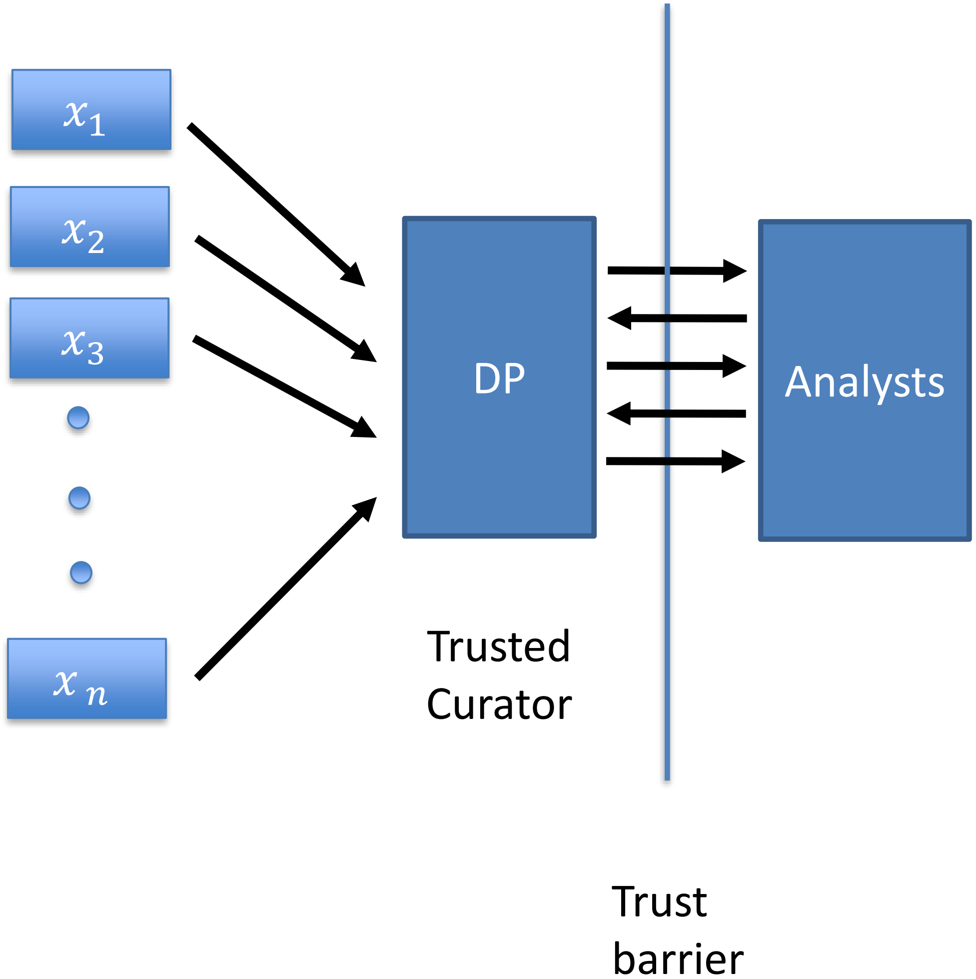
CS208: Applied Privacy for Data Science
Other Distributed Models for DP

