Elastic (indistinguishability) metrics for Location Privacy

Marco Stronati
marco@stronati.org
joint work with
K. Chatzikokolakis and C. Palamidessi

Scope

Privacy for LBS

Reducing accuracy
Goal: limited semantic inference
(not anonimity)

Utility

f(accuracy)

Privacy Definition

Mechanism

$$x \longrightarrow \mathcal{M} \longrightarrow z$$

Privacy Definition

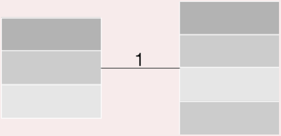
Mechanism

$$\color{blue}{x} \quad \longrightarrow \quad \mathcal{M} \quad \longrightarrow \quad \color{red}{z}$$

DP: Differential Privacy

$$P[z \mid x] \leq e^{\epsilon} P[z \mid x'] \qquad \forall x, x'.\ x \sim x'$$

[Dwork, McSherry, Nissim, Smith: Calibrating noise to sensitivity in private data analysis. TCC'06]



Privacy Definition

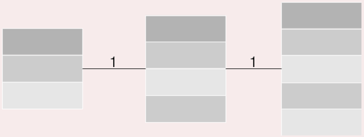
Mechanism

$$x \longrightarrow \mathcal{M} \longrightarrow z$$

DP: Differential Privacy

$$P[z \mid x] \leq e^{\epsilon} P[z \mid x'] \qquad \forall x, x'.\ x \sim x'$$

[Dwork, McSherry, Nissim, Smith: Calibrating noise to sensitivity in private data analysis. TCC'06]



Privacy Definition

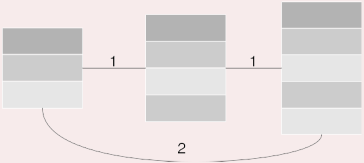
Mechanism

$$x \longrightarrow \mathcal{M} \longrightarrow z$$

DP: Differential Privacy

$$P[z \mid x] \leq e^{\epsilon} P[z \mid x'] \qquad \forall x, x'.\ x \sim x'$$

[Dwork, McSherry, Nissim, Smith: Calibrating noise to sensitivity in private data analysis. TCC'06]



Privacy Definition

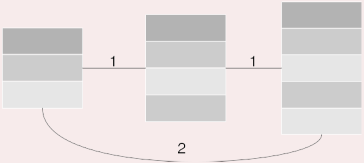
Mechanism

$$x \longrightarrow \mathcal{M} \longrightarrow z$$

DP: Differential Privacy

$$P[z \mid x] \leq e^{\epsilon \cdot d_H(x,x')} P[z \mid x'] \qquad \forall x, x'.\ x \sim x'$$

[Dwork, McSherry, Nissim, Smith: Calibrating noise to sensitivity in private data analysis. TCC'06]



Privacy Definition

Mechanism

$$x \longrightarrow \mathcal{M} \longrightarrow z$$

DP: Differential Privacy

$$P[z \mid x] \leq e^{\epsilon \cdot d_H(x,x')} P[z \mid x'] \qquad \forall x, x'.\ x \sim x'$$

[Dwork, McSherry, Nissim, Smith: Calibrating noise to sensitivity in private data analysis. TCC'06]

$d_{\mathcal{X}}$-privacy

$$P[z \mid x] \leq e^{d_{\mathcal{X}}(x,x')} P[z \mid x'] \qquad \forall x, x'$$

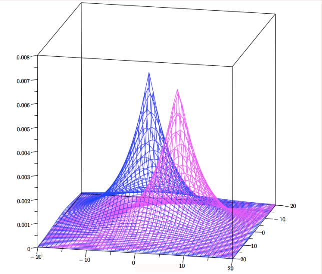
[Chatzikokolakis, Andres, Bordenabe, Palamidessi: Broadening the Scope of Differential Privacy Using Metrics. PETS'13]

Geo-indistinguishability

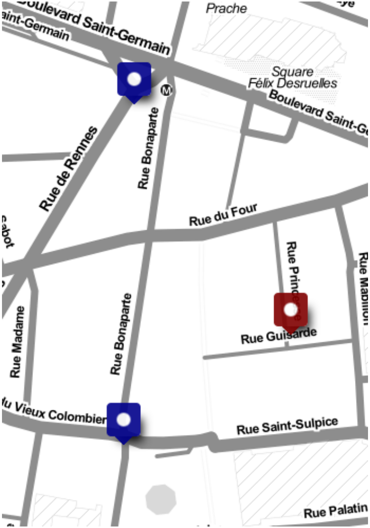
Metric: scaled Euclidean

$$d_{\mathcal{X}}(x, x') = \epsilon \cdot d_E(x, x')$$

Mechanism: Planar Laplacian



[Andrés, Bordenabe, Chatzikokolakis, Palamidessi: Geo-indistinguishability: differential privacy for location-based systems. CCS'13]



