Separating Computational and Statistical Differential Privacy in the Client-Server Model

Mark Bun   Yi-Hsiu Chen   Salil Vadhan

CS@Princeton   SEAS@Harvard   SEAS/CRCS@Harvard

November 2, 2016

Overview

- Differential Privacy (DP)
- Computational Differential Privacy (CDP)
- Previous Work & Main Contributions
- Sketch Result: Separation of CDP and DP
- Conclusion

Differential Privacy (Client-Server Setting)

Database: D

Name	Age	Height	Smoke
Alice	13	147	Y
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

Analyst

Differential Privacy (Client-Server Setting)

Database: D

Name	Age	Height	Smoke
Alice	13	147	Y
Charlie	27	176	N
⋮	⋮	⋮	⋮
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xleftarrow{q}$ $\xrightarrow{M(D,q)}$ Analyst

Differential Privacy (Client-Server Setting)

Database: D

Name	Age	Height	Smoke
Alice	13	147	Y
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

Differential Privacy (Client-Server Setting)

Database: D

Name	Age	Height	Smoke
Alice	13	147	Y
Charlie	27	176	N
⋮	⋮	⋮	⋮
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
⋮	⋮	⋮	⋮
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

distribution of $M(D) \approx$ distribution of $M(D')$

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

M is (ε, δ)-differentially private if $\forall\ D \sim D'$ and output set T,

$$\boxed{\Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

[Dwork, McSherry, Nissim, Smith '06]

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
⋮	⋮	⋮	⋮
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

M is (ε, δ)-differentially private if $\forall\ D \sim D'$ and output set T,

$$\boxed{\Pr[M(D) \in T] \leq \underset{\substack{\wr\wr \\ 1+\varepsilon}}{e^{\varepsilon}} \Pr[M(D') \in T] + \delta}$$

[Dwork, McSherry, Nissim, Smith '06]

$1 + \varepsilon$ (ε: small constant), (δ: negligible)

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

M is (ε, δ)-differentially private if $\forall\ D \sim D'$ and output set T,

$$\boxed{\Pr[M(D) \in T] \le e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

[Dwork, McSherry, Nissim, Smith '06]

$\wr$

$1 + \varepsilon$ (ε: small constant), (δ: negligible)

Example: Estimate how many people smoke (in D)

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

M is (ε, δ)-differentially private if $\forall\ D \sim D'$ and output set T,

$$\boxed{\Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

[Dwork, McSherry, Nissim, Smith '06]

$\wr$

$1 + \varepsilon$ (ε: small constant), (δ: negligible)

Example: Estimate how many people smoke (in D)

$$M(D) = \text{true answer } + \text{Noise}(O(1/\varepsilon))$$

Differential Privacy (Client-Server Setting)

Database: D'

Name	Age	Height	Smoke
Bob	15	168	N
Charlie	27	176	N
⋮	⋮	⋮	⋮
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

M is (ε, δ)-differentially private if $\forall\ D \sim D'$ and output set T,

$$\boxed{\Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

[Dwork, McSherry, Nissim, Smith '06]

$\wr$

$1 + \varepsilon$ (ε: small constant), (δ: negligible)

Example: Estimate how many people smoke (in D)

$$M(D) = \text{true answer } + \text{Noise}(O(1/\varepsilon))$$

Privacy vs. Utility

Differential Privacy Results

Algorithms:

- Histogram [DMNS06]
- Exponential Mechanism [MT07]
- Synthetic Data [BLR08]
- Private Multiplicative Weights [HR10]
- Boosting [DRV10]
- Private Learning [KLNRS08]
- Statistical Estimation [Smith10]
- Streaming [DNPR10, MMNW11]
- ...

Differential Privacy Results

Algorithms:

- Histogram [DMNS06]
- Exponential Mechanism [MT07]
- Synthetic Data [BLR08]
- Private Multiplicative Weights [HR10]
- Boosting [DRV10]
- Private Learning [KLNRS08]
- Statistical Estimation [Smith10]
- Streaming [DNPR10, MMNW11]
- ...

Lower Bound Results:

- Reconstruction Attack [DN03]
- Geometric Argument [HT10]
- Synthetic Dataset [DNRRV09, UV11]
- Fingerprinting Codes [Ull13, BUV14]
- Private Learning [BBKN10]
- Discrepancy Lower Bound [MN12]
- ...