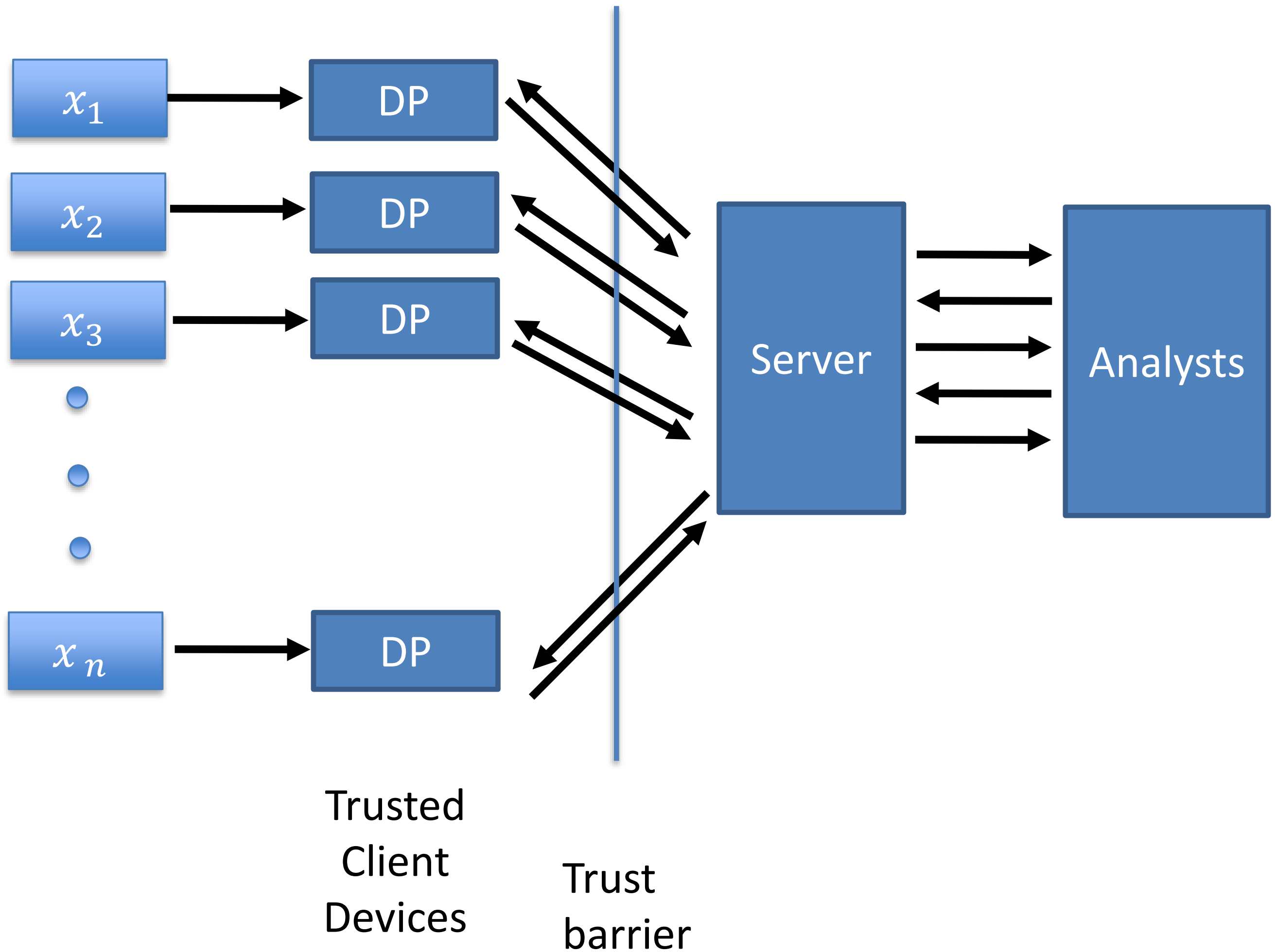
School of Engineering & Applied Sciences
Harvard University

