# On the application of optimization methods for secured multiparty computations

**C. Weeraddana**[⋆], G. Athanasiou[⋆], M. Jakobsson[⋆], C. Fischione[⋆], and J. S. Baras[⋆⋆]

[⋆]KTH Royal Institute of Technology, Stockholm, Sweden
[⋆⋆]University of Maryland, MD, USA
{chatw, georgioa, mjakobss, carlofi}@kth.se; baras@umd.edu

ACCESS ISS 18.09.13

# Motivation – Why Privacy/Security ?

# Motivation – Why Privacy/Security ?

- social networks


# Motivation – Why Privacy/Security ?

- social networks
- healthcare data



# Motivation – Why Privacy/Security ?

- social networks
- healthcare data
- e-commerce




# Motivation – Why Privacy/Security ?

- social networks
- healthcare data
- e-commerce
- banks, and government services




# Motivation – Why Privacy/Security ?

- real world:
  - different parties, such as persons and organizations **always interact**
  - they collaborate for mutual benefits

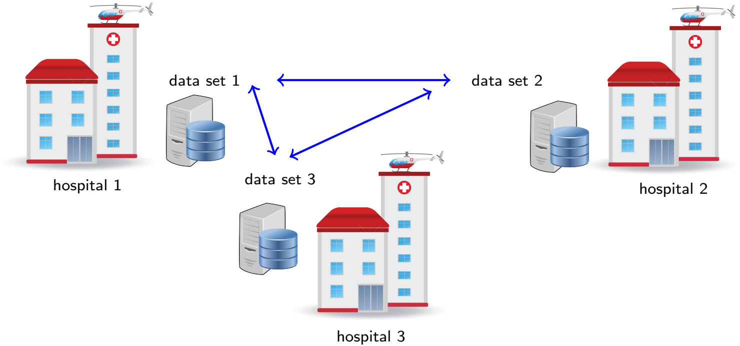
# Motivation – Why Privacy/Security ?

- real world:
  - different parties, such as persons and organizations **always interact**
  - they collaborate for mutual benefits

- collaboration is more appealing **if** security/privacy is guaranteed

# Real World

- **example 1**
  - hospitals coordinate $\Rightarrow$ inference for better diagnosis
  - larger data sets $\Rightarrow$ higher the accuracy of the inference
  - **challenge:** neither of the data set should be revealed

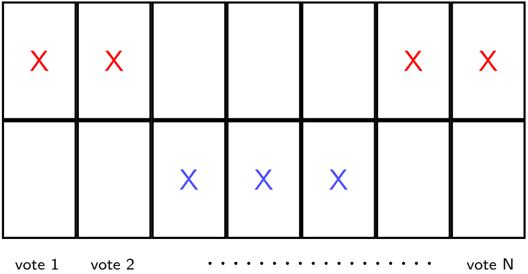


# Real World

- **example 2**
  - cloud customers outsource their problems to the cloud
  - **challenge:** problem data shouldn't be revealed to the cloud

# Real World

- **example 3**
  - secured e-voting systems
  - **challenge:** neither of the vote should be revealed

# Secured Multiparty Computation

- solve, **in a secured manner**, the $n$-party problem of the form:

$$f(\mathbf{A}_1, \ldots, \mathbf{A}_n) = \inf_{\mathbf{x} \in \{\mathbf{x} | \mathbf{g}(\mathbf{x}, \mathbf{A}_1, \ldots, \mathbf{A}_n) \preceq \mathbf{0}\}} f_0(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{A}_1, \ldots, \mathbf{A}_n)$$

- $\mathbf{A}_i$ is the private data belonging to party $i$
- $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is the decision variable
- $f_0(\cdot)$ is the global objective function
- $\mathbf{g}(\cdot)$ is the vector-valued constraint function
- $f(\cdot)$ is the desired optimal value

# Secured Multiparty Computation

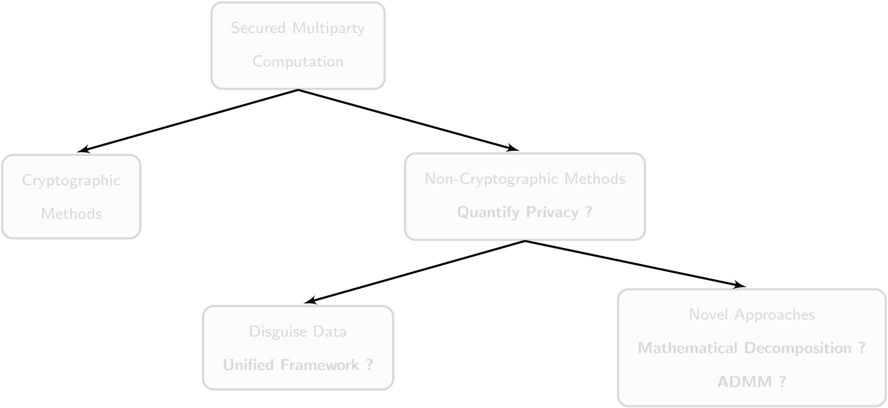
- solve, **in a secured manner**, the $n$-party problem of the form:

$$f(\mathbf{A}_1, \ldots, \mathbf{A}_n) = \inf_{\mathbf{x} \in \{\mathbf{x} | \mathbf{g}(\mathbf{x}, \mathbf{A}_1, \ldots, \mathbf{A}_n) \preceq \mathbf{0}\}} f_0(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{A}_1, \ldots, \mathbf{A}_n)$$

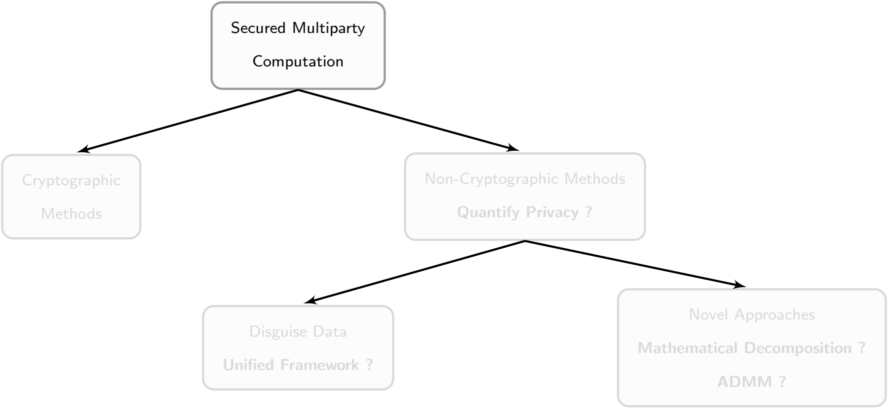
  - $\mathbf{A}_i$ is the private data belonging to party $i$
  - $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is the decision variable
  - $f_0(\cdot)$ is the global objective function
  - $\mathbf{g}(\cdot)$ is the vector-valued constraint function
  - $f(\cdot)$ is the desired optimal value

- can we perform such computations with "acceptable" privacy guaranties ?

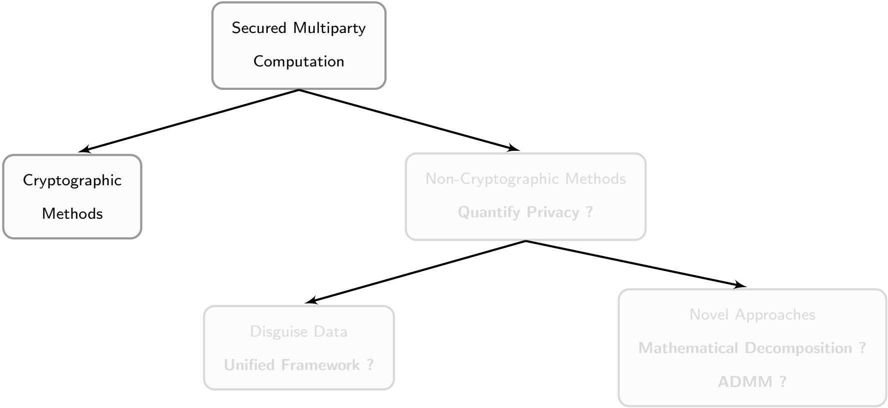
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

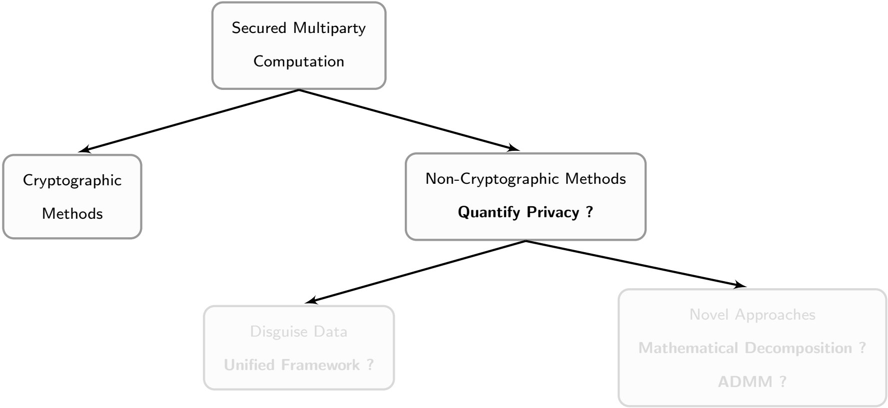
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