Differential Privacy Results

Algorithms:

- Histogram [DMNS06]
- Exponential Mechanism [MT07]
- Synthetic Data [BLR08]
- Private Multiplicative Weights [HR10]
- Boosting [DRV10]
- Private Learning [KLNRS08]
- Statistical Estimation [Smith10]
- Streaming [DNPR10, MMNW11]
- ...

Lower Bound Results:

- Reconstruction Attack [DN03]
- Geometric Argument [HT10]
- Synthetic Dataset [DNRRV09, UV11]
- Fingerprinting Codes [UII13, BUV14]
- Private Learning [BBKN10]
- Discrepancy Lower Bound [MN12]
- ...

Q: Can we obtain improved algorithms
by relaxing the definition?

Computational Differential Privacy (CDP)

Def M is (ε, δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

Computational Differential Privacy (CDP)

Def M is (ε, δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D)\ \in\ T]\ \leq\ e^{\varepsilon} \Pr[M(D')\ \in\ T] + \delta}$$

$$\boxed{\forall A\ ,\quad \Pr[A(M(D)) = 1] \leq e^{\varepsilon} \Pr[A(M(D')) = 1] + \delta}$$

Computational Differential Privacy (CDP)

Def M is (ε, δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

$$|||$$

$$\boxed{\forall A\ ,\quad \Pr[A(M(D)) = 1] \leq e^{\varepsilon} \Pr[A(M(D')) = 1] + \delta}$$

$$\Downarrow$$

Def M is ε-IND-CDP if $\forall\ D \sim D'$

$$\boxed{\forall\, \mathrm{poly}\text{-time } A,\ \Pr[A(M(D)) = 1] \leq e^{\varepsilon} \Pr[A(M(D')) = 1] + \mathrm{negl}}$$

[Mironov, Pandey, Reingold, Vadhan '09]

Computational Differential Privacy (CDP)

Def M is (ε, δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D) \in T] \leq e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

$$|||$$

$$\boxed{\forall A\ ,\quad \Pr[A(M(D)) = 1] \leq e^{\varepsilon} \Pr[A(M(D')) = 1] + \delta}$$

$$\Downarrow$$

Def M is ε-IND-CDP if $\forall\ D \sim D'$

$$\boxed{\forall\, \text{poly-time } A,\ \Pr[A(M(D)) = 1] \leq e^{\varepsilon} \Pr[A(M(D')) = 1] + \mathrm{negl}}$$

[Mironov, Pandey, Reingold, Vadhan '09]

Def M is ε-SIM-CDP if $\exists\ (\varepsilon, \mathrm{negl})$-DP M' s.t. $\forall\ D$

$$\boxed{M(D) \overset{\mathrm{c}}{\approx} M'(D)}$$

[Mironov, Pandey, Reingold, Vadhan '09]

Computational Differential Privacy (CDP)

Def M is (ε, δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D) \in T] \le e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

$$|||$$

$$\boxed{\forall A\ ,\quad \Pr[A(M(D)) = 1] \le e^{\varepsilon} \Pr[A(M(D')) = 1] + \delta}$$

$$\Downarrow$$

$\{M_k\}_{k \in \mathbb{N}}$ is ε-IND-CDP if $\forall\ \{D_k\}_{k \in \mathbb{N}} \sim \{D'_k\}_{k \in \mathbb{N}}$

$$\boxed{\forall\, \mathrm{poly}(k)\text{-time } A, \Pr[A(M_k(D_k)) = 1] \le e^{\varepsilon} \Pr[A(M_k(D'_k)) = 1] + \mathrm{negl}(k)}$$

[Mironov, Pandey, Reingold, Vadhan '09]

$\{M_k\}_{k \in \mathbb{N}}$ is ε-SIM-CDP if $\exists\ (\varepsilon, \mathrm{negl}(k))$-DP $\{M'_k\}_{k \in \mathbb{N}}$ s.t. $\forall\ \{D_k\}_{k \in \mathbb{N}}$

$$\boxed{\{M_k(D_k)\}_{k \in \mathbb{N}} \overset{c}{\approx} \{M'_k(D_k)\}_{k \in \mathbb{N}}}$$

