Differentially Private Resource Sharing*

Utku Karaca[†], İlker Birbil, Nurşen Aydın, Gizem Mullaoğlu

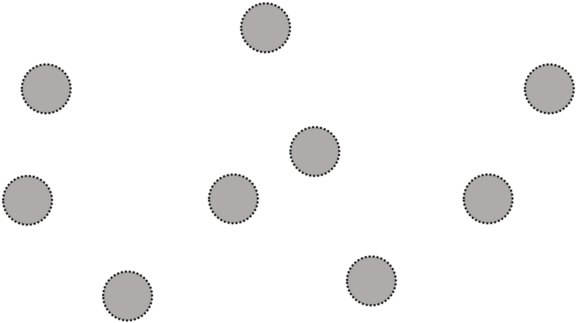
†Econometric Institute, Erasmus University Rotterdam

Dutch Seminar on Optimization
December 9, 2021

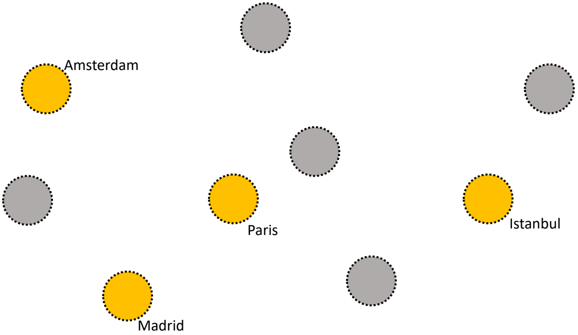
*https://arxiv.org/abs/2110.10498

Agenda

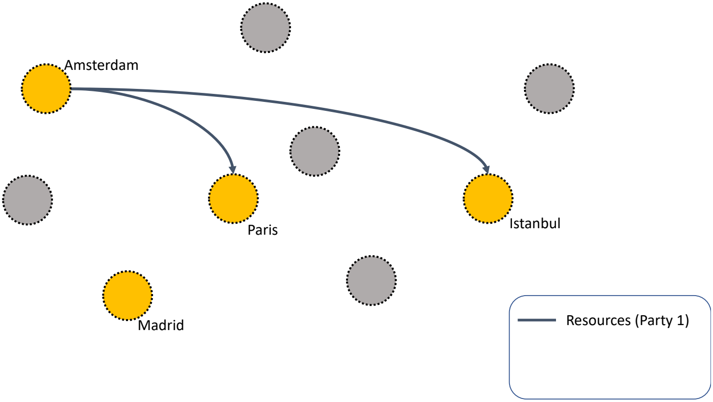
Motivation



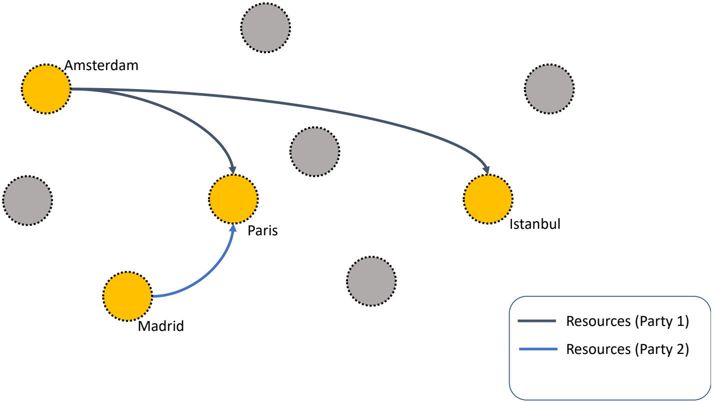
Motivation



Motivation

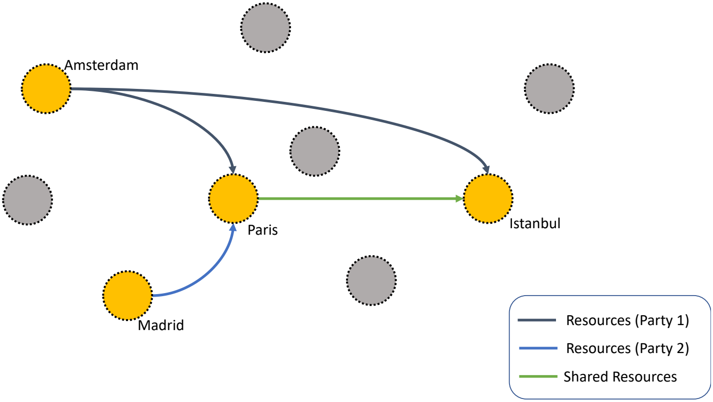


Motivation



ERASMUS UNIVERSITEIT ROTTERDAM

Motivation


Amsterdam
Paris
Istanbul
Madrid
Resources (Party 1)
Resources (Party 2)
Shared Resources

Motivation

- Unused capacities (flights, trucks, ships, manufacturing lines, etc.)
- Sustainability in logistics and production
- Resource sharing