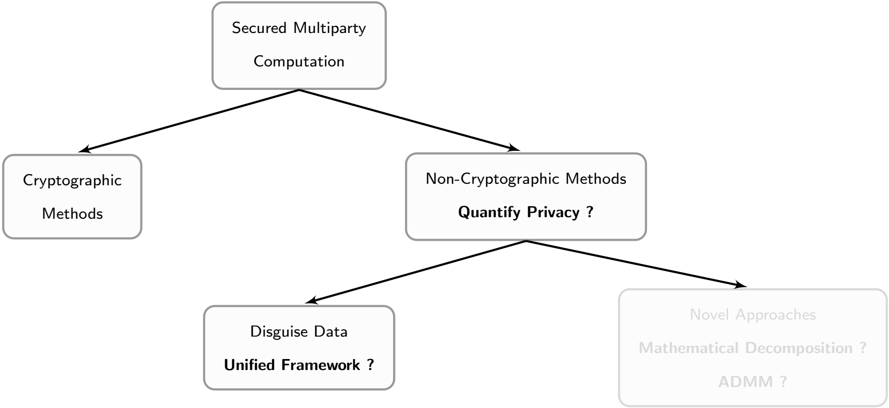
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

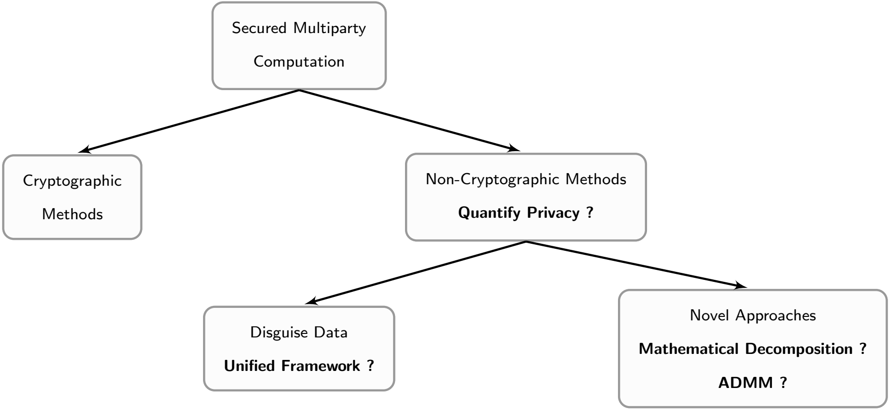
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
**Quantify Privacy ?**
Disguise Data
**Unified Framework ?**
Novel Approaches
**Mathematical Decomposition ?**
**ADMM ?**

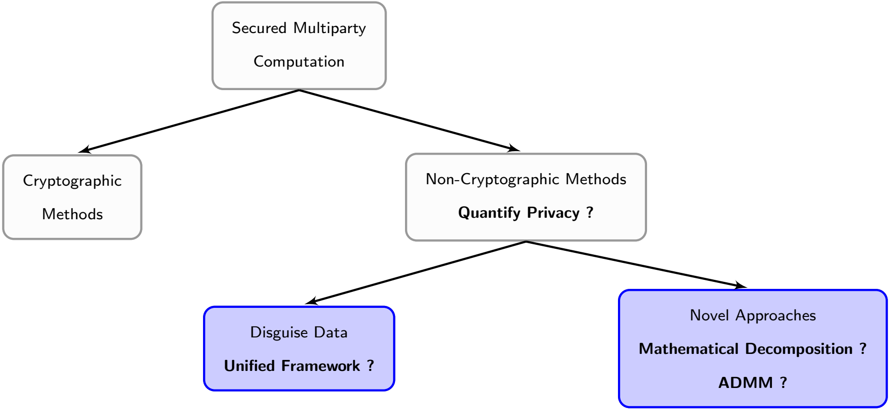
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

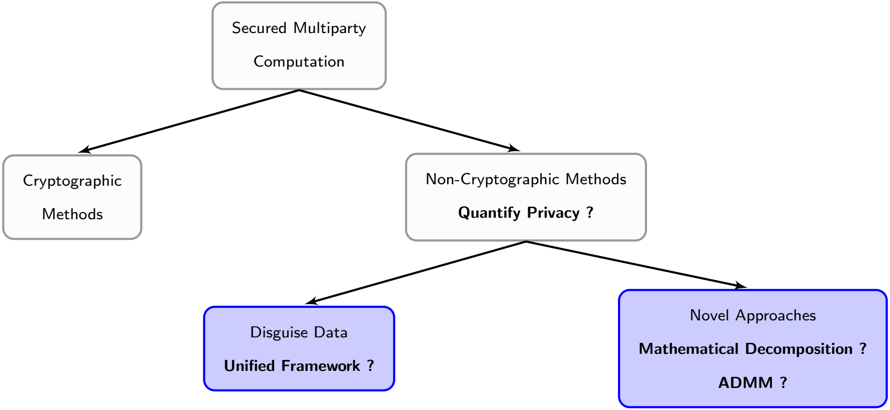
# Overview


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

# Overview


Secured Multiparty
Computation
Cryptographic
Methods
Non-Cryptographic Methods
Quantify Privacy ?
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

# Our Contributions



# Our Contributions

ROYAL INSTITUTE OF TECHNOLOGY

- **unified framework** for existing methods for disguising private data
  - absence of a systematic approach reduces the scope of applicability
  - unintended mistakes (e.g., [Du01, Vai09])
  - standard proof techniques for privacy guaranties.
- **decomposition methods, ADMM**
- **general definition** for privacy ⇒ quantify the privacy
- **a number of examples**
- **comparison**: efficiency, scalability, and many others
- for details, see [WAJ+13]

[WAJ+13] P. C. Weeraddana, G. Athanasiou, M. Jakobsson, C. Fischione, and J. S. Baras. Per-se privacy preserving distributed optimization

# UNIFIED FRAMEWORK FOR DISGUISING PRIVATE DATA

# General Formulation

ROYAL INSTITUTE OF TECHNOLOGY

we pose the design or decision making problem

$$\begin{array}{ll} \text{minimize} & f_0(\mathbf{x}) \\ \text{subject to} & f_i(\mathbf{x}) \leq 0, \; i = 1, \ldots, q \\ & \mathbf{C}\mathbf{x} - \mathbf{d} = \mathbf{0} \end{array} \quad (1)$$

- optimization variable is $\mathbf{x} \in \mathbb{R}^n$
- $f_i, \; i = 0, \ldots, q$ are *convex*
- $\mathbf{C} \in \mathbb{R}^{p \times n}$ with $\text{rank}(\mathbf{C}) = p$
- $\mathbf{d} \in \mathbb{R}^p$

- **we would like to solve the problem in a privacy preserving manner**

# Unification, Disguising Private Data for SMC

## Proposition (change of variables)

- $\phi : \mathbb{R}^m \to \mathbb{R}^n$ *be a function, with image covering the problem domain* $\mathcal{D}$
- *change of variables:*

$$\mathbf{x} = \phi(\mathbf{z}) \ . \tag{2}$$

- *resulting problem:*

$$\begin{array}{ll} \text{minimize} & f_0(\phi(\mathbf{z})) \\ \text{subject to} & f_i(\phi(\mathbf{z})) \leq 0, \ i = 1, \dots, q \\ & \mathbf{C}\phi(\mathbf{z}) - \mathbf{d} = \mathbf{0} \end{array} \tag{3}$$

- $\mathbf{x}^\star$ *solves problem (1)* $\Rightarrow \mathbf{z}^\star = \phi^{-1}(\mathbf{x}^\star)$ *solves problem (3)*
- $\mathbf{z}^\star$ *solves problem (3)* $\Rightarrow \mathbf{x}^\star = \phi(\mathbf{z}^\star)$ *solves problem (1)*

# Unification, Disguising Private Data for SMC

## Proposition (change of variables)

- $\phi : \mathbb{R}^m \to \mathbb{R}^n$ *be a function, with image covering the problem domain* $\mathcal{D}$
- *change of variables:*

$$\mathbf{x} = \phi(\mathbf{z}) \ . \tag{2}$$

- *resulting problem:*

$$\begin{array}{ll} \textit{minimize} & f_0(\phi(\mathbf{z})) \\ \textit{subject to} & f_i(\phi(\mathbf{z})) \leq 0, \ i = 1, \dots, q \\ & \mathbf{C}\phi(\mathbf{z}) - \mathbf{d} = \mathbf{0} \end{array} \tag{3}$$