April 7, 2022

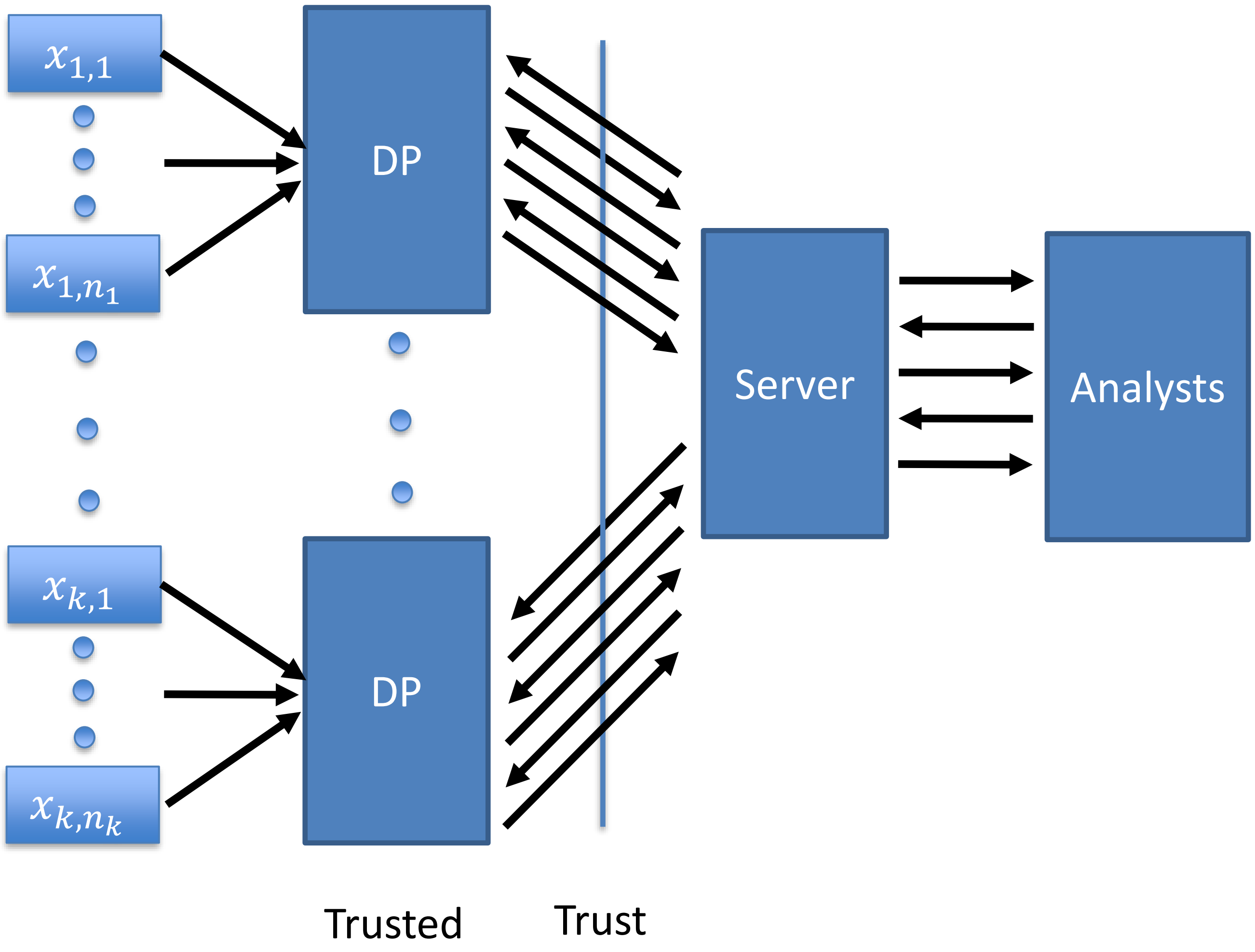
Central DP



Local DP


x_1
x_2
x_3
x_n
DP
DP
DP
DP
Server
Analysts
Trusted Client Devices
Trust barrier

Federated DP



Comparing the Models

- Federated DP with k delegates, $n = n_1 + \cdots + n_k$
  - "horizontally partitioned" data
  - $k = 1$: central DP
  - $k = n$: local DP

- Error for sum of bounded values (like in DP-SGD) = $\Theta\left(\frac{\sqrt{k}}{\varepsilon}\right)$.
  - Interpolates between local & central model

- Error for set intersection when $k = 2$: $\Theta\left(\frac{\sqrt{n}}{\varepsilon}\right)$
  - No better than local model!

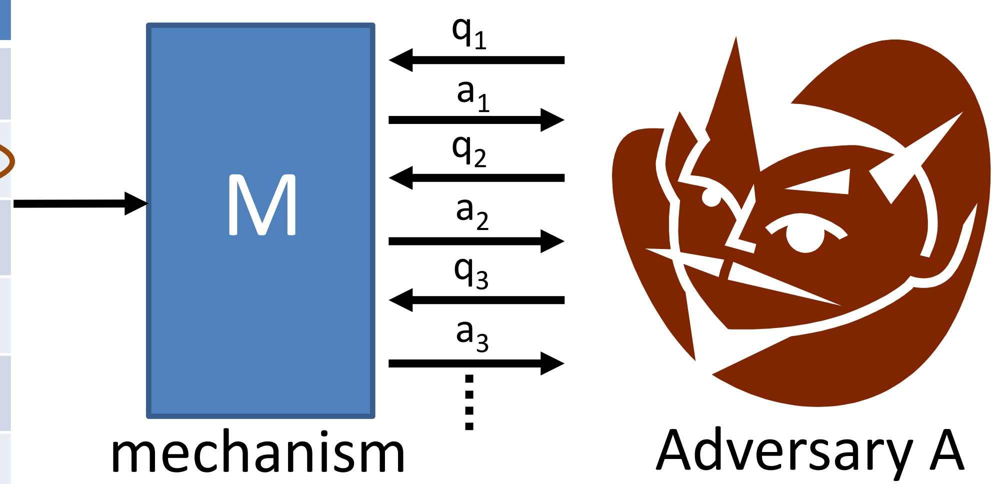
DP in terms of adversaries

- Def: An algorithm $M: \mathcal{X}^n \to \mathcal{Y}$ is **$(\boldsymbol{\epsilon}, \boldsymbol{\delta})$-differentially private** if $\forall$ neighboring $x, x' \in \mathcal{X}^n$ and $\forall\, T \subseteq \mathcal{Y}$,
$$\Pr[M(x) \in T] \leq e^{\epsilon} \cdot \Pr[M(x') \in T] + \delta$$