Motivation

- Willingness to collaborate
- Concerns about data sharing
- Regulations and privacy guarantees

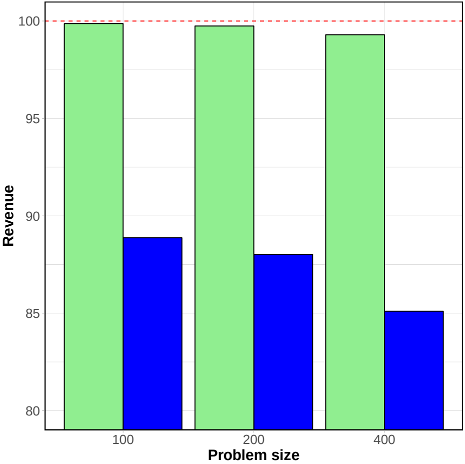
Motivation

- Willingness to collaborate
- Concerns about data sharing
- Regulations and privacy guarantees

Motivation

- Willingness to collaborate
- Concerns about data sharing
- Regulations and privacy guarantees

Motivation: Contribution of Collaboration



Modeling

$\mathcal{K}$: set of parties
u_k : utility vector for party k
$\mathrm{A}_k, \mathrm{B}_k$: shared and individual constraint matrices
c : shared resource capacities
b_k : individual constraint constants

$$\begin{aligned} \text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^\mathsf{T} \mathrm{x}_k, \\ \text{subject to} \quad & \sum_{k \in \mathcal{K}} \mathrm{A}_k \mathrm{x}_k \leq \mathrm{c}, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \qquad k \in \mathcal{K}. \end{aligned}$$

$$\boldsymbol{\mathcal{X}}_k = \{\mathrm{x}_k \in \mathbb{R}^{n_k} : \mathrm{B}_k \mathrm{x}_k \leq \mathrm{b}_k\}$$

ERASMUS UNIVERSITEIT ROTTERDAM

Modeling

$\mathcal{K}$: set of parties
u_k : utility vector for party k
$\mathrm{A}_k, \mathrm{B}_k$: shared and individual constraint matrices
c : shared resource capacities
b_k : individual constraint constants

$$\begin{aligned} \text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^\intercal \mathrm{x}_k, \\ \text{subject to} \quad & \sum_{k \in \mathcal{K}} \mathrm{A}_k \mathrm{x}_k \leq \mathrm{c}, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \qquad k \in \mathcal{K}. \end{aligned}$$

$$\boldsymbol{\mathcal{X}}_k = \{\mathrm{x}_k \in \mathbb{R}^{n_k} : \mathrm{B}_k \mathrm{x}_k \leq \mathrm{b}_k\}$$

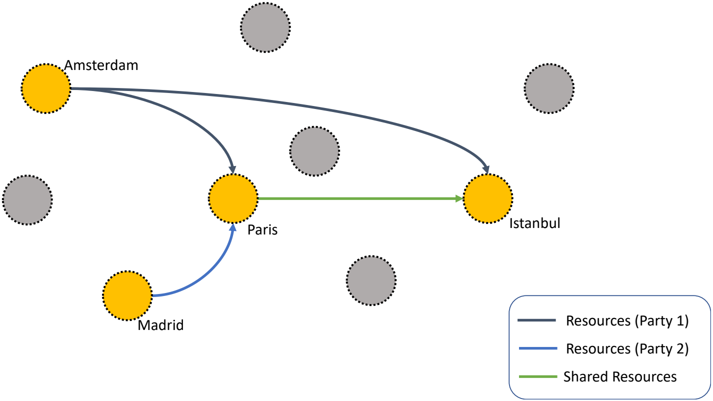
Modeling

$$
\begin{aligned}
\text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^\intercal \mathrm{x}_k, \\
\text{subject to} \quad & \sum_{k \in \mathcal{K}} \mathrm{A}_k \mathrm{x}_k \leq \mathrm{c}, \\
& \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \qquad\qquad\qquad\qquad k \in \mathcal{K}.
\end{aligned}
$$

$$
\boldsymbol{\mathcal{X}}_k = \{\mathrm{x}_k \in \mathbb{R}^{n_k} : \mathrm{B}_k \mathrm{x}_k \leq \mathrm{b}_k\}
$$

Definition (Data set)

$\mathcal{D}_k : \{\mathrm{A}_k, \mathrm{B}_k, \mathrm{b}_k, \mathrm{u}_k\}$.