- $\mathbf{x}^\star$ *solves problem (1)* $\Rightarrow \mathbf{z}^\star = \phi^{-1}(\mathbf{x}^\star)$ *solves problem (3)*
- $\mathbf{z}^\star$ *solves problem (3)* $\Rightarrow \mathbf{x}^\star = \phi(\mathbf{z}^\star)$ *solves problem (1)*

privacy is via the function compositions:

$$\hat{f}_i(\mathbf{z}) = f_i(\phi(\mathbf{z})) \ , \ \mathrm{dom} \hat{f}_i = \{\mathbf{z} \in \mathrm{dom}\phi \mid \phi(\mathbf{z}) \in \mathrm{dom} f_i\}$$

$$\hat{h}_i(\mathbf{z}) = \mathbf{C}\phi(\mathbf{z}) - \mathbf{d} \ , \ \mathrm{dom}\hat{h}_i = \{\mathbf{z} \in \mathrm{dom}\phi \mid \phi(\mathbf{z}) \in \mathbb{R}^n\}$$

# Example of Change of Variables

- **original problem (big LP):**

$$\begin{array}{ll} \text{minimize} & \mathbf{c}^{\mathsf{T}}\mathbf{x} \\ \text{subject to} & \mathbf{A}\mathbf{x} \geq \mathbf{b} \end{array}$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$

# Example of Change of Variables

- **original problem (big LP):**

$$\begin{array}{ll} \text{minimize} & \mathbf{c}^{\mathsf{T}}\mathbf{x} \\ \text{subject to} & \mathbf{A}\mathbf{x} \geq \mathbf{b} \end{array}$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$

- **affine transformation:** $\mathbf{x} = \phi(\mathbf{z}) = \mathbf{B}\mathbf{z} - \mathbf{a}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$, $\text{rank}(B) = n$, $\mathbf{a} \in \mathbb{R}^n$.

# Example of Change of Variables

- **original problem (big LP):**

$$\begin{array}{ll} \text{minimize} & \mathbf{c}^{\mathsf{T}}\mathbf{x} \\ \text{subject to} & \mathbf{A}\mathbf{x} \geq \mathbf{b} \end{array}$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$

- **affine transformation:** $\mathbf{x} = \phi(\mathbf{z}) = \mathbf{B}\mathbf{z} - \mathbf{a}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$, rank$(B) = n$, $\mathbf{a} \in \mathbb{R}^n$.

- **equivalent problem (outsourced to the cloud):**

$$\begin{array}{ll} \text{minimize} & \hat{\mathbf{c}}^{\mathsf{T}}\mathbf{z} \\ \text{subject to} & \hat{\mathbf{A}}\mathbf{z} \geq \hat{\mathbf{b}} \end{array}$$

  - variable is $\mathbf{z} \in \mathbb{R}^p$
  - data: $\hat{\mathbf{c}} = \mathbf{B}^{\mathsf{T}}\mathbf{c} \in \mathbb{R}^p$, $\hat{\mathbf{A}} = \mathbf{A}\mathbf{B} \in \mathbb{R}^{m \times p}$, $\hat{\mathbf{b}} = \mathbf{b} - \mathbf{A}\mathbf{a} \in \mathbb{R}^m$

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \dots, K \end{array}$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \dots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \dots, K$

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \ldots, K \end{array}$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \ldots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \ldots, K$

- **affine transformation:** $x_i = \phi_i(z_i) = z_i - \alpha_i$, $n = 1, \ldots, K$.

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \ldots, K \end{array}$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \ldots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \ldots, K$

- **affine transformation:** $x_i = \phi_i(z_i) = z_i - \alpha_i$, $n = 1, \ldots, K$.

- **equivalent problem:**

$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^{K} z_i \\ \text{subject to} & z_i = a_i + \alpha_i \ , i = 1, \ldots, K \end{array}$$

  - variables are $z_i \in \mathbb{R}$, $i = 1, \ldots, K$

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \ldots, K \end{array} \longrightarrow p^\star$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \ldots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \ldots, K$

- **affine transformation:** $x_i = \phi_i(z_i) = z_i - \alpha_i$, $n = 1, \ldots, K$.

- **equivalent problem:**

$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^{K} z_i \\ \text{subject to} & z_i = a_i + \alpha_i \ , i = 1, \ldots, K \end{array}$$

  - variables are $z_i \in \mathbb{R}$, $i = 1, \ldots, K$

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \ldots, K \end{array} \longrightarrow p^\star$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \ldots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \ldots, K$

- **affine transformation:** $x_i = \phi_i(z_i) = z_i - \alpha_i$, $n = 1, \ldots, K$.

- **equivalent problem:**

$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^{K} z_i \\ \text{subject to} & z_i = a_i + \alpha_i \ , i = 1, \ldots, K \end{array} \longrightarrow q^\star$$

  - variables are $z_i \in \mathbb{R}$, $i = 1, \ldots, K$

# Example of Change of Variables

- **original problem (find average of $K$ private numbers):**

$$\begin{array}{ll} \text{minimize} & (1/K)\sum_{i=1}^{K} x_i \\ \text{subject to} & x_i = a_i \ , i = 1, \ldots, K \end{array} \longrightarrow p^\star$$

  - variables are $x_i \in \mathbb{R}$, $i = 1, \ldots, K$
  - private numbers: $a_i \in \mathbb{R}$, $i = 1, \ldots, K$

- **affine transformation:** $x_i = \phi_i(z_i) = z_i - \alpha_i$, $n = 1, \ldots, K$.

- **equivalent problem:**

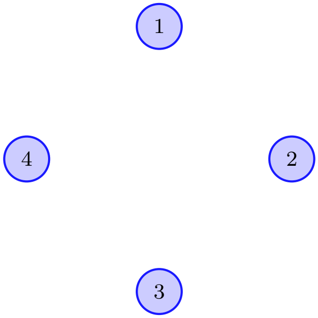
$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^{K} z_i \\ \text{subject to} & z_i = a_i + \alpha_i \ , i = 1, \ldots, K \end{array} \longrightarrow q^\star$$

  - variables are $z_i \in \mathbb{R}$, $i = 1, \ldots, K$

- $p^\star = \frac{1}{K}\left(q^\star - \sum_{i=1}^{K} \alpha_i\right)$

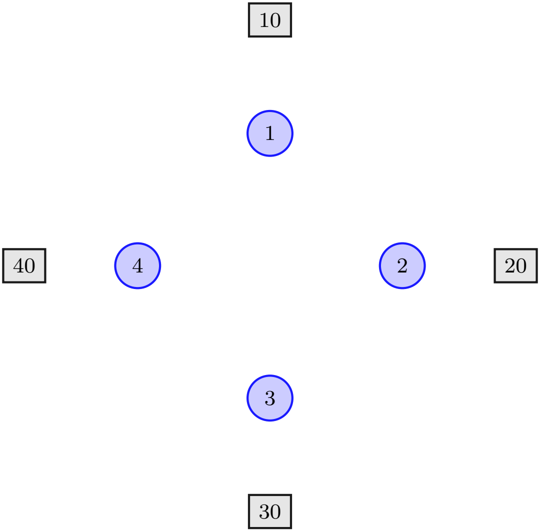
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



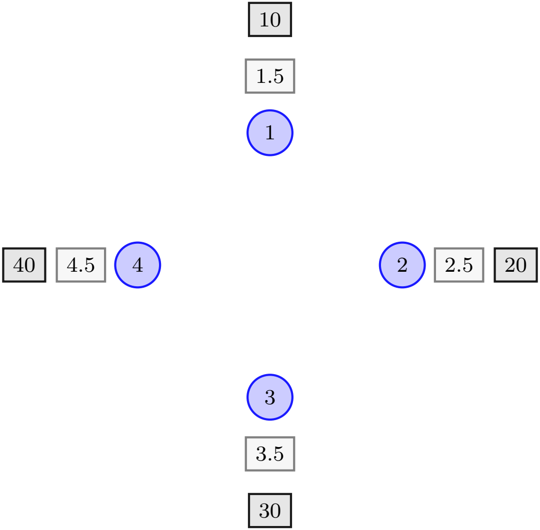
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



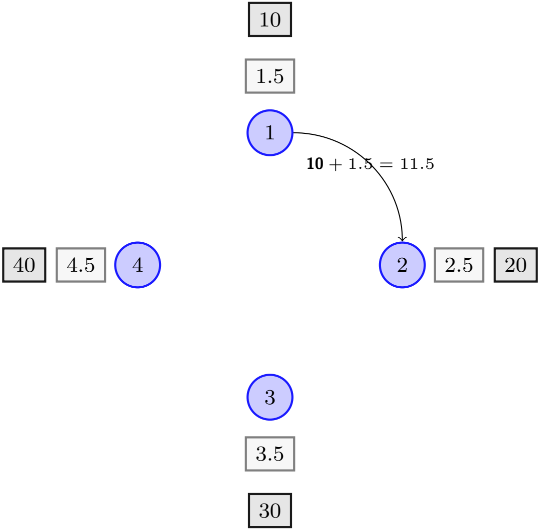
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