[Mironov, Pandey, Reingold, Vadhan '09]

Computational Differential Privacy (CDP)

Def M is (ε,δ)-DP if $\forall\ D \sim D'$,

$$\boxed{\forall T, \Pr[M(D) \in T] \le e^{\varepsilon} \Pr[M(D') \in T] + \delta}$$

$$|||$$

$$\boxed{\forall A\ ,\quad \Pr[A(M(D)) = 1] \le e^{\varepsilon} \Pr[A(M(D')) = 1] + \delta}$$

$$\Downarrow$$

$\{M_k\}_{k\in\mathbb{N}}$ is ε-IND-CDP if $\forall\ \{D_k\}_{k\in\mathbb{N}} \sim \{D'_k\}_{k\in\mathbb{N}}$

$$\boxed{\forall\, \text{poly}(k)\text{-time } A, \Pr[A(M_k(D_k)) = 1] \le e^{\varepsilon} \Pr[A(M_k(D'_k)) = 1] + \text{negl}(k)}$$

[Mironov, Pandey, Reingold, Vadhan '09]

$\{M_k\}_{k\in\mathbb{N}}$ is ε-SIM-CDP if $\exists\ (\varepsilon, \text{negl}(k))$-DP $\{M'_k\}_{k\in\mathbb{N}}$ s.t. $\forall\ \{D_k\}_{k\in\mathbb{N}}$

$$\boxed{\{M_k(D_k)\}_{k\in\mathbb{N}} \overset{c}{\approx} \{M'_k(D_k)\}_{k\in\mathbb{N}}}$$

[Mironov, Pandey, Reingold, Vadhan '09]

$$\boxed{\text{DP} \subseteq \text{SIM-CDP} \subseteq \text{IND-CDP}}$$

Previous Work: Multiparty Protocols

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Goal Computing a joint function of private datasets.

Previous Work: Multiparty Protocols

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Goal Computing a joint function of private datasets.

$$\begin{array}{ccc} & \xrightarrow{\hspace{6em}} & \\ \text{Alice} & \xleftarrow{\hspace{6em}} & \text{Bob} \\ D_A & \vdots & D_B \\ & \xrightarrow{\hspace{6em}} & \end{array}$$

Previous Work: Multiparty Protocols

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Goal Computing a joint function of private datasets.

$$\begin{array}{ccc} & \longrightarrow & \\ \text{Alice} & \longleftarrow & \text{Bob} \\ D_A & \vdots & D_B \\ & \longrightarrow & \end{array}$$

Privacy [BNO08] Privacy of D_A should be maintained against Bob and D_B against Alice

Previous Work: Multiparty Protocols

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Goal Computing a joint function of private datasets.

$$\begin{array}{ccc} & \longrightarrow & \\ \text{Alice} & \longleftarrow & \text{Bob} \\ D_A & \vdots & D_B \\ & \longrightarrow & \end{array}$$

Privacy [BNO08] Privacy of D_A should be maintained against Bob and D_B against Alice

> DP $\subsetneq$ SIM-CDP in the case of two or more parties.

Previous Work: Multiparty Protocols

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Goal Computing a joint function of private datasets.

$$\begin{array}{ccc} & \longrightarrow & \\ \text{Alice} & \longleftarrow & \text{Bob} \\ D_A & \vdots & D_B \\ & \longrightarrow & \end{array}$$

Privacy [BNO08] Privacy of D_A should be maintained against Bob and D_B against Alice

$\boxed{\text{DP} \subsetneq \text{SIM-CDP in the case of two or more parties.}}$

2-party task Hamming distance

n-party task Sum of n bits

DP Error: $\Theta(\sqrt{n})$ [BNO08, MPRV09, MMPRTV10, CSS12]

CDP Error: $O(1)$ (using MPC) [DKMMN06, BNO08]

Our Focus: Client-Server Setting

Database: D

Name	Age	Height	Smoke
Alice	13	147	Y
Charlie	27	176	N
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Eve	42	173	Y

$\Leftrightarrow$ Randomized Mechanism M $\xrightarrow{M(D)}$ Analyst

Our Focus: Client-Server Setting

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

Our Focus: Client-Server Setting

[Groce, Katz, Yerukhimovich '11]

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

- Error $= L_p$ norm on $\mathbb{R}^{O(1)} \Rightarrow$ can convert IND-CDP to DP with $1/\operatorname{poly}(k)$ additive increase in error.
- Cannot separate IND-CDP and DP with black-box 'generic' crypto primitives (e.g. OWF, TDP).