Amsterdam
Paris
Istanbul
Madrid
Resources (Party 1)
Resources (Party 2)
Shared Resources

Problem Reformulation

$$
\begin{aligned}
\text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^{\mathsf{T}} \mathrm{x}_k, & \\
\text{subject to} \quad & \mathrm{A}_k \mathrm{x}_k \leq \mathrm{s}_k, & k \in \mathcal{K}, \\
& \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, & k \in \mathcal{K}, \\
& \sum_{k \in \mathcal{K}} \mathrm{s}_k = \mathrm{c}, & \\
& \mathrm{s}_k \geq 0, & k \in \mathcal{K}.
\end{aligned}
$$

Problem Reformulation

$$L(\mathrm{x}, \mathrm{s}, \boldsymbol{\lambda}) := \mathrm{c}^{\mathsf{T}}\boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} \mathrm{u}_k^{\mathsf{T}}\mathrm{x}_k - \mathrm{s}_k^{\mathsf{T}}\boldsymbol{\lambda}$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathrm{u}_k^{\mathsf{T}}\mathrm{x}_k - \mathrm{s}_k^{\mathsf{T}}\boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathrm{A}_k\mathrm{x}_k \leq \mathrm{s}_k, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathrm{s}_k \geq 0. \end{aligned}$$

ERASMUS UNIVERSITEIT ROTTERDAM

Problem Reformulation

$$L(\mathrm{x}, \mathrm{s}, \boldsymbol{\lambda}) := \mathrm{c}^{\intercal}\boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} \mathrm{u}_k^{\intercal}\mathrm{x}_k - \mathrm{s}_k^{\intercal}\boldsymbol{\lambda}$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathrm{u}_k^{\intercal}\mathrm{x}_k - \mathrm{s}_k^{\intercal}\boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathrm{A}_k\mathrm{x}_k \leq \mathrm{s}_k, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathrm{s}_k \geq 0. \end{aligned}$$

Problem Reformulation

$$g(\lambda; \mathcal{D}_{\mathcal{K}}) := \text{maximize} \sum_{k\in\mathcal{K}} u_k^\top x_k + \left(c - \sum_{k\in\mathcal{K}} s_k\right)^\top \lambda,$$

$$\begin{aligned} \text{subject to } & A_k x_k \le s_k, && k \in \mathcal{K}, \\ & x_k \in \boldsymbol{\mathcal{X}}_k, && k \in \mathcal{K}, \\ & s_k \ge 0, && k \in \mathcal{K}. \end{aligned}$$

ERASMUS UNIVERSITEIT ROTTERDAM

Problem Reformulation: Lagrange Dual Model

$$g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}}) = \mathrm{c}^{\intercal}\boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k)$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := &\text{maximize} && \mathrm{u}_k^{\intercal}\mathrm{x}_k - \mathrm{s}_k^{\intercal}\boldsymbol{\lambda}, \\ &\text{subject to} && \mathrm{A}_k \mathrm{x}_k \leq \mathrm{s}_k, \\ & && \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & && \mathrm{s}_k \geq 0. \end{aligned}$$

$$\min_{\boldsymbol{\lambda}} \; g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}})$$

ERASMUS UNIVERSITEIT ROTTERDAM

Problem Reformulation: Lagrange Dual Model

$$g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}}) = \mathsf{c}^\intercal \boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k)$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathsf{u}_k^\intercal \mathsf{x}_k - \mathsf{s}_k^\intercal \boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathsf{A}_k \mathsf{x}_k \leq \mathsf{s}_k, \\ & \mathsf{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathsf{s}_k \geq 0. \end{aligned}$$

$$\min_{\boldsymbol{\lambda}} \; g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}})$$

Problem Reformulation: Lagrange Dual Model

$$g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}}) = \mathsf{c}^\intercal \boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k)$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathsf{u}_k^\intercal \mathsf{x}_k - \mathsf{s}_k^\intercal \boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathsf{A}_k \mathsf{x}_k \leq \mathsf{s}_k, \\ & \mathsf{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathsf{s}_k \geq 0. \end{aligned}$$

$$\min_{\boldsymbol{\lambda}} g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}})$$

ERASMUS UNIVERSITEIT ROTTERDAM

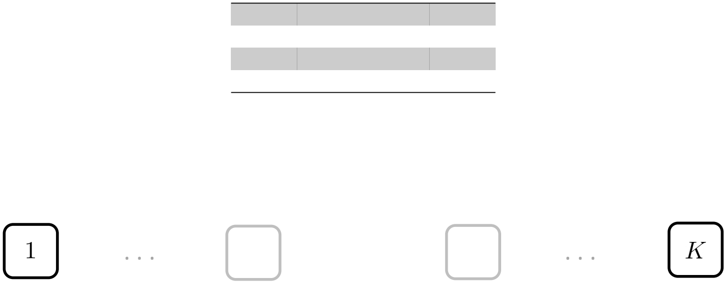
Problem Reformulation: Lagrange Dual Model

$$g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}}) = \mathsf{c}^\intercal \boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k)$$