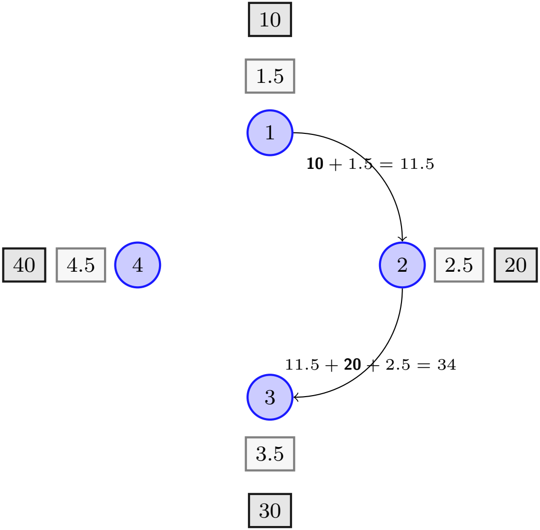
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



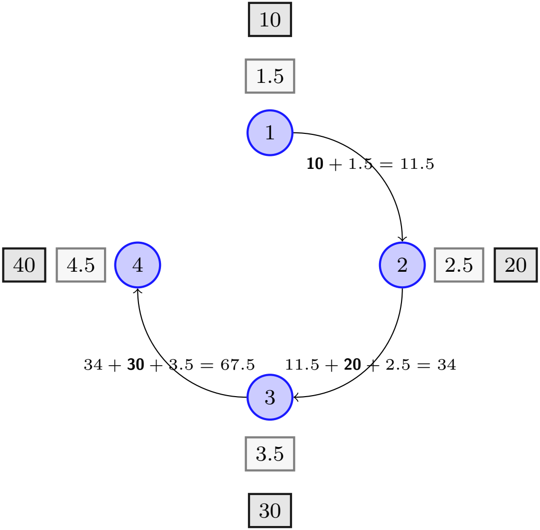
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



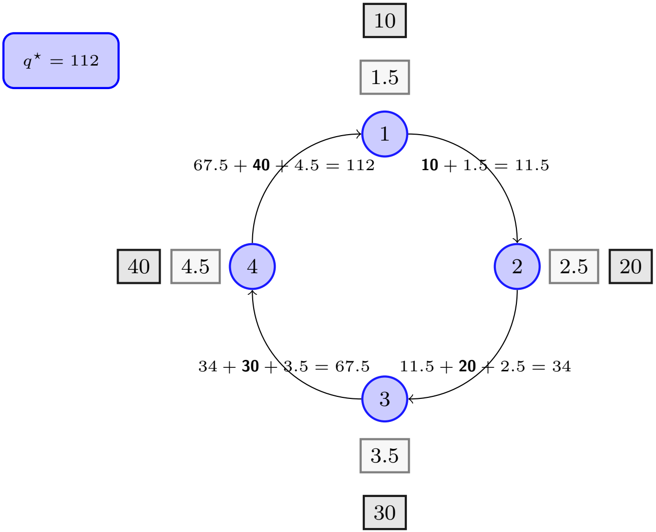
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



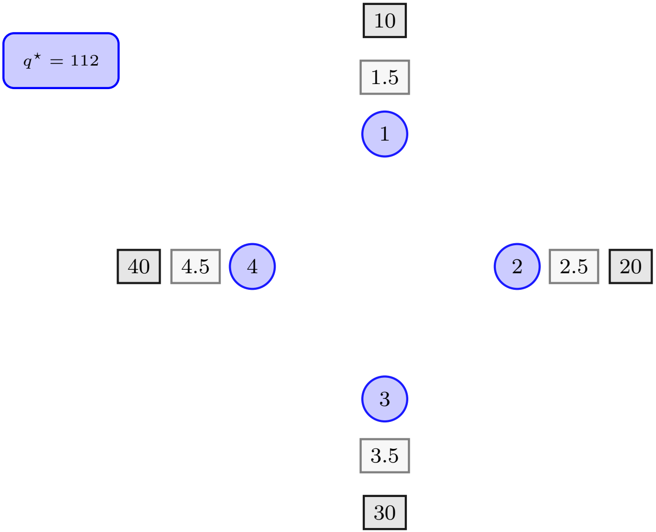
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



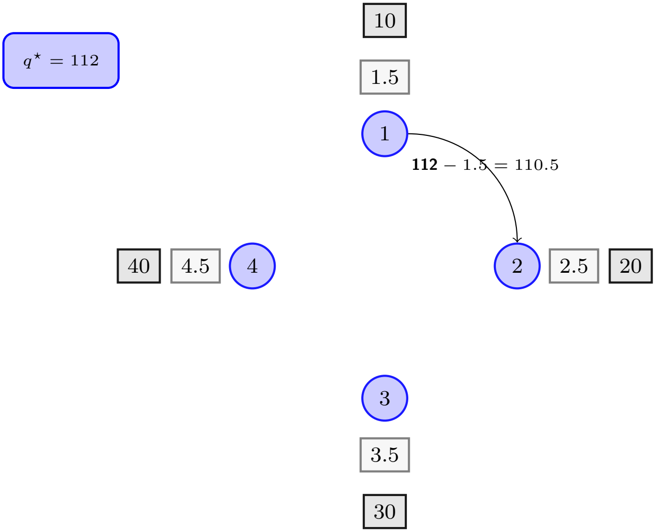
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



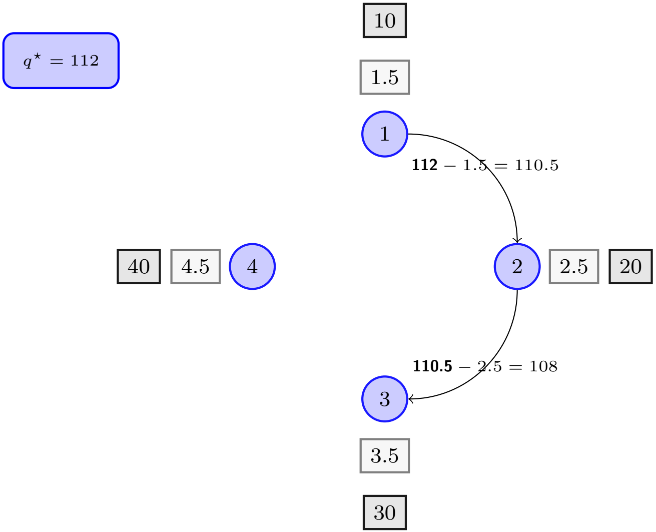
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



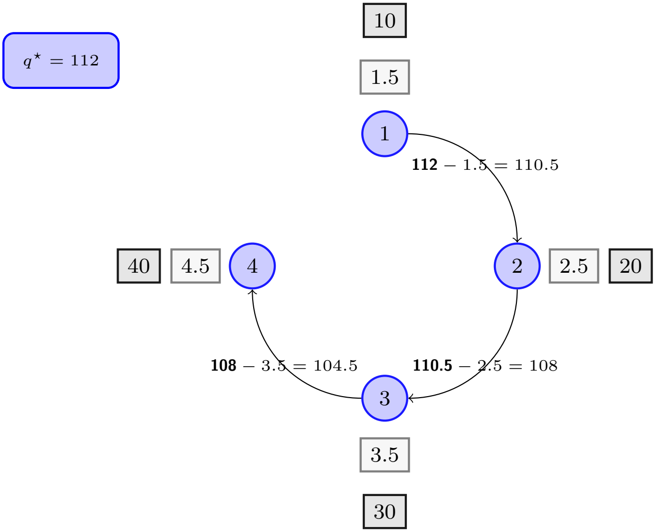
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



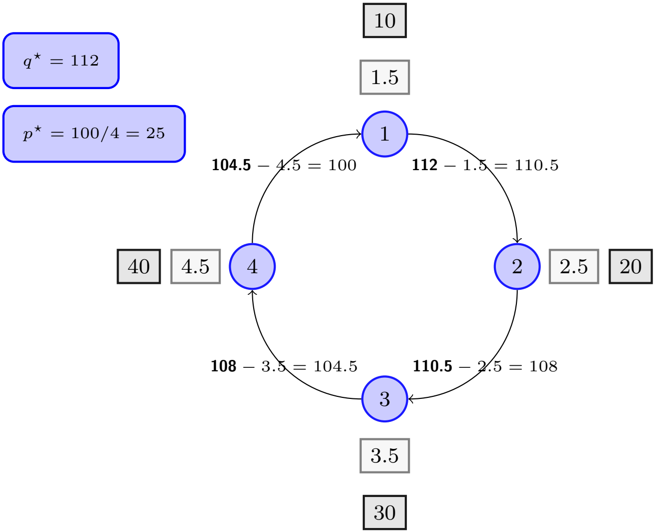
# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