- Equivalently: $\forall$ neighboring $x, x' \in \mathcal{X}^n$ and $\forall\, A : \mathcal{Y} \to \{0,1\}$,
$$\Pr\left[A\left(M(x)\right) = 1\right] \leq e^{\epsilon} \cdot \Pr\left[A\left(M(x')\right) = 1\right] + \delta$$

DP for Interactive Mechanisms

Sex	Blood	⋯	HIV?
F	B	⋯	Y
F	A		Y
M	O	⋯	N
M	O	⋯	Y
F	A	⋯	N
M	B	⋯	Y



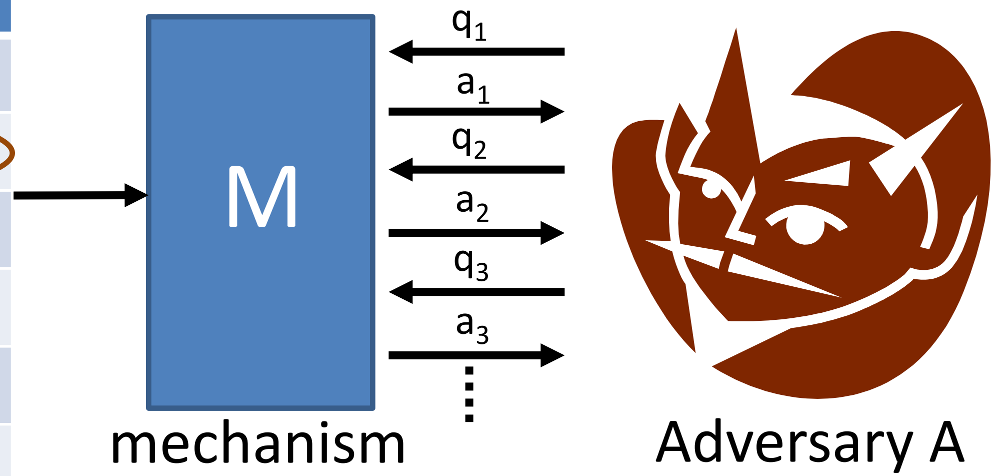
1st Attempt: for all D, D' differing on one row, all $q_1,\ldots,q_t$, all T

$$\Pr[\underbrace{M(D, q_1, \ldots, q_t)} \in T] \leq e^{\varepsilon} \cdot \Pr[\underbrace{M(D', q_1, \ldots, q_t)} \in T] + \delta$$

vectors of answers $a_1, \ldots, a_t$

DP for Interactive Mechanisms

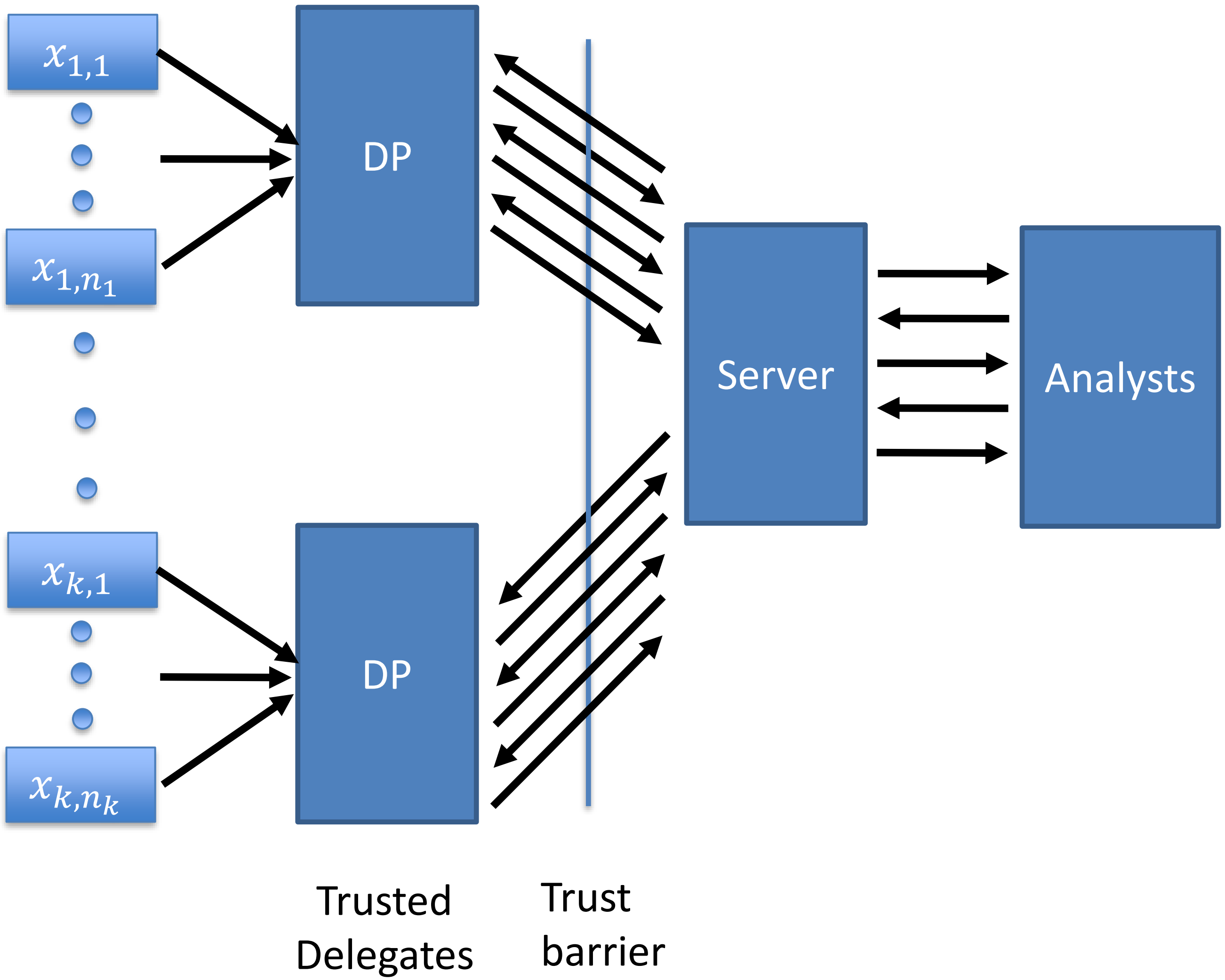
Sex	Blood	⋯	HIV?
F	B	⋯	Y
F	**A**		**Y**
M	O	⋯	N
M	O	⋯	Y
F	A	⋯	N
M	B	⋯	Y