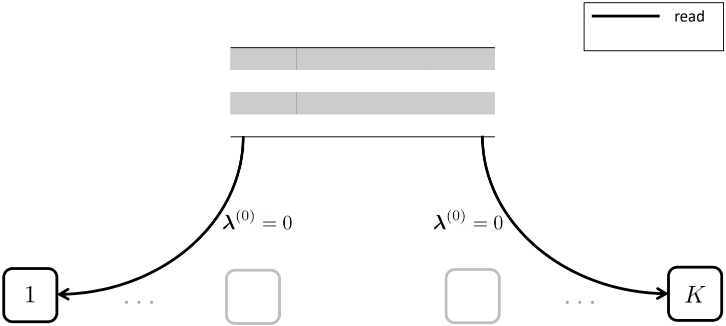
$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathsf{u}_k^\intercal \mathsf{x}_k - \mathsf{s}_k^\intercal \boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathsf{A}_k \mathsf{x}_k \leq \mathsf{s}_k, \\ & \mathsf{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathsf{s}_k \geq 0. \end{aligned}$$

$$\min_{\boldsymbol{\lambda}} g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}})$$

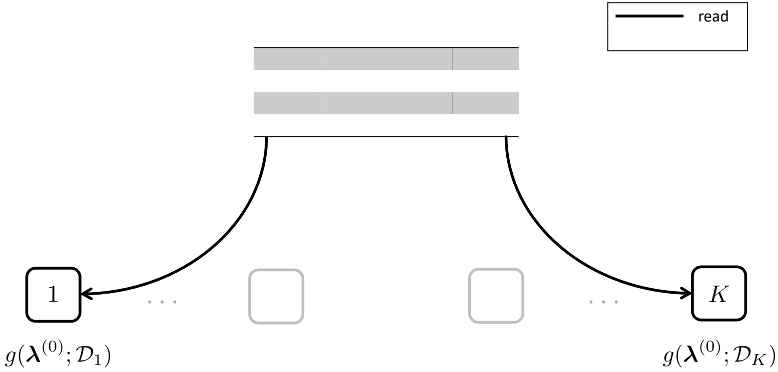
Methodology: Data-hiding via Decomposition



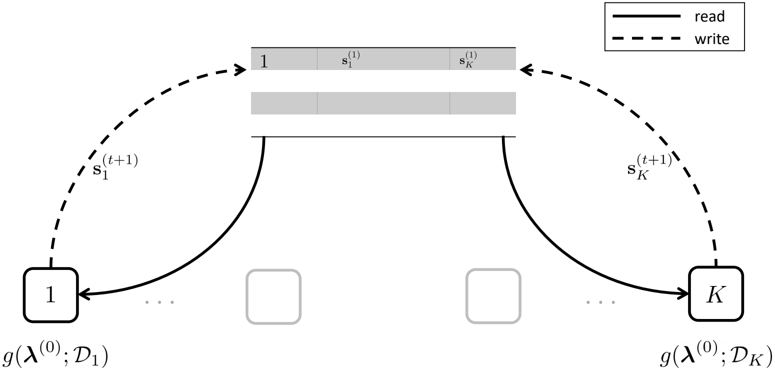
Methodology: Data-hiding via Decomposition



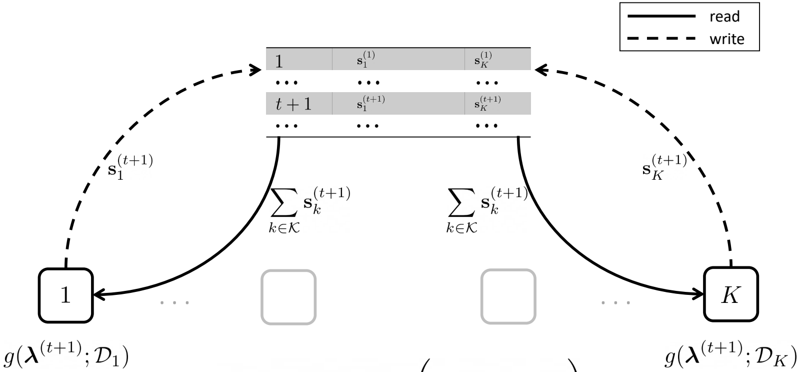
Methodology: Data-hiding via Decomposition



Methodology: Data-hiding via Decomposition



Methodology: Data-hiding via Decomposition



$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathbf{c} - \sum_{k\in\mathcal{K}} \mathbf{s}_k^{(t+1)} \right)$$

Theoretical Results

$$\begin{aligned} \text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^\mathsf{T} \mathrm{x}_k, \\ \text{subject to} \quad & \sum_{k \in \mathcal{K}} \mathrm{A}_k \mathrm{x}_k \leq \mathrm{c}, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \qquad\qquad k \in \mathcal{K} \end{aligned}$$

$$g(\boldsymbol{\lambda}; \mathcal{D}_\mathcal{K}) = \mathrm{c}^\mathsf{T} \boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k)$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_k) := \text{maximize} \quad & \mathrm{u}_k^\mathsf{T} \mathrm{x}_k - \mathrm{s}_k^\mathsf{T} \boldsymbol{\lambda}, \\ \text{subject to} \quad & \mathrm{A}_k \mathrm{x}_k \leq \mathrm{s}_k, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \mathrm{s}_k \geq 0. \end{aligned}$$