# Example of Change of Variables

- **original problem (find average of $K$ numbers):**



# Unification, Disguising Private Data for SMC

## Proposition (transformation of objective and constraint functions)

- $\psi_0 : \mathbb{D}_0 \subseteq \mathbb{R} \to \mathbb{R}$ *is monotonically increasing and* $\mathbb{D}_0 \supseteq$ *image* $f_0$
- $\psi_i : \mathbb{D}_i \subseteq \mathbb{R} \to \mathbb{R}$, *with* $\mathbb{D}_i \supseteq$ *image* $f_i$ *and* $\psi_i(z) \leq 0 \Leftrightarrow z \leq 0$
- $\psi : \mathbb{R}^p \to \mathbb{R}^m$ *satisfies* $\psi(\mathbf{z}) = \mathbf{0} \Leftrightarrow \mathbf{z} = \mathbf{0}$
- *if* $\mathbf{x}^\star$ *solves*

$$\begin{array}{ll} \text{minimize} & \psi_0(f_0(\mathbf{x})) \\ \text{subject to} & \psi_i(f_i(\mathbf{x})) \leq 0, \; i = 1, \ldots, q \\ & \psi(\mathbf{C}\mathbf{x} - \mathbf{d}) = \mathbf{0} \end{array} \tag{4}$$

  *then solution* $\mathbf{x}^\star$ *problem (1)*
- *the optimal value of problem (1),* $p^\star$*, and that of problem (4),* $q^\star$*, are related by*

$$\psi_0(p^\star) = q^\star \ . \tag{5}$$

# Unification, Disguising Private Data for SMC

KTH VETENSKAP OCH KONST
ROYAL INSTITUTE OF TECHNOLOGY

## Proposition (transformation of objective and constraint functions)

- $\psi_0 : \mathbb{D}_0 \subseteq \mathbb{R} \to \mathbb{R}$ *is monotonically increasing and* $\mathbb{D}_0 \supseteq$ *image*$f_0$
- $\psi_i : \mathbb{D}_i \subseteq \mathbb{R} \to \mathbb{R}$, *with* $\mathbb{D}_i \supseteq$ *image*$f_i$ *and* $\psi_i(z) \leq 0 \Leftrightarrow z \leq 0$
- $\psi : \mathbb{R}^p \to \mathbb{R}^m$ *satisfies* $\psi(\mathbf{z}) = \mathbf{0} \Leftrightarrow \mathbf{z} = \mathbf{0}$
- *if* $\mathbf{x}^\star$ *solves*

$$\begin{array}{ll} \text{minimize} & \psi_0(f_0(\mathbf{x})) \\ \text{subject to} & \psi_i(f_i(\mathbf{x})) \leq 0, \ i = 1, \ldots, q \\ & \psi(\mathbf{C}\mathbf{x} - \mathbf{d}) = \mathbf{0} \end{array} \quad (4)$$

  *then solution* $\mathbf{x}^\star$ *problem (1)*
- *the optimal value of problem (1),* $p^\star$, *and that of problem (4),* $q^\star$, *are related by*

$$\psi_0(p^\star) = q^\star \ . \quad (5)$$

privacy is via the function compositions:

$$\bar{f}_i(\mathbf{x}) = \psi_i(f_i(\mathbf{x})) \ , \ \text{dom} \bar{f}_i = \{\mathbf{x} \in \text{dom} f_i \mid f_i(\mathbf{x}) \in \text{dom} \psi_i\}$$

$$\bar{h}_i(\mathbf{x}) = \psi(\mathbf{C}\mathbf{x} - \mathbf{d}) \ \ \text{dom} \bar{h}_i = \mathbb{R}^n$$

# Example of Transformation of Objective

- **original problem:**

$$\text{minimize} \quad ||\mathbf{Ax} - \mathbf{b}||_2$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$
  - $\text{rank}(\mathbf{A}) = n$

# Example of Transformation of Objective

- **original problem:**

$$\text{minimize} \quad ||\mathbf{A}\mathbf{x} - \mathbf{b}||_2$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$
  - $\text{rank}(\mathbf{A}) = n$

- $\psi_0(z) = z^2 + b$

# Example of Transformation of Objective

- **original problem:**

$$\text{minimize} \quad ||\mathbf{A}\mathbf{x} - \mathbf{b}||_2$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - private data: $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{b} \in \mathbb{R}^m$
  - $\text{rank}(\mathbf{A}) = n$

- $\psi_0(z) = z^2 + b$

- **equivalent problem:**

$$\text{minimize } ||\mathbf{A}\mathbf{x} - \mathbf{b}||_2^2 - \mathbf{b}^\mathsf{T}\mathbf{b} = \mathbf{x}^\mathsf{T}\hat{\mathbf{A}}\mathbf{x} - 2\hat{\mathbf{b}}^\mathsf{T}\mathbf{x}$$

  - variable is $\mathbf{x} \in \mathbb{R}^n$
  - data: $\hat{\mathbf{A}} = \mathbf{A}^\mathsf{T}\mathbf{A} \in \mathbb{R}^{n \times n}$, $\hat{\mathbf{b}} = \mathbf{A}^\mathsf{T}\mathbf{b} \in \mathbb{R}^{n \times 1}$

# DECOMPOSITION TECHNIQUES

# Example of Decomposition

- **original problem:**

$$\begin{array}{ll} \text{minimize} & \alpha_1 x_1^2 + \alpha_2 x_2^2 \\ \text{subject to} & \beta_1 x_1 + \beta_2 x_2 = 1 \end{array}$$

  - variable is $x_1, x_2 \in \mathbb{R}$
  - private data: $\underbrace{\alpha_1, \beta_1 \in \mathbb{R}}_{\text{party 1}}, \ \underbrace{\alpha_2, \beta_2 \in \mathbb{R}}_{\text{party 2}}$

# Example of Decomposition

ROYAL INSTITUTE OF TECHNOLOGY

- **original problem:**

$$\begin{array}{ll} \text{minimize} & \alpha_1 x_1^2 + \alpha_2 x_2^2 \\ \text{subject to} & \beta_1 x_1 + \beta_2 x_2 = 1 \end{array}$$

  - variable is $x_1, x_2 \in \mathbb{R}$
  - private data: $\underbrace{\alpha_1, \beta_1 \in \mathbb{R}}_{\text{party 1}}, \ \underbrace{\alpha_2, \beta_2 \in \mathbb{R}}_{\text{party 2}}$

dualize, dual variable $\lambda$

dual decomposition algorithm

# Example of Decomposition

- **original problem:**

$$\begin{array}{ll} \text{minimize} & \alpha_1 x_1^2 + \alpha_2 x_2^2 \\ \text{subject to} & \beta_1 x_1 + \beta_2 x_2 = 1 \end{array}$$

  - variable is $x_1, x_2 \in \mathbb{R}$
  - private data: $\underbrace{\alpha_1, \beta_1 \in \mathbb{R}}_{\text{party 1}}$, $\underbrace{\alpha_2, \beta_2 \in \mathbb{R}}_{\text{party 2}}$

dualize, dual variable $\lambda$

dual decomposition algorithm

- **$k$th subproblem solved by entity $i$:**

$$\text{minimize } \alpha_i x_i^2 + \lambda^{(k)} \beta_i x_i$$

  - variable is $x_i \in \mathbb{R}$

# Example of Decomposition

- **original problem:**

$$\begin{array}{ll} \text{minimize} & \alpha_1 x_1^2 + \alpha_2 x_2^2 \\ \text{subject to} & \beta_1 x_1 + \beta_2 x_2 = 1 \end{array}$$

  - variable is $x_1, x_2 \in \mathbb{R}$
  - private data: $\underbrace{\alpha_1, \beta_1 \in \mathbb{R}}_{\text{party 1}}, \underbrace{\alpha_2, \beta_2 \in \mathbb{R}}_{\text{party 2}}$

dualize, dual variable $\lambda$

dual decomposition algorithm

- **$k$th subproblem solved by entity $i$:**

$$\text{minimize } \alpha_i x_i^2 + \lambda^{(k)} \beta_i x_i$$

  - variable is $x_i \in \mathbb{R}$

- **dual variable update at each entity $i$:**

$$\lambda^{(k+1)} = \lambda^{(k)} - (1/k)\Big( \underbrace{\beta_1 x_1^{(k)}}_{-\lambda^{(k)}\beta_1^2/\alpha_1} + \underbrace{\beta_2 x_2^{(k)}}_{-\lambda^{(k)}\beta_2^2/\alpha_2} -1\Big)$$

