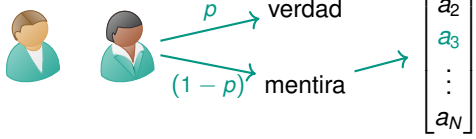
¿Estás en Romero Donallo?



$$c = \sum_{i=1}^{n} a_i$$

Ejemplo de protocolo DP: Randomized Response

¿Estás en Romero Donallo?

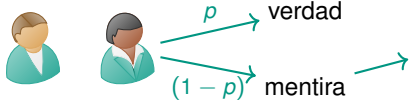


$c = \sum_{i=1}^{n} a_i \longrightarrow \tilde{n} = \frac{c-(1-p)}{N(2p-1)}$

Estimador de máxima verosimilitud (MLE)

Ejemplo de protocolo DP: Randomized Response

¿Estás en Romero Donallo?



$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_N \end{bmatrix}$$

$$c = \sum_{i=1}^{n} a_i \longrightarrow \tilde{n} = \frac{c-(1-p)}{N(2p-1)}$$

Estimador de máxima verosimilitud (MLE)

Privacidad

El Protocolo de Respuesta Aleatoria (RR) es ε-DP con

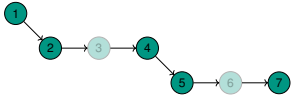
$$\varepsilon \leq \max \frac{\Pr(\mathcal{M}(x) = z)}{\Pr(\mathcal{M}(y) = z)} = \frac{p}{1-p}$$

Utilidad

$\mathbb{E}(\tilde{n}) = n$ y la varianza tiende a cero:

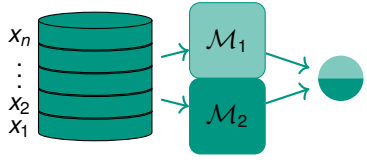
$$\mathrm{Var}(\tilde{n}) = \frac{1}{N}\left(\frac{1}{16(p-0.5)^2} - (n-0.5)^2\right) \to 0$$

Nuestra investigación



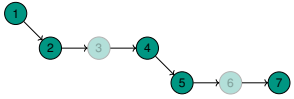
Algoritmos LDP para streaming

Resistencia frente a ataques



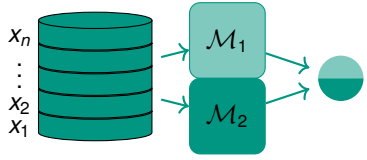
Propiedades de composición

Nuestra investigación



Algoritmos LDP para streaming

Resistencia frente a ataques



Propiedades de composición

Resumiendo. . .

Esta es mi trayectoria y espero que ayude a proteger la vuestra.