Our Focus: Client-Server Setting

[Groce, Katz, Yerukhimovich '11]

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

- Error $= L_p$ norm on $\mathbb{R}^{O(1)} \Rightarrow$ can convert IND-CDP to DP with $1/\operatorname{poly}(k)$ additive increase in error.
- Cannot separate IND-CDP and DP with black-box 'generic' crypto primitives (e.g. OWF, TDP).

Our Results

Thm1 (DP $\neq$ SIM-CDP) Assume NIZKs for NP & sub-exponentially secure OWF.

Then $\exists$ poly-time computable utility function $U(D, M(D))$ s.t.

1. $\exists$ poly-time SIM-CDP mechanism M^{CDP} s.t.
$$\forall D, \Pr[U(D, M^{\mathrm{CDP}}(D)) = 1] \geq 1 - \operatorname{negl}(k).$$
2. $\forall$ poly-time DP mechanism $M^{\mathrm{DP}}, \exists D$ s.t.
$$\Pr[U(D, M^{\mathrm{DP}}(D)) = 1] \leq \operatorname{negl}(k).$$

Our Focus: Client-Server Setting

[Groce, Katz, Yerukhimovich '11]

DP $\subseteq$ SIM-CDP $\subseteq$ IND-CDP

- Error $= L_p$ norm on $\mathbb{R}^{O(1)} \Rightarrow$ can convert IND-CDP to DP with $1/\operatorname{poly}(k)$ additive increase in error.
- Cannot separate IND-CDP and DP with black-box 'generic' crypto primitives (e.g. OWF, TDP).

Our Results

Thm1 (DP $\neq$ SIM-CDP) Assume NIZKs for NP & sub-exponentially secure OWF.

Then $\exists$ poly-time computable utility function $U(D, M(D))$ s.t.

1. $\exists$ poly-time SIM-CDP mechanism M^{CDP} s.t.
$$\forall D, \Pr[U(D, M^{\mathrm{CDP}}(D)) = 1] \geq 1 - \operatorname{negl}(k).$$
2. $\forall$ poly-time DP mechanism $M^{\mathrm{DP}}, \exists D$ s.t.
$$\Pr[U(D, M^{\mathrm{DP}}(D)) = 1] \leq \operatorname{negl}(k).$$

Thm2 (Extension of [GKY11]) Error $=$ metric with $O(\log k)$ doubling dimension $\Rightarrow$ can convert IND-CDP to DP with $O(1)$ multiplicative increase in error.

Proof Outline

- Tools
  - "Exponentially Extractable" Zaps [Dwork, Naor '07]. (Based on NIZK)
  - Sub-exponentially Strongly Unforgeable Digital Signature Scheme (Based on sub-exponentially secure OWF)

Proof Outline

- Tools
  - "Exponentially Extractable" Zaps [Dwork, Naor '07]. (Based on NIZK)
  - Sub-exponentially Strongly Unforgeable Digital Signature Scheme (Based on sub-exponentially secure OWF)
- Define Task: zap proof of existence of a signature.

Proof Outline

- Tools
  - "Exponentially Extractable" Zaps [Dwork, Naor '07]. (Based on NIZK)
  - Sub-exponentially Strongly Unforgeable Digital Signature Scheme (Based on sub-exponentially secure OWF)
- Define Task: zap proof of existence of a signature.
- Claims
  1. $\exists$ a (non-efficient) DP mechanism with high utility.
  2. $\exists$ an efficient SIM-CDP with high utility. ($\stackrel{c}{\approx}$ to the DP mechanism)
  3. No efficient DP mechanism with non-negligible utility (Otherwise break the signature scheme).