ROYAL INSTITUTE OF TECHNOLOGY

# Quantify Privacy

# Quantify Privacy

ROYAL INSTITUTE OF TECHNOLOGY

**Definition (Attacker model, Passive adversary)**

- an entity involved in solving the global problem
- does not deviate from the intended protocol
- it obtain messages exchanged during different stages of the solution method
- keeps a record of all information it receives
- try to learn and to discover others' private data

# Quantify Privacy

## Definition (Attacker model, Passive adversary)

- an entity involved in solving the global problem
- does not deviate from the intended protocol
- it obtain messages exchanged during different stages of the solution method
- keeps a record of all information it receives
- try to learn and to discover others' private data

## Definition (Adversarial knowledge)

- the set $\mathcal{K}$ of information that an adversary might exploit to discover private data
- set $\mathcal{K}$ can encompass
  - *real-valued components*: $\mathcal{K}_{\mathrm{real}}$
  - transformed variants of private data
  - statements

# Quantify Privacy

## Definition (Privacy index, $(\xi, \eta) \in [0,1) \times \mathbb{N}$)

- private data $c \in \mathcal{C}$ is related to some adversarial knowledge $\mathbf{k} \in \mathcal{K}_{\text{real}} \subseteq \mathcal{K}$ by a vector values function $f_c : \mathcal{C} \times \mathcal{K}_{\text{real}} \to \mathbb{R}^m$, such that $f_c(c, \mathbf{k}) \leq \mathbf{0}$
- consider the uncertainty set

$$\mathcal{U} = \{c \mid f_c(c, \mathbf{k}) \leq \mathbf{0},\ f_c \text{ is arbitrary},\ \mathcal{K}\} \tag{6}$$

- then

$$\xi = 1 - 1/N_{\mathcal{K}}\ , \quad N_{\mathcal{K}} \text{ is the cardinality of } \mathcal{U} \tag{7}$$

$$\eta = \text{affine dimension of } \mathcal{U} \tag{8}$$

# Quantify Privacy

**Definition (Privacy index, $(\xi, \eta) \in [0,1) \times \mathbb{N}$)**

- private data $c \in \mathcal{C}$ is related to some adversarial knowledge $\mathbf{k} \in \mathcal{K}_{\text{real}} \subseteq \mathcal{K}$ by a vector values function $f_c : \mathcal{C} \times \mathcal{K}_{\text{real}} \to \mathbb{R}^m$, such that $f_c(c, \mathbf{k}) \le \mathbf{0}$
- consider the uncertainty set

$$\mathcal{U} = \{c \,|\; f_c(c, \mathbf{k}) \le \mathbf{0},\; f_c \text{ is arbitrary},\; \mathcal{K}\} \tag{6}$$

- then

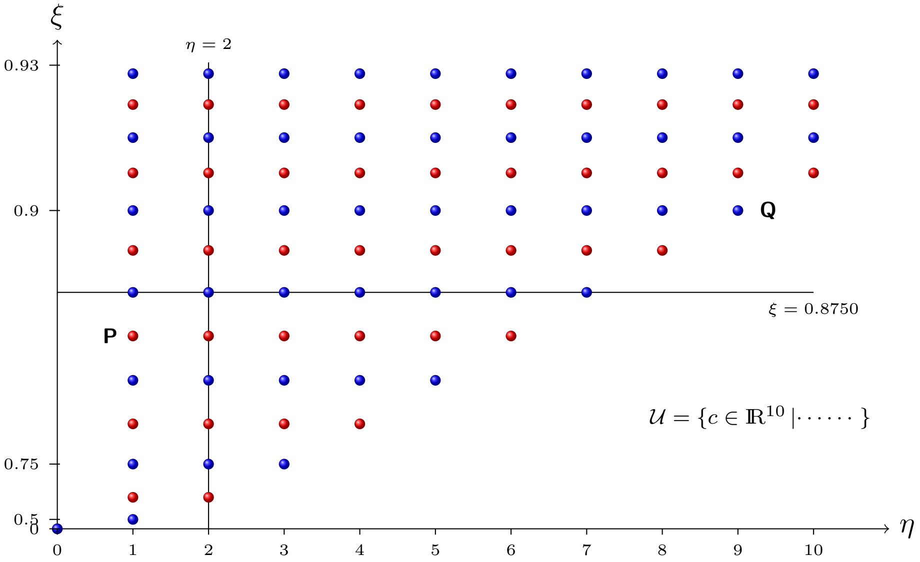
$$\xi = 1 - 1/N_{\mathcal{K}}\ , \quad N_{\mathcal{K}} \text{ is the cardinality of } \mathcal{U} \tag{7}$$

$$\eta = \text{affine dimension of } \mathcal{U} \tag{8}$$

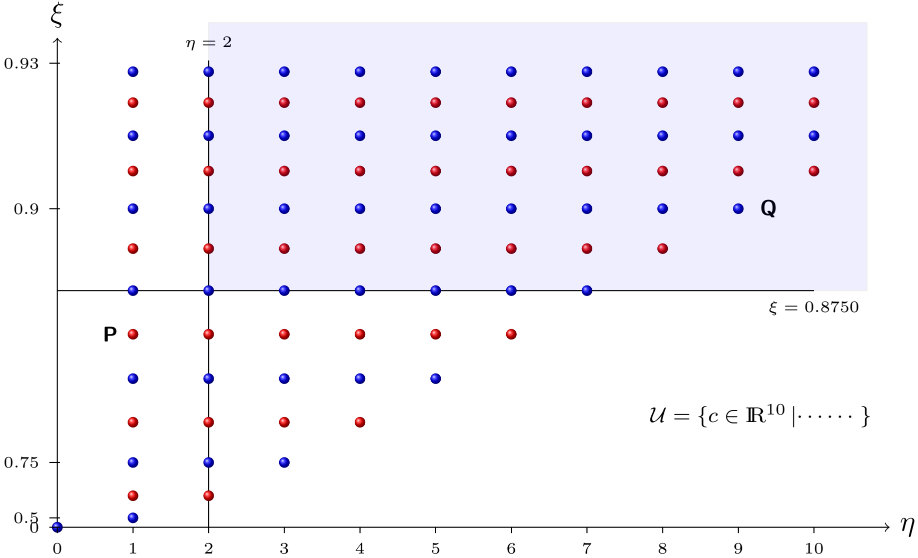
$\xi$ : a measure of probability that the adversary guesses wrong