Family picture

$d_{\mathcal{X}}$-privacy

Differential Privacy

geo-indistinguishability

Family picture

$d_{\mathcal{X}}$-privacy

Differential Privacy

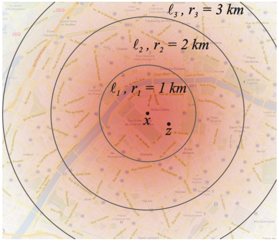
geo-indistinguishability
OptQL
Predictive

(In)Distinguishability Metric

What is it that you want to be
similar to?
(how much?)

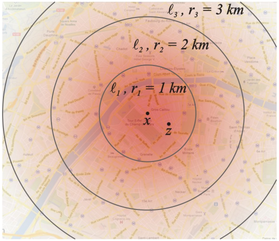
Euclidean Metric

- Space is privacy
- ϵ tunes how much



Euclidean Metric

- Space is privacy
- ϵ tunes how much



Requirement

I want to be indistinguishable from a certain amount of space.

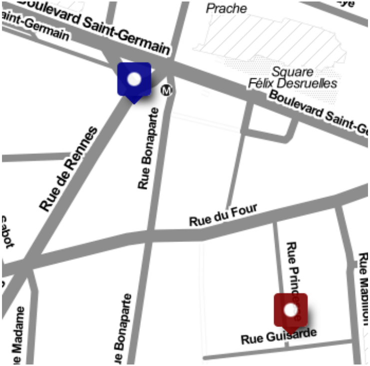
$$req(l)$$

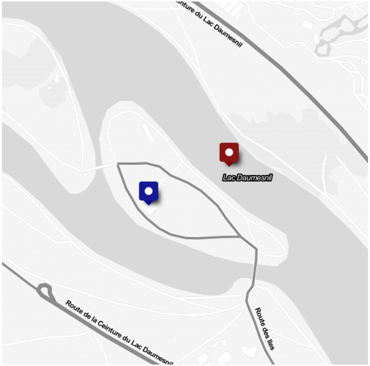
Problems

- Space is not necessarily privacy...
- Different areas offer different level of privacy

Problems

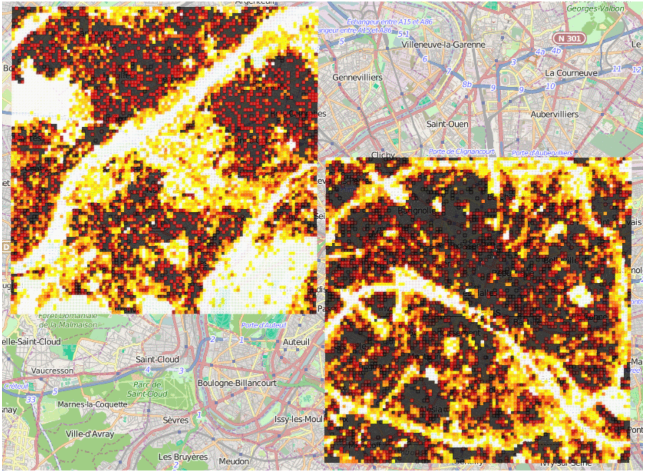
- Space is not necessarily privacy...
- Different areas offer different level of privacy





OSM enriched Grid

`OpenStreetMap`: buildings + (POIs x 3)



Privacy Requirement

Requirement

I want to be indistinguishable from a certain amount of privacy mass.

We use a quadratic curve (much like for space).