ERASMUS UNIVERSITEIT ROTTERDAM

Theoretical Results

$$\begin{aligned} \text{maximize} \quad & \sum_{k \in \mathcal{K}} \mathrm{u}_k^\intercal \mathrm{x}_k, \\ \text{subject to} \quad & \sum_{k \in \mathcal{K}} \mathrm{A}_k \mathrm{x}_k \leq \mathrm{c}, \\ & \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \qquad k \in \mathcal{K} \end{aligned}$$

$$\begin{aligned} g(\boldsymbol{\lambda}; \mathcal{D}_{\mathcal{K}}) =& \mathrm{c}^\intercal \boldsymbol{\lambda} + \sum_{k \in \mathcal{K}} g(\boldsymbol{\lambda}; \mathcal{D}_k) \\ g(\boldsymbol{\lambda}; \mathcal{D}_k) :=& \text{maximize} \quad \mathrm{u}_k^\intercal \mathrm{x}_k - \mathrm{s}_k^\intercal \boldsymbol{\lambda}, \\ & \text{subject to} \quad \mathrm{A}_k \mathrm{x}_k \leq \mathrm{s}_k, \\ & \qquad \mathrm{x}_k \in \boldsymbol{\mathcal{X}}_k, \\ & \qquad \mathrm{s}_k \geq 0. \end{aligned}$$

Pros:

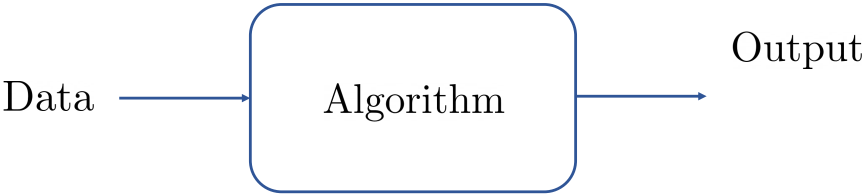
- Almost no data is shared except s_k
- Convergence to optimal

Cons:

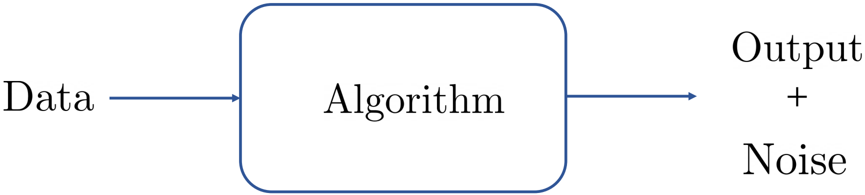
- Information leakage
- No formal privacy guarantee