$\eta$ : indicates how effective the transformation disguises the private data

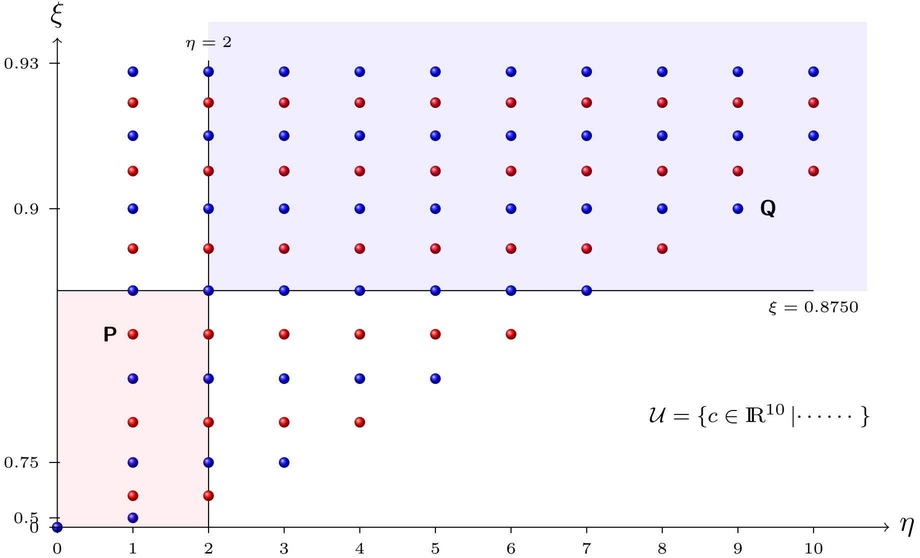
# Quantify Privacy



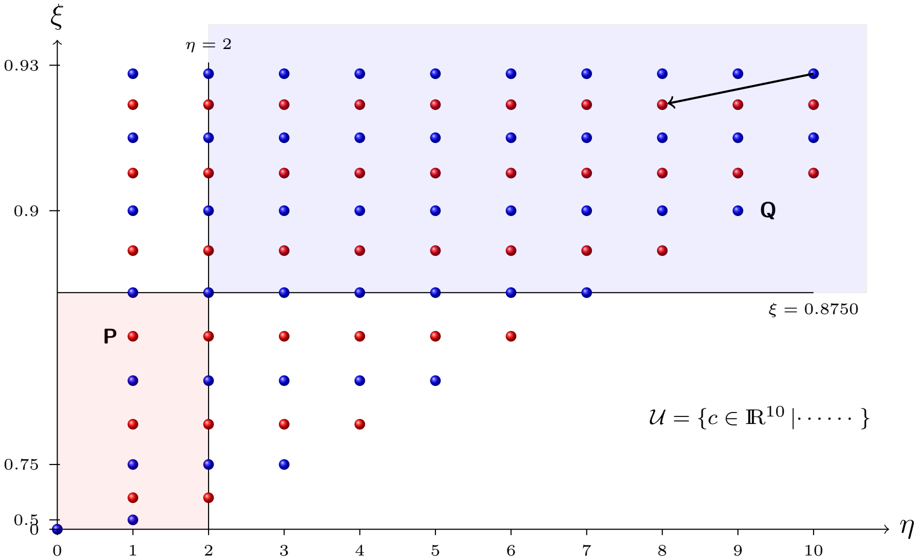
# Quantify Privacy



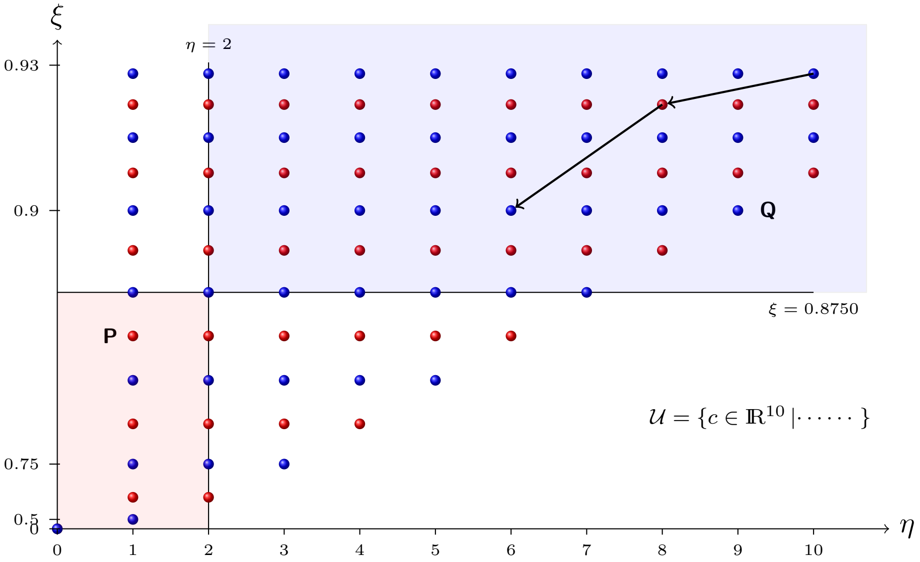
# Quantify Privacy



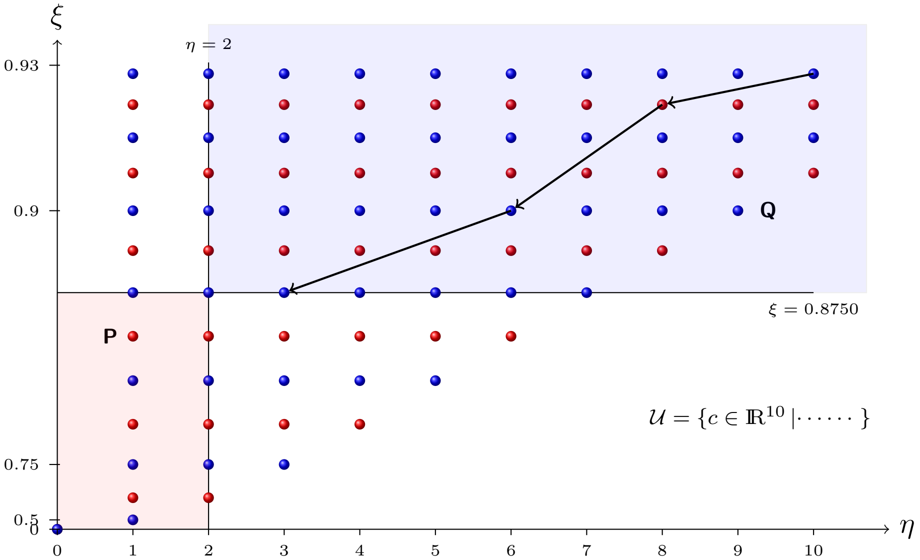
# Quantify Privacy



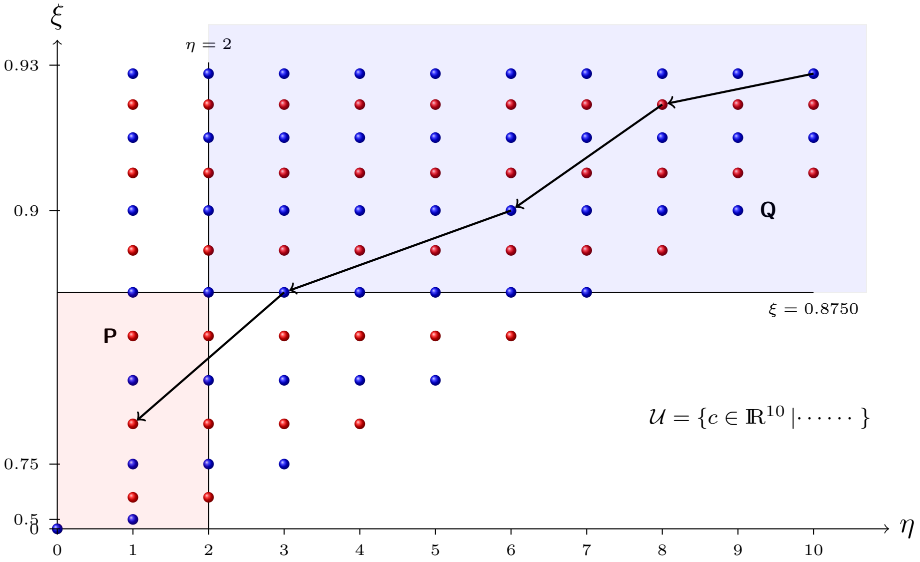
# Quantify Privacy



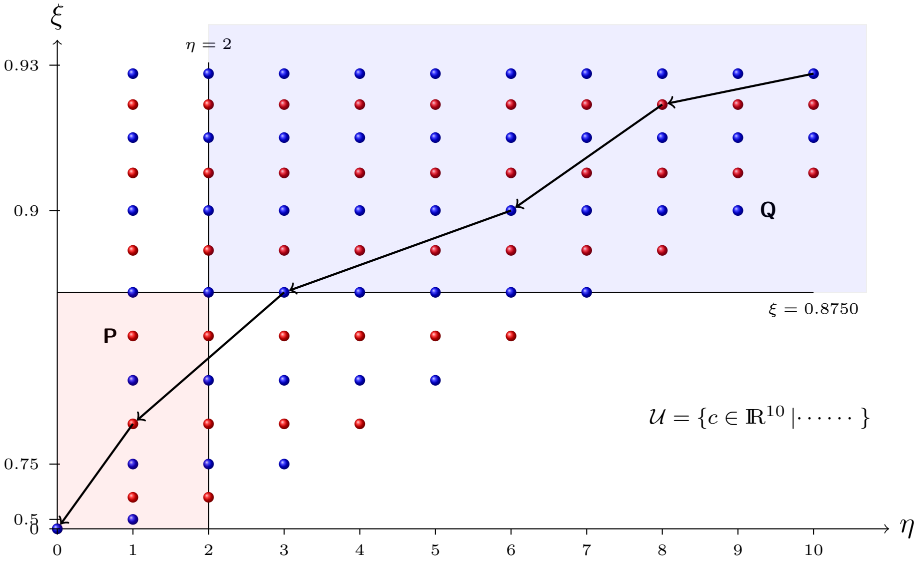
# Quantify Privacy



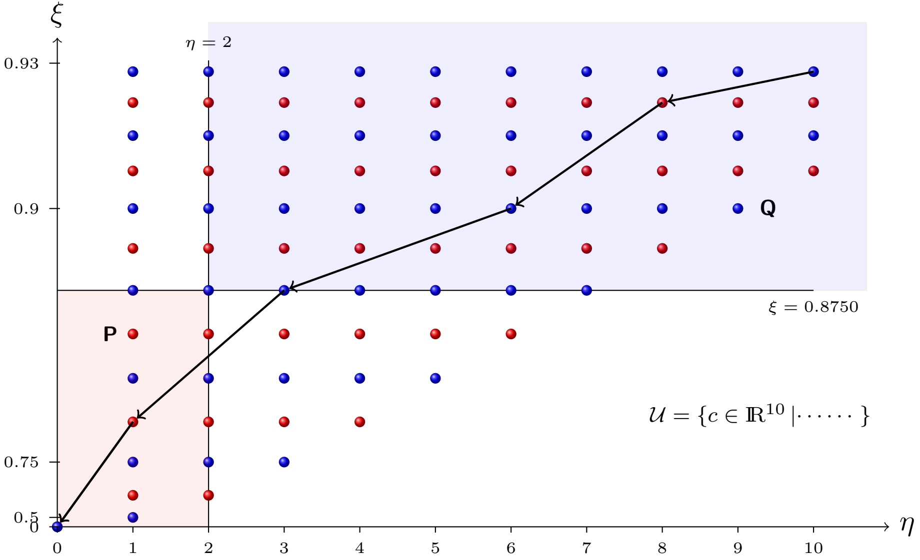
# Quantify Privacy



# Quantify Privacy



# Quantify Privacy



# Privacy Index in a Least-Squares Problem

- **original problem:**

$$\text{minimize} \quad ||\mathbf{a}x - \mathbf{b}||_2$$

  - variable is $x \in \mathbb{R}$
  - private data: $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2) \in \mathbb{R}^6$, $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2) \in \mathbb{R}^6$
  - 2-parties: party $1$ owns $\mathbf{a}_1, \mathbf{b}_1$ , party $1$ owns $\mathbf{a}_2, \mathbf{b}_2$