Better: for all D, D' differing on one row, all adversarial strategies A

$$\Pr[A \text{ outputs 1 after interacting w}/M(D)]$$
$$\leq e^{\varepsilon} \cdot \Pr[A \text{ outputs 1 after interacting w}/M(D')] + \delta$$

Federated DP

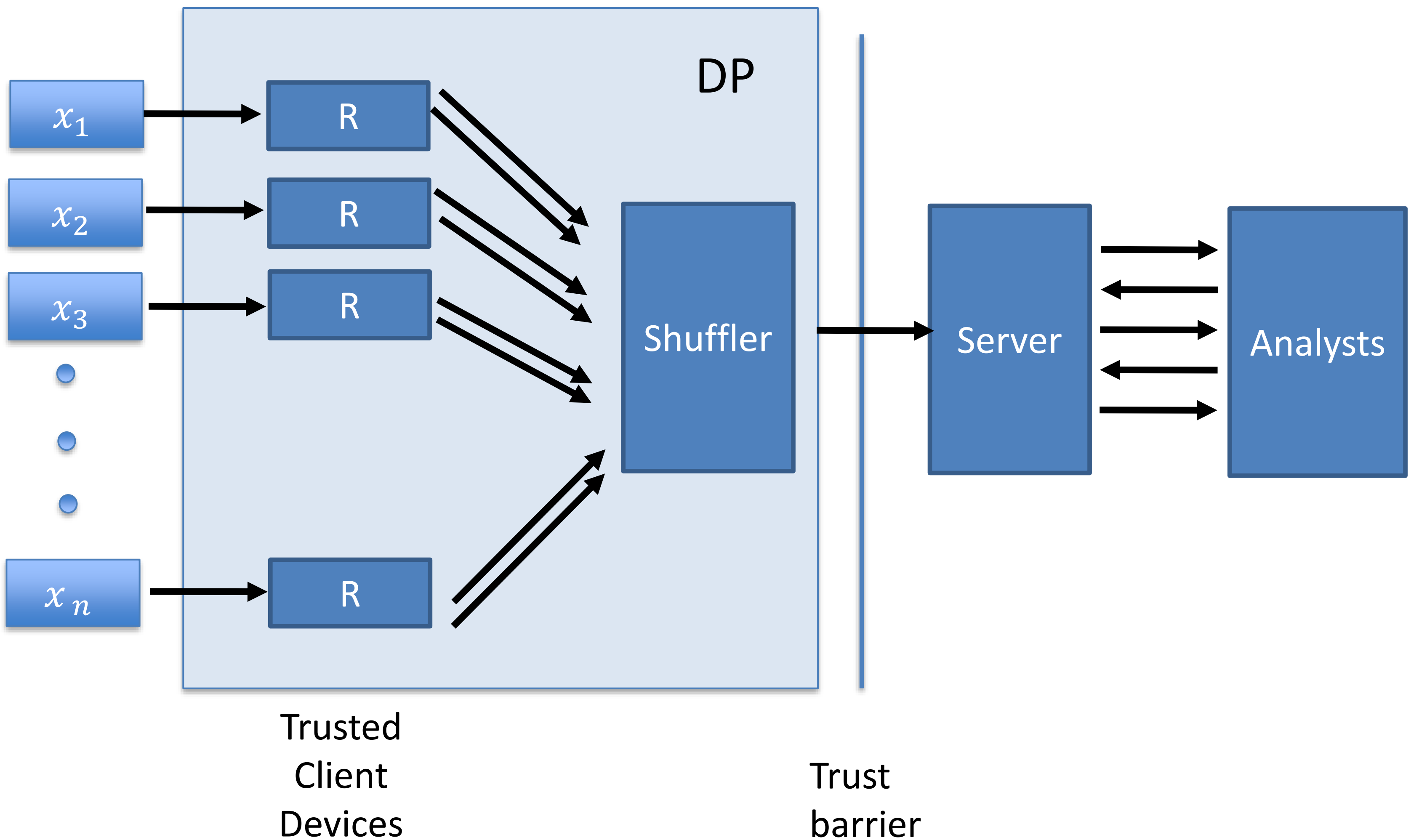


Other Models

- Can we get the “best of both worlds”?
  - Privacy protections like the local model
  - Accuracy like the central model

- Two approaches
  - The shuffle model
  - Using cryptography (secure multiparty computation)

Shuffle DP


x_1
x_2
x_3
x_n
R
R
R
R
DP
Shuffler
Server
Analysts
Trusted Client Devices
Trust barrier

Binary Sum with Shuffle DP

- Suppose each $x_i \in \{0,1\}$ and R = (weak) randomized response

$$R(x_i) = \begin{cases} \mathrm{Ber}(1/2) & \text{w.p. } p \\ x_i & \text{w.p. } 1-p \end{cases}$$

<u>Analyzing the privacy of client i:</u>

- Shuffling ⇒ only information revealed is

$$S = \sum_j R(x_j) = R(x_i) + S_{-i}$$

- $S_{-i} \approx (1-p)\sum_{j \neq i} x_i + \mathrm{Bin}(pn, 1/2)$
- $\sigma^2 = \frac{c \ln(1/\delta)}{\varepsilon^2} \Rightarrow (\varepsilon, \delta)$-DP

<u>Accuracy:</u> error $O(\sigma) = O\left(\frac{\sqrt{\ln(1/\delta)}}{\varepsilon}\right)$. No dependence on n!

Privacy Amplification by Shuffling

$$R(x_i) = \begin{cases} \mathrm{Ber}(1/2) & \text{w.p. } p = \dfrac{c \ln(1/\delta)}{\varepsilon^2 n} \\ x_i & \text{w.p. } 1 - p \end{cases}$$