Building a metric satisfying the requirement

Graph-based algo:

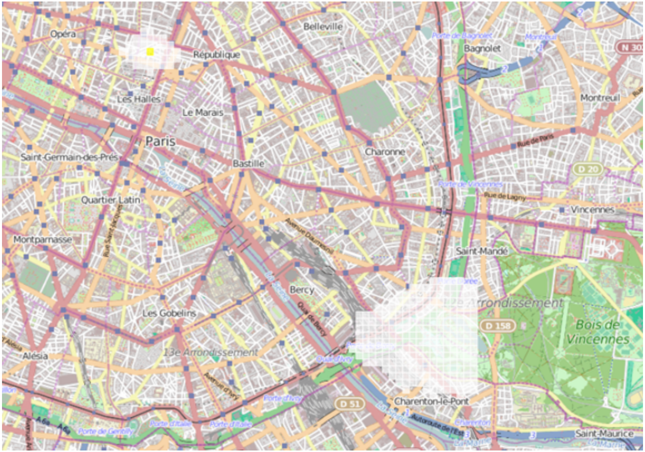
- start with a disconnetted graph
- interate over all nodes
  - compute `mass`
  - add an edge with $l = req^{-1}(\texttt{mass})$
- we stop at $l^{\top}$

Exponential Mechanism

$$P[z \mid x] \;\sim\; e^{-d_{\mathcal{X}}(x,z)}$$

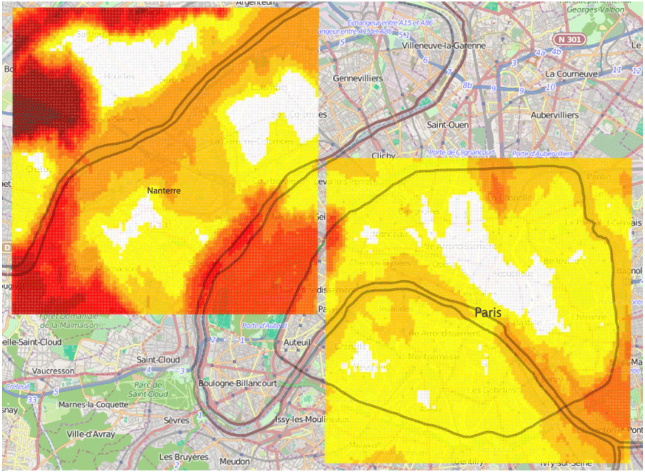
Exponential Mechanism

$$P[z \mid x] \sim e^{-d_{\mathcal{X}}(x,z)}$$



Exponential Mechanism

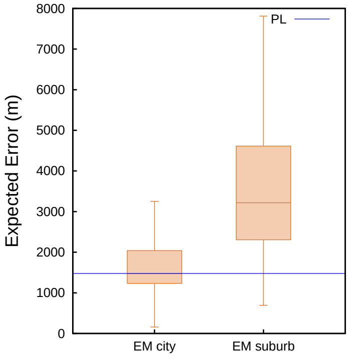
$$P[z \mid x] \ \sim \ e^{-d_{\mathcal{X}}(x,z)}$$

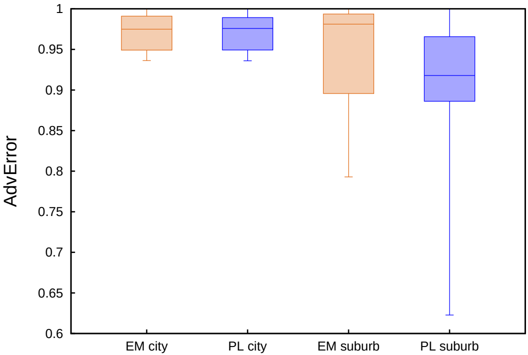


Evaluation

- Comparison with geo-indistinguishability
- Fixed Utility as Expected Error
- Compare Privacy as Adversarial Error
- Gowalla and Brightkite datasets

[Shokri, Theodorakopoulos, Boudec, Hubaux. Quantifying location privacy. S&P'11]





Fences

- linear growth of epsilon
- fences for recurrent places
- achieve "better privacy" consuming less ϵ

$$d_F(x,x') = \begin{cases} d_{\mathcal{X}}(x,x') & x,x' \notin F \\ 0 & x,x' \in F \\ \infty & o.w. \end{cases}$$

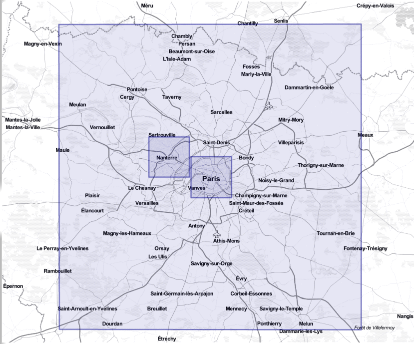
On the practicality of our method

Preprocessing

- query osm (highly parallel)
- normalize
- add fences
- build metric (sequential)

On the phone

- download portion of the map
- compute pdf
- draw



Tiled Mechanism

Use different ϵ in a private way.