Zaps (2-message public coin witness indistinguishability)

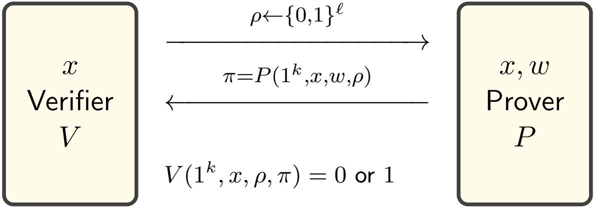
$L \in \mathbf{NP}$ witness relation: $(x, w) \in R_L$ security parameter: k

Verifier		Prover
x	$\xrightarrow{\rho \leftarrow \{0,1\}^\ell}$	x, w
Verifier V	$\xleftarrow{\pi = P(1^k, x, w, \rho)}$	Prover P

$V(1^k, x, \rho, \pi) = 0$ or 1

Zaps (2-message public coin witness indistinguishability)

$L \in \mathbf{NP}$ witness relation: $(x, w) \in R_L$ security parameter: k



- *Completeness*
- *Soundness*
- *Witness Indistinguishability* (vs. adversarial V^*)

Zaps (2-message public coin witness indistinguishability)

$L \in \mathbf{NP}$ witness relation: $(x, w) \in R_L$ security parameter: k

x
Verifier
V

$$\xrightarrow{\rho \leftarrow \{0,1\}^\ell}$$

$$\xleftarrow{\pi = P(1^k, x, w, \rho)}$$

x, w
Prover
P

$V(1^k, x, \rho, \pi) = 0$ or 1

- *Completeness*
- *Soundness*
- *Witness Indistinguishability* (vs. adversarial V^*)
- *Extractability*: Algorithm E running in time $2^{O(k)}$ s.t. $\forall x$

$$(x, \rho, \pi) \longrightarrow \boxed{\text{Extractor } E} \longrightarrow w = E(1^k, x, \rho, \pi)$$

The Task

- $(\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$: Sub-exponentially secure signature scheme.
- $(P_{\mathrm{zap}}, V_{\mathrm{zap}}, E_{\mathrm{zap}})$: Exponentially extractable zap.

The Task

- $(\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$: Sub-exponentially secure signature scheme.
- $(P_{\mathrm{zap}}, V_{\mathrm{zap}}, E_{\mathrm{zap}})$: Exponentially extractable zap.

Dataset D $\rightarrow$ Mechanism M $\rightarrow$ $M(D) = \pi$: Zap proof that "$\exists(m, \sigma)$ s.t. $\mathrm{Ver}_{vk}(m, \sigma) = 1$"

The Task

- $(\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$: Sub-exponentially secure signature scheme.
- $(P_{\mathrm{zap}}, V_{\mathrm{zap}}, E_{\mathrm{zap}})$: Exponentially extractable zap.

Dataset D → Mechanism M → $M(D) = \pi$: Zap proof that "$\exists (m, \sigma)$ s.t. $\mathrm{Ver}_{vk}(m, \sigma) = 1$"

- Utility: $U(D, M(D)) = 0$ or 1.
  - If $> 90\%$ rows are of the form $(\hat{vk}, \hat{\rho}, m_i, \sigma_i)$ where $\mathrm{Ver}_{\hat{vk}}(m_i, \sigma_i) = 1$, then output $V_{\mathrm{zap}}(\hat{vk}, \hat{\rho}, \pi)$.
  - Otherwise, output 1.

Claims to Prove

1. There exists (inefficient) DP mechanism M^{unb}.

2. There exists an efficient mechanism M^{CDP}.

3. No efficient DP mechanism achieves good utility.

Claims to Prove

1. There exists (inefficient) DP mechanism M^{unb}.

   Alg 1. Find the majority $(\hat{vk}, \hat{\rho})$ pair in a differentially private way.

   2. Generate zap proof using the lexicographically first witness (m, σ).

2. There exists an efficient mechanism M^{CDP}.

3. No efficient DP mechanism achieves good utility.

Claims to Prove

1. There exists (inefficient) DP mechanism M^{unb}.

   Alg
   1. Find the majority $(\hat{vk}, \hat{\rho})$ pair in a differentially private way.
   2. Generate zap proof using the lexicographically first witness (m, σ).