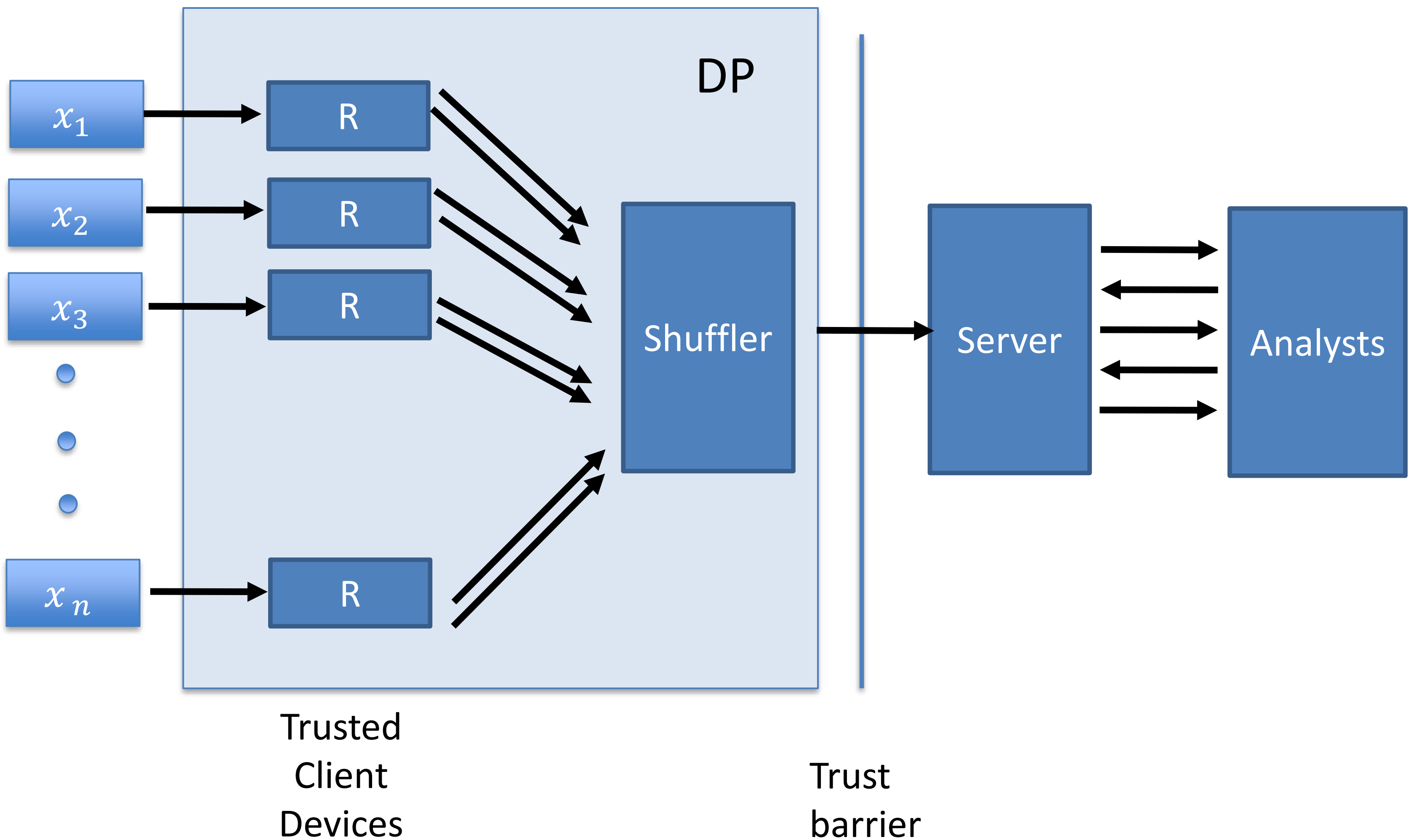
- Note that R is only $\varepsilon_0 = \ln\left(\frac{1-p/2}{p/2}\right) \approx \ln\left(\frac{\varepsilon^2 n}{\ln(1/\delta)}\right)$-DP.

- General amplification thm: if R is ε_0-DP, then $M(x_1, \ldots, x_n) = \mathrm{Shuffle}\big(R(x_1), \ldots, R(x_n)\big)$ is (ε, δ)-DP with relation as above

