Testing Privacy

Sofya Raskhodnikova
Penn State University

Joint work with Kashyap Dixit (Penn State), Madhav Jha (Penn State), Abharadeep Thakurta (Penn State → Stanford + MSR)
Testing Privacy

Let my “privacy preserving” program access your database

Does this program really preserve privacy?

Program $f$

$\text{Database Curator}$

$\text{Database}$

User/Attacker

$\text{Does this program really preserve privacy?}$

$\text{Let my “privacy preserving” program access your database}$

$f(\text{Database})$/Access Denied
Our Contributions

• The notion of a privacy tester
• A connection between testing a variant of differential privacy and property testing if a function is Lipschitz
• An efficient tester for the Lipschitz property w.r.t. a product distribution over domain \( \{0,1\}^n \)
• A privacy reconstructor based on a privacy tester
Lipschitz Functions

Two datasets $x, x'$ are neighbors if they differ in one person’s data.

A function $f$ is $c$-Lipschitz if for all neighboring datasets $x$ and $x'$,

$$|f(x) - f(x')| \leq c$$
Differential Privacy [Dwork McSherry Nissim Smith 06]
An algorithm $A$ is $\alpha$-differentially private if
• for all neighboring datasets $x, x'$ and
• for all subsets $Y \subseteq \text{Range}(A)$
\[
\frac{\Pr[A(x) \in Y]}{\Pr[A(x') \in Y]} \leq e^\alpha
\]
Differential Privacy [Dwork McSherry Nissim Smith 06]

An algorithm $A$ with discrete range is $\alpha$-differentially private if

- for all neighboring datasets $x, x'$ and
- for all values $y \in \text{Range}(A) = \{1, \ldots, r\}$

$$\frac{\Pr[A(x) = y]}{\Pr[A(x') = y]} \leq e^\alpha$$
Differential Privacy and the Lipschitz Property

Differential Privacy [Dwork McSherry Nissim Smith 06]

An algorithm $A$ with discrete range is $\alpha$-differentially private if

- for all neighboring datasets $x, x'$ and
- for all values $y \in \text{Range}(A) = \{1, \ldots, r\}$
  \[
  \frac{\Pr[A(x) = y]}{\Pr[A(x') = y]} \leq e^\alpha
  \]

Key Observation:

Algorithm $A$ is $\alpha$-differentially private

\[\Downarrow\]

for all $y \in \text{Range}(A)$, functions $f_y(x) = \ln(\Pr[A(x) = y])$ are $\alpha$-Lipschitz
Verifying if $f$ is $c$-Lipschitz?

• Undecidable
  
  if $f$ is given by a TM

• NP-hard
  
  if $f$ is given by a circuit
  – even for finite domains

Goal: do it approximately
Testing if a Function is $c$-Lipschitz

Property Testing model was defined by [Rubinfeld Sudan 96, Goldreich Goldwasser Ron 98]

- $\text{dist}(f) = \text{fraction of inputs on which } f \text{ differs from closest Lipschitz function}$

- $f$ is $\varepsilon$-far from Lipschitz if $\text{dist}(f) \geq \varepsilon$

Efficient Lipschitz testers [Jha Raskhodnikova 11, Chakrabarty Seshadhri 13]
Testing if a Function is $c$-Lipschitz

Property Testing model was defined by

$\varepsilon, c$ ▼

Lipschitz Tester

Function $f$

Accept with $\Pr \geq 2/3$ if $f$ is $c$-Lipschitz.

Reject with $\Pr \geq 2/3$ if $f$ is $\varepsilon$-far from $c$-Lipschitz.

$\text{dist}(f) =$ fraction of inputs on which $f$ differs from closest Lipschitz function $= \min_{\text{Lipschitz } g} \Pr[f(x) \neq g(x)]$

• $f$ is $\varepsilon$-far from Lipschitz if $\text{dist}(f) \geq \varepsilon$.  

[Rubinfeld Sudan 96, Goldreich Goldwasser Ron 98]
Testing if a Function is $c$-Lipschitz

Property Testing model was defined by [Rubinfeld Sudan 96, Goldreich Goldwasser Ron 98]

\[ \text{dist}(\Pi f) = \frac{\text{fraction of inputs on which } f \text{ differs from closest Lipschitz function}}{\min_{\text{Lipschitz } g} \Pr_x[f(x) \neq g(x)]} \]

• More generally, $\text{dist}_\Pi(f, g) = \min_{\text{Lipschitz } g} \Pr_{x \sim \Pi}[f(x) \neq g(x)]$

• $f$ is $\varepsilon$-far from Lipschitz if $\text{dist}_\Pi(f) \geq \varepsilon$.

This work: efficient Lipschitz testers w.r.t. product distributions over $\{0,1\}^n$
Algorithm $A$ is $(\alpha, \epsilon')$-DPTD w.r.t. distribution $\Pi$ on datasets if there exists a set $\text{Bad}$ such that $\Pr_{x \sim \Pi} [x \in \text{Bad}] \leq \epsilon'$, and for all $y \in \text{Range}(A)$, the functions $f_y(x) = \ln(\Pr[A(x) = y])$ are $\alpha$-Lipschitz on Domain\Bad.
Differential Privacy on Typical Datasets (DPTD)

- Related to a variant of DP in [Bhaskar Bhowmick Goyal Laxman Thakurta 11]

Algorithm $A$ is $(\alpha, \epsilon')$-DPTD w.r.t. distribution $\Pi$ on datasets if there exists a set $\text{Bad}$ such that $\Pr_{x \sim \Pi} [x \in \text{Bad}] \leq \epsilon'$, and for all $y \in \text{Range}(A)$, functions $f_y(x) = \ln(\Pr[A(x) = y])$ are $\alpha$-Lipschitz on Domain \setminus \text{Bad}.

\[
\frac{\Pr[A(x) = y]}{\Pr[A(x') = y]} \leq e^{\alpha \cdot \text{Ham}(x,x')}
\]
Privacy Tester

If algorithm $A$ is $\alpha$-differentially private then

all functions $f_y$ are $\alpha$-Lipschitz.
Privacy Tester

If algorithm $A$ is not $(\alpha, \epsilon')$-DPTD then some $f_y$ is $\epsilon$-far from $\alpha$-Lipschitz for $\epsilon = \epsilon' / |Range(A)|$. 
Privacy Reconstructor

Algorithm A → Privacy Tester → Output A(x)

Distribution Π on datasets → Lipschitz Tester → YES → α, ε'

$ f_y $
Privacy Reconstructor

Algorithm A

$f_y$

Distribution $\Pi$ on datasets

$\alpha, \epsilon'$

Access Denied

NO

Lipschitz Tester

Privacy Tester
Privacy Reconstructor

Given $A$, privacy reconstructor transforms it into $A'$:

- **(privacy)** $A'$ is *differentially private on typical datasets* (DPTD)

- **(utility)** If $A$ is differentially private then output distributions of $A$ and $A'$ are identical