2. There exists an efficient mechanism M^{CDP}.

   Alg
   1. Find the majority $(\hat{vk}, \hat{\rho})$ pair in a differentially private way.
   2. Generate zap proof using a witness from the dataset.

   CDP $M^{\mathrm{CDP}} \overset{c}{\approx} M^{\mathrm{unb}}$ due to WI of zap.

3. No efficient DP mechanism achieves good utility.

Claims to Prove

1. There exists (inefficient) DP mechanism M^{unb}.

   Alg 1. Find the majority $(\hat{vk}, \hat{\rho})$ pair in a differentially private way.
   2. Generate zap proof using the lexicographically first witness (m, σ).

2. There exists an efficient mechanism M^{CDP}.

   Alg 1. Find the majority $(\hat{vk}, \hat{\rho})$ pair in a differentially private way.
   2. Generate zap proof using a witness from the dataset.

   CDP $M^{\text{CDP}} \overset{\text{c}}{\approx} M^{\text{unb}}$ due to WI of zap.

3. No efficient DP mechanism achieves good utility.

   Idea If there exists such an M, combine M and $2^{O(k_{\text{zap}})}$-time zap extractor to construct a $2^{O(k_{\text{zap}})}$-time forger for digital signature.

   Violate Sub-exponential-security of digital signature. (complexity leveraging [CGGM00])

Conclusion

- DP $\subsetneq$ SIM-CDP $\subseteq$ IND-CDP (in client-server model)
  Assuming sub-exponential OWF and NIZK, we construct a task s.t.
  - There exists an efficient SIM-CDP mechanism with good utility.
  - Every efficient DP mechanism only has negligible utility.

Conclusion

- DP $\subsetneq$ SIM-CDP $\subseteq$ IND-CDP (in client-server model)
  Assuming sub-exponential OWF and NIZK, we construct a task s.t.
  - There exists an efficient SIM-CDP mechanism with good utility.
  - Every efficient DP mechanism only has negligible utility.
- In many natural cases (e.g. answering $O(\log n)$ counting queries), a CDP mechanism cannot do much better then DP mechanisms.

Conclusion

- DP $\subsetneq$ SIM-CDP $\subseteq$ IND-CDP (in client-server model)
  Assuming sub-exponential OWF and NIZK, we construct a task s.t.
  - There exists an efficient SIM-CDP mechanism with good utility.
  - Every efficient DP mechanism only has negligible utility.
- In many natural cases (e.g. answering $O(\log n)$ counting queries), a CDP mechanism cannot do much better then DP mechanisms.

Open Problems:

- Natural separation of DP and SIM-CDP
  (e.g. poly-many counting queries)
- More cases where CDP mechanisms can be converted to DP mechanisms.

Conclusion

- DP $\subsetneq$ SIM-CDP $\subseteq$ IND-CDP (in client-server model)
  Assuming sub-exponential OWF and NIZK, we construct a task s.t.
  - There exists an efficient SIM-CDP mechanism with good utility.
  - Every efficient DP mechanism only has negligible utility.
- In many natural cases (e.g. answering $O(\log n)$ counting queries), a CDP mechanism cannot do much better then DP mechanisms.

Open Problems:

- Natural separation of DP and SIM-CDP
  (e.g. poly-many counting queries)
- More cases where CDP mechanisms can be converted to DP mechanisms.
- A task that is solvable by an IND-CDP mechanism but impossible for DP (would imply SIM-CDP $\neq$ IND-CDP).

Conclusion

- DP $\subsetneq$ SIM-CDP $\subseteq$ IND-CDP (in client-server model)
  Assuming sub-exponential OWF and NIZK, we construct a task s.t.
  - There exists an efficient SIM-CDP mechanism with good utility.
  - Every efficient DP mechanism only has negligible utility.
- In many natural cases (e.g. answering $O(\log n)$ counting queries), a CDP mechanism cannot do much better then DP mechanisms.

Open Problems:

- Natural separation of DP and SIM-CDP
  (e.g. poly-many counting queries)
- More cases where CDP mechanisms can be converted to DP mechanisms.
- A task that is solvable by an IND-CDP mechanism but impossible for DP (would imply SIM-CDP $\neq$ IND-CDP).

Thanks!