ERASMUS UNIVERSITEIT ROTTERDAM

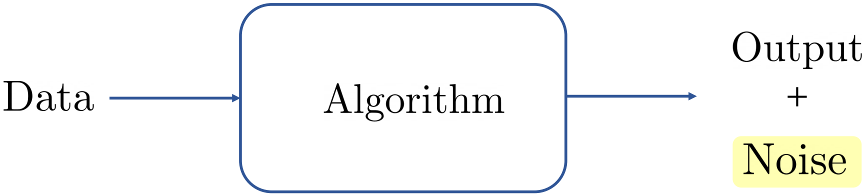
Basics of Differential Privacy



Basics of Differential Privacy

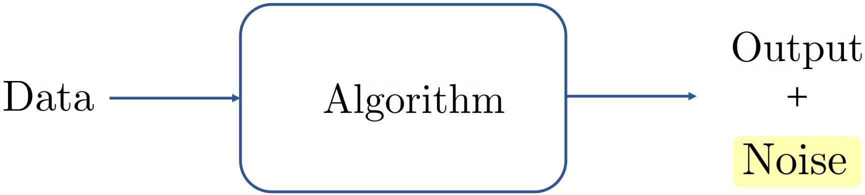


Basics of Differential Privacy: Laplace Mechanism



$$\text{Noise} \sim \text{Lap}(0, \Delta f/\varepsilon)$$

Basics of Differential Privacy: Sensitivity



$$\text{Noise} \sim \text{Lap}(0, \Delta f / \varepsilon)$$

Basics of Differential Privacy: Basic Composition Theorem

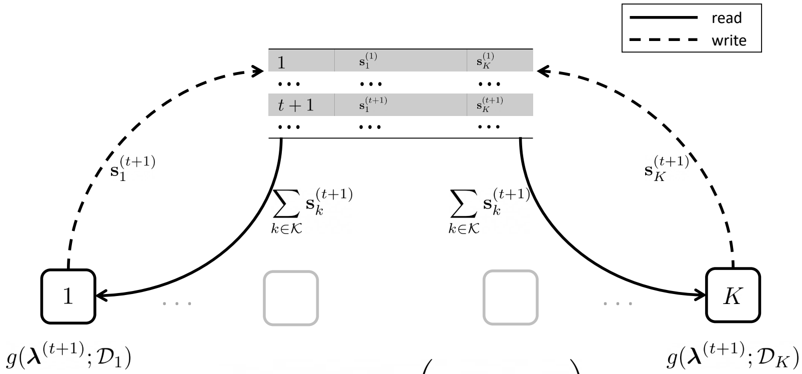
(ε, δ) Algorithm + (ε, δ) Algorithm

$=$

$(2\varepsilon, 2\delta)$ Algorithm

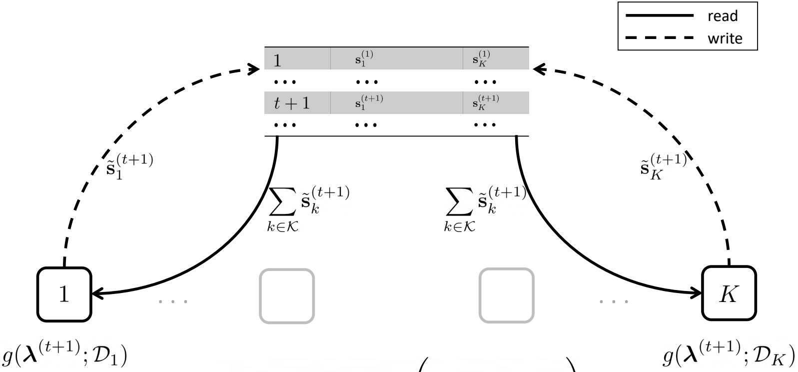
ERASMUS UNIVERSITEIT ROTTERDAM

Recall: Data-hiding via Decomposition



$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathbf{c} - \sum_{k \in \mathcal{K}} \mathbf{s}_k^{(t+1)} \right)$$

Differentially Private Algorithm



$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathbf{c} - \sum_{k\in\mathcal{K}} \tilde{\mathbf{s}}_k^{(t+1)} \right)$$

Differentially Private Algorithm

$$\begin{aligned} \left(\mathrm{x}_k^{(t+1)}, \mathrm{s}_k^{(t+1)}\right)_{k\in\mathcal{K}} &= \arg\max_{\mathrm{x},\mathrm{s}} L(\mathrm{x}, \mathrm{s}, \boldsymbol{\lambda}^{(t)}), \\ \boldsymbol{\lambda}^{(t+1)} &= \boldsymbol{\lambda}^{(t)} - \nu^{(t)}\left(\mathrm{c} - \textstyle\sum_{k\in\mathcal{K}} \tilde{\mathrm{s}}_k^{(t+1)}\right), \end{aligned} \tag{1}$$

$$\tilde{\mathrm{s}}_k^{(t+1)} = \mathrm{s}_k^{(t+1)} + \boldsymbol{\omega}_k^{(t+1)},$$

$\boldsymbol{\omega}_k \sim \mathrm{Lap}(0, T\Delta_k/\varepsilon)$.
$\Delta_k = \|\bar{\mathrm{s}}_k\|_\infty$:

- If no agreement: $\bar{\mathrm{s}}_k \leq \mathrm{c}$.

ERASMUS UNIVERSITEIT ROTTERDAM

Differentially Private Algorithm

After T iteration, the difference between ε-differentially private algorithm objective function and optimal objective function:

ε-differential privacy

$$\min_{t=1,\dots,T-1}(\mathbb{E}[L(\mathrm{x}_k^{(t+1)}, \mathrm{s}_k^{(t+1)}, \boldsymbol{\lambda}^{(t)}) - L(\mathrm{x}_k^*, \mathrm{s}_k^*, \boldsymbol{\lambda}^*)]) \leq M\sqrt{\frac{2T\sigma}{\varepsilon^2} + \frac{\|\bar{\mathrm{s}}_{\mathcal{K}}\|^2}{T}}.$$

$\|\boldsymbol{\lambda}^{(0)} - \boldsymbol{\lambda}^*\| \leq M$, $\sigma = \sum_{k\in\mathcal{K}} \|\bar{\mathrm{s}}_k\|^2$ and $\bar{\mathrm{s}}_{\mathcal{K}} = \sum_{k\in\mathcal{K}} \bar{\mathrm{s}}_k$.

(ε, δ)-differential privacy ($\varepsilon \in (0, 0.9)$ ve $\delta \in (0, 1]$)

$$\min_{t=1,\dots,T-1}(\mathbb{E}[L(\mathrm{x}_k^{(t+1)}, \mathrm{s}_k^{(t+1)}, \boldsymbol{\lambda}^{(t)}) - L(\mathrm{x}_k^*, \mathrm{s}_k^*, \boldsymbol{\lambda}^*)]) \leq M\sqrt{\frac{8\log\left(e + \frac{\varepsilon}{\delta}\right)\sigma}{\varepsilon^2} + \frac{\|\bar{\mathrm{s}}_{\mathcal{K}}\|^2}{T}},$$

$\|\boldsymbol{\lambda}^{(0)} - \boldsymbol{\lambda}^*\| \leq M$, $\sigma = \sum_{k\in\mathcal{K}} \|\bar{\mathrm{s}}_k\|^2$ and $\bar{\mathrm{s}}_{\mathcal{K}} = \sum_{k\in\mathcal{K}} \bar{\mathrm{s}}_k$.