Shuffle vs. Central DP

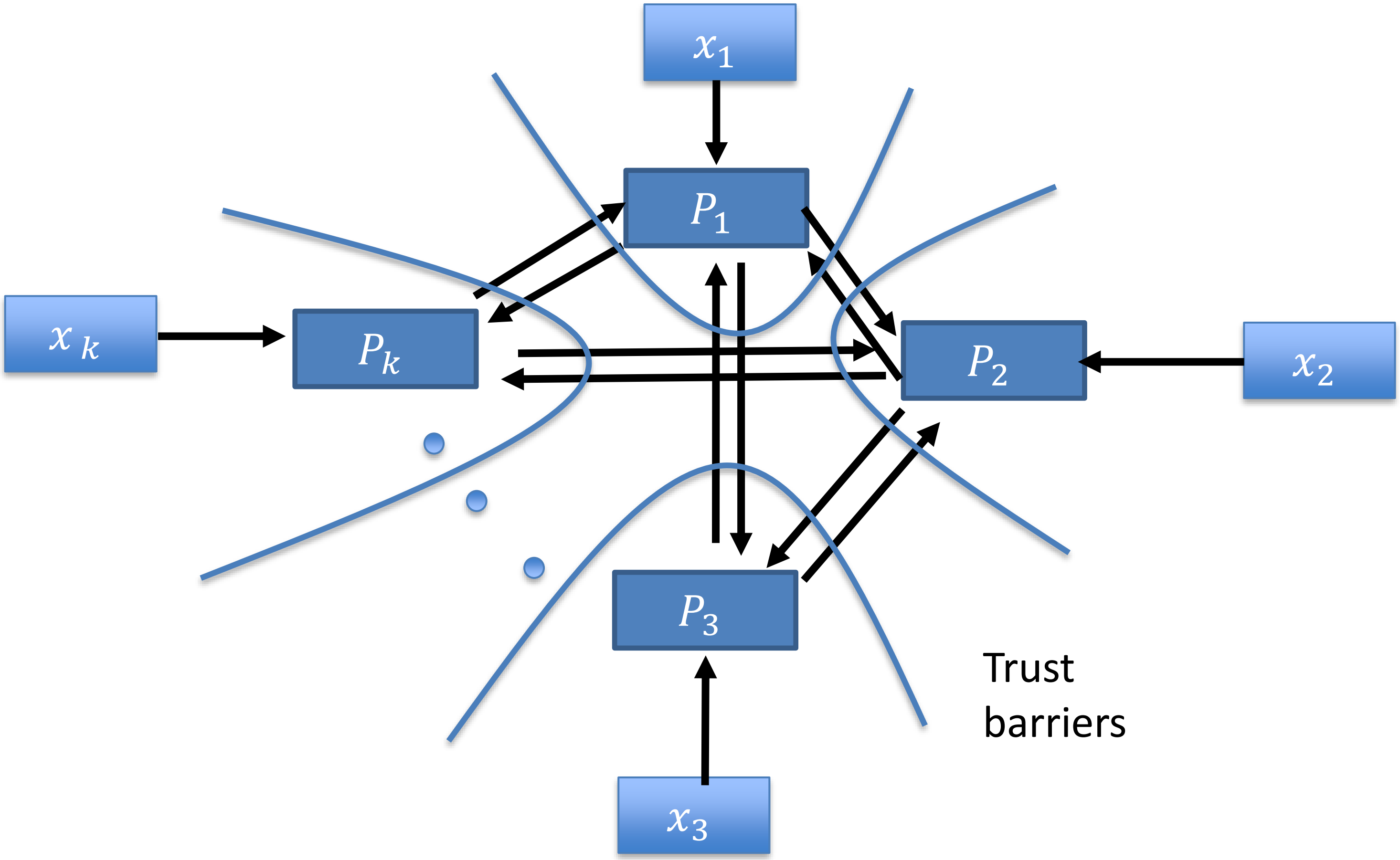
- There is a many-message shuffle-DP protocol with error $O(1/\varepsilon)$, matching the central model.
- For other problems, shuffle seems to give accuracy strictly between local and central.
  - E.g. best known error for histograms: $O\left(\frac{\ln(1/\delta)}{\varepsilon^2}\right)$.
  - Don't know matching upper & lower bounds for most problems, especially for multi-message shuffle protocols.
- Q: trust considerations for shuffle model?

Shuffle DP



DP
x_1
x_2
x_3
x_n
R
R
R
R
Shuffler
Server
Analysts
Trusted
Client
Devices
Trust
barrier

Secure Multiparty Computation



Requirement: At end of protocol, each party P_i learns $f_i(x_1, \dots, x_n)$ and nothing else!

Example: Binary Sum

- Round 1: for $i = 1, \dots, n$, party i should:
  - Receive a value v from party $i - 1$ ($v = 0$ if $i = 1$)
  - Choose a uniformly random number $r_i \in \{0,1, \dots, n\}$
  - Send party $i + 1$ the value $v + x_i + r_i \bmod (n - 1)$

- Round 2: for $i = 1, \dots, n$, party i should:
  - Receive a value v from party $i - 1$ (party n if $i = 0$)
  - Send party $i + 1$ the value $v - r_i \bmod (n - 1)$

- Claim: party n learns $\sum_i x_i$ and nothing else, no one else learns anything.

MPC is Always Possible (in theory)