Differentially Private Algorithm

After T iteration, the difference between ε-differentially private algorithm objective function and optimal objective function:

ε-differential privacy

$$\min_{t=1,\ldots,T-1}(\mathbb{E}[L(\mathrm{x}_k^{(t+1)},\mathrm{s}_k^{(t+1)},\boldsymbol{\lambda}^{(t)})-L(\mathrm{x}_k^*,\mathrm{s}_k^*,\boldsymbol{\lambda}^*)])\leq M\sqrt{\frac{2T\sigma}{\varepsilon^2}+\frac{\|\bar{\mathrm{s}}_{\mathcal{K}}\|^2}{T}}.$$

$\|\boldsymbol{\lambda}^{(0)}-\boldsymbol{\lambda}^*\|\leq M$, $\sigma=\sum_{k\in\mathcal{K}}\|\bar{\mathrm{s}}_k\|^2$ and $\bar{\mathrm{s}}_{\mathcal{K}}=\sum_{k\in\mathcal{K}}\bar{\mathrm{s}}_k$.

(ε,δ)-differential privacy ($\varepsilon\in(0,0.9)$ ve $\delta\in(0,1]$)

$$\min_{t=1,\ldots,T-1}(\mathbb{E}[L(\mathrm{x}_k^{(t+1)},\mathrm{s}_k^{(t+1)},\boldsymbol{\lambda}^{(t)})-L(\mathrm{x}_k^*,\mathrm{s}_k^*,\boldsymbol{\lambda}^*)])\leq M\sqrt{\frac{8\log\left(e+\frac{\varepsilon}{\delta}\right)\sigma}{\varepsilon^2}+\frac{\|\bar{\mathrm{s}}_{\mathcal{K}}\|^2}{T}},$$

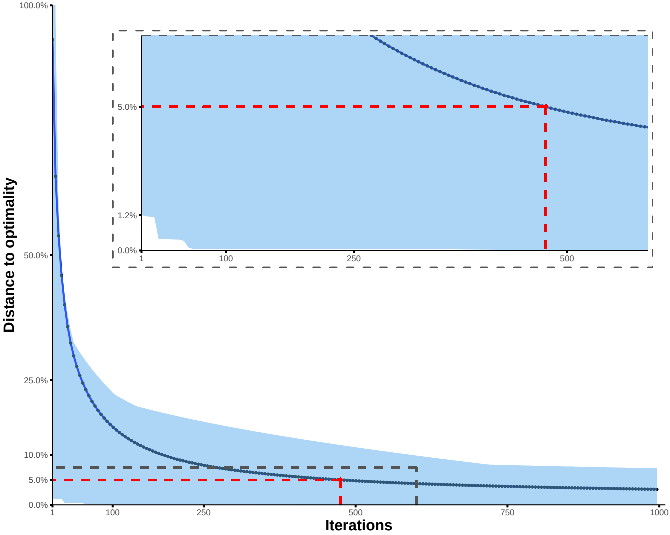
$\|\boldsymbol{\lambda}^{(0)}-\boldsymbol{\lambda}^*\|\leq M$, $\sigma=\sum_{k\in\mathcal{K}}\|\bar{\mathrm{s}}_k\|^2$ and $\bar{\mathrm{s}}_{\mathcal{K}}=\sum_{k\in\mathcal{K}}\bar{\mathrm{s}}_k$.

ERASMUS UNIVERSITEIT ROTTERDAM

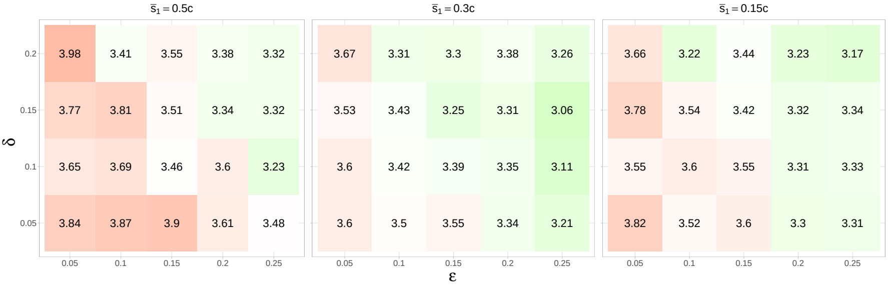
Simulation Study: The Setup

- Production planning example
- Five parties sharing five capacities
- Individual capacities and demand constraints
- Diminishing step-length
- Results over 100 simulation runs
- Focus is on one party ($k = 1$)

Simulation Study: Data-Private Model



Simulation Study: Differential Privacy($\bar{s}_{\mathcal{K}} = 1.20c$)



Simulation Study: Differential Privacy($\bar{s}_{\mathcal{K}} = 1.50c$)

$\bar{s}_1 = 0.5c$

δ \ ε	0.05	0.1	0.15	0.2	0.25
0.2	13.6	11.69	10.76	9	9.71
0.15	13.46	12.42	10.56	9.76	9.55
0.1	12.32	11.86	10.84	11.25	9.55
0.05	13.92	11.52	12.07	11.99	10.78

$\bar{s}_1 = 0.3c$

δ \ ε	0.05	0.1	0.15	0.2	0.25
0.2	13.94	11.64	10.27	9.28	9.11
0.15	13.3	12.2	10.63	9.46	8.71
0.1	12.49	11.5	10.38	11.23	9.61
0.05	14	11.4	12.02	11.3	10.6

$\bar{s}_1 = 0.15c$

δ \ ε	0.05	0.1	0.15	0.2	0.25
0.2	14.61	12.25	11.27	11.13	9.27
0.15	14.08	13.25	11.71	10.52	9.77
0.1	13.55	12.31	11.01	12.51	10.99
0.05	14.83	13.02	12.62	11.61	11.08

Some Progress...

- Current results with diminishing step length
- Upgrades: Momentum based updates on (stochastic) subgradient method

$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathsf{c} - \sum_{k \in \mathcal{K}} \mathsf{s}_k^{(t+1)} \right) + \rho \left(\boldsymbol{\lambda}^{(t)} - \boldsymbol{\lambda}^{(t-1)} \right)$$

$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathsf{c} - \sum_{k \in \mathcal{K}} \tilde{\mathsf{s}}_k^{(t+1)} \right) + \rho \left(\boldsymbol{\lambda}^{(t)} - \boldsymbol{\lambda}^{(t-1)} \right)$$

  - Better results on data-private model
  - Theoretically a tighter bound for the differentially-private model

ERASMUS UNIVERSITEIT ROTTERDAM

Some Progress...

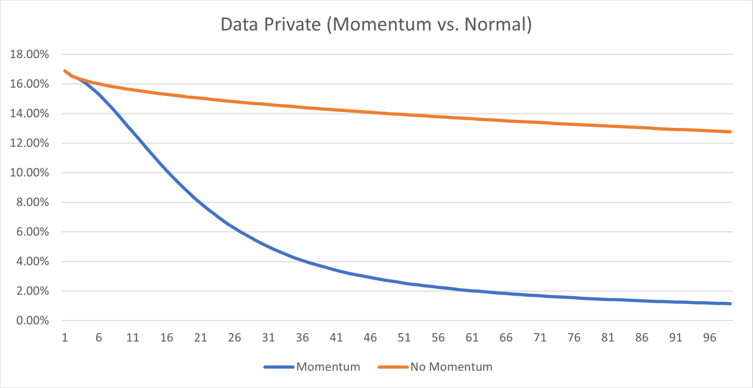
- Current results with diminishing step length
- Upgrades: Momentum based updates on (stochastic) subgradient method

$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathsf{c} - \sum_{k \in \mathcal{K}} \mathsf{s}_k^{(t+1)} \right) + \rho \left(\boldsymbol{\lambda}^{(t)} - \boldsymbol{\lambda}^{(t-1)} \right)$$

$$\boldsymbol{\lambda}^{(t+1)} = \boldsymbol{\lambda}^{(t)} - \nu^{(t)} \left(\mathsf{c} - \sum_{k \in \mathcal{K}} \tilde{\mathsf{s}}_k^{(t+1)} \right) + \rho \left(\boldsymbol{\lambda}^{(t)} - \boldsymbol{\lambda}^{(t-1)} \right)$$

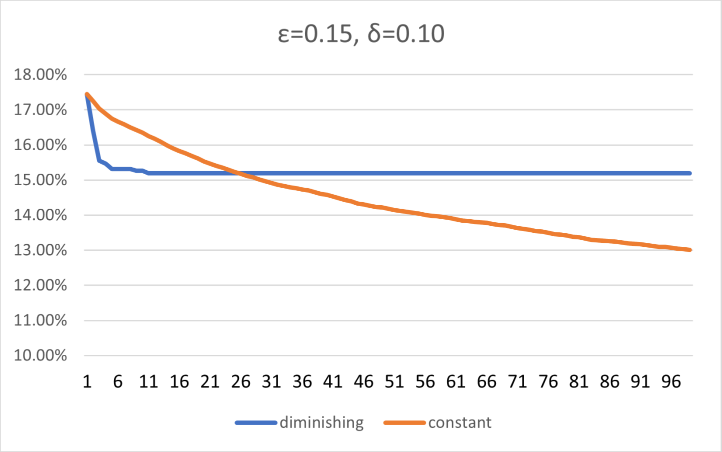
  - Better results on data-private model
  - Theoretically a tighter bound for the differentially-private model

Progress on Data-Private Model



ERASMUS UNIVERSITEIT ROTTERDAM

Progress on Differentially Private Model



Next Steps...

- Privacy in other mathematical models
- Feasibility of the solutions
- Real-life applications

Thank you!
Questions & Comments: karaca@ese.eur.nl