Theorem (1980's): Assume that secure cryptography exists. Then for all polynomial-time computable functions $f_1, \dots, f_n$ (even randomized), there is a polynomial-time secure MPC protocol with security against:

- All feasible (e.g. polynomial-time) adversaries
- Even if they deviate from the protocol
- Even if they control $n-1$ parties

DP+MPC

Applying Secure MPC to f_1=any central DP algorithm, we get a protocol Π

- Accuracy of central DP
- Privacy of local DP against feasible adversaries A
  - Even ones that deviate from protocol
  - And corrupt up to $n-1$ parties

Why aren't we done?

Ways to make MPC more efficient

- Focus on specific functionalities (e.g. summation without noise)
- Restrict to passive ("honest but curious") adversaries
- Restrict sizes of coalitions ("threshold adversaries")
- Use trusted hardware (secure enclaves, Intel SGX)

DP vs. Crypto

Model	Utility	Privacy	Who Holds Data?
Centralized Differential Privacy	statistical analysis of dataset	individual-specific info	trusted curator
Local or Federated Differential Privacy	statistical analysis of dataset	individual-specific info	original users (or delegates)
Secure Multiparty Computation	any query desired	everything other than result of query	original users (or delegates)
Fully Homomorphic (or Functional) Encryption	any query desired	everything (except possibly result of query)	untrusted server