- **equivalent problem:**

$$\text{minimize } ||\mathbf{a}x - \mathbf{b}||_2^2 - \mathbf{b}^\mathsf{T}\mathbf{b} = (r_1 + r_2)x^2 - 2(s_1 + s_2)x$$

  - variable is $x \in \mathbb{R}$
  - data: $r_i = \mathbf{a}_i^\mathsf{T}\mathbf{a}_i \ i = 1, 2$; $s_i = \mathbf{a}_i^\mathsf{T}\mathbf{b}_i, \ i = 1, 2$

# Privacy Index in a Least-Squares Problem

- **original problem:**

$$\text{minimize} \quad ||\mathbf{a}x - \mathbf{b}||_2$$

  - variable is $x \in \mathbb{R}$
  - private data: $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2) \in \mathbb{R}^6$, $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2) \in \mathbb{R}^6$
  - 2-parties: party $1$ owns $\mathbf{a}_1, \mathbf{b}_1$ , party $1$ owns $\mathbf{a}_2, \mathbf{b}_2$

- **equivalent problem:**

$$\text{minimize } ||\mathbf{a}x - \mathbf{b}||_2^2 - \mathbf{b}^\mathsf{T}\mathbf{b} = (r_1 + r_2)x^2 - 2(s_1 + s_2)x$$

  - variable is $x \in \mathbb{R}$
  - data: $r_i = \mathbf{a}_i^\mathsf{T}\mathbf{a}_i \ i = 1, 2;\ \ s_i = \mathbf{a}_i^\mathsf{T}\mathbf{b}_i,\ \ i = 1, 2$

# Privacy Index in a Least-Squares Problem

- party 2 is the adversary and wants to discover $\mathbf{a}_1$

- knowledge of party 2

$$\mathcal{K} = \Big\{ r_1, s_1, \{ r_1 = \mathbf{a}_1^\mathsf{T} \mathbf{a}_1 \}, \{ s_1 = \mathbf{b}_1^\mathsf{T} \mathbf{a}_1 \} \Big\}$$

- the uncertainty set of $\mathbf{a}_1$:

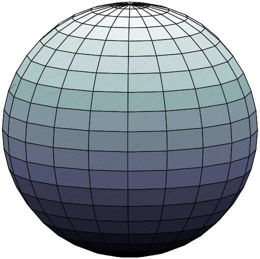
$$\mathcal{U} = \Big\{ \mathbf{a}_1 \;\Big|\; r_1 = \mathbf{a}_1^\mathsf{T} \mathbf{a}_1, s_1 = \mathbf{b}_1^\mathsf{T} \mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \Big\}$$

# Privacy Index in a Least-Squares Problem

- the uncertainty set of $\mathbf{a}_1$:

$$\mathcal{U} = \left\{ \mathbf{a}_1 \ \middle| \ r_1 = \mathbf{a}_1^{\mathsf{T}} \mathbf{a}_1, s_1 = \mathbf{b}_1^{\mathsf{T}} \mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \right\}$$

# Privacy Index in a Least-Squares Problem

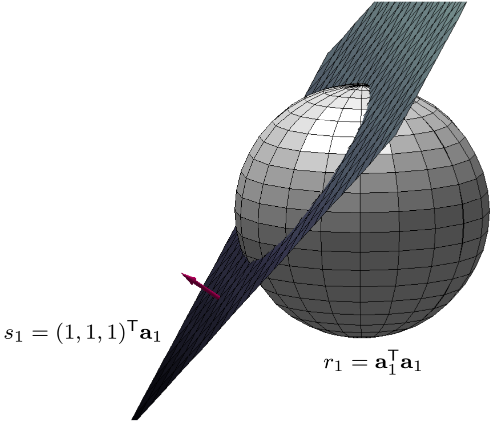


$r_1 = \mathbf{a}_1^\mathsf{T}\mathbf{a}_1$

- the uncertainty set of $\mathbf{a}_1$:

$$\mathcal{U} = \left\{ \mathbf{a}_1 \;\middle|\; r_1 = \mathbf{a}_1^\mathsf{T}\mathbf{a}_1, s_1 = \mathbf{b}_1^\mathsf{T}\mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \right\}$$

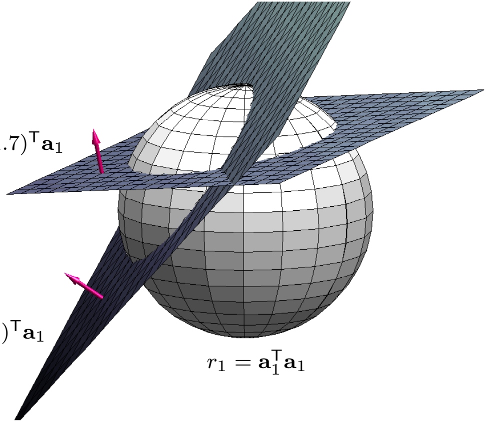
# Privacy Index in a Least-Squares Problem




- the uncertainty set of $\mathbf{a}_1$:

$$\mathcal{U} = \left\{ \mathbf{a}_1 \;\middle|\; r_1 = \mathbf{a}_1^{\mathsf{T}}\mathbf{a}_1, s_1 = \mathbf{b}_1^{\mathsf{T}}\mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \right\}$$

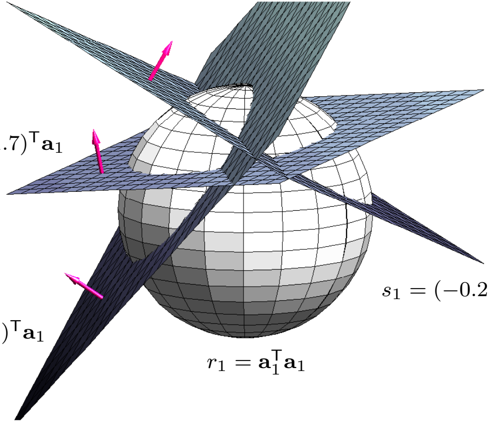
# Privacy Index in a Least-Squares Problem




- the uncertainty set of $\mathbf{a}_1$:

$$\mathcal{U} = \left\{ \mathbf{a}_1 \;\middle|\; r_1 = \mathbf{a}_1^\mathsf{T}\mathbf{a}_1, s_1 = \mathbf{b}_1^\mathsf{T}\mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \right\}$$

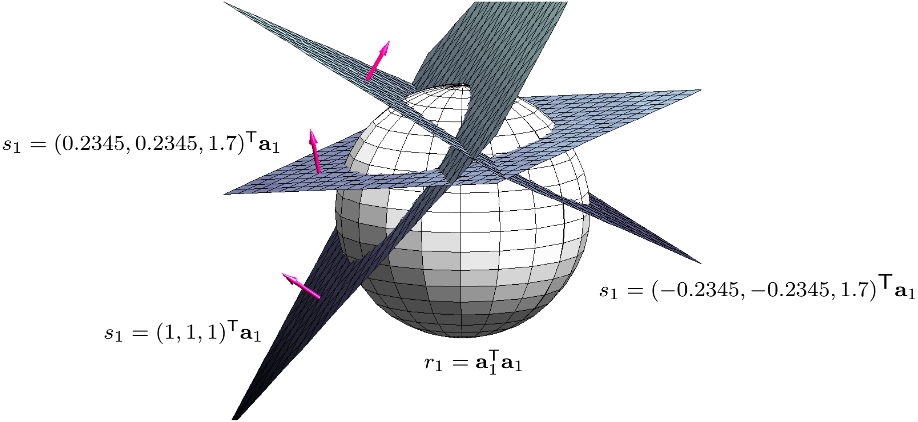
# Privacy Index in a Least-Squares Problem




- the uncertainty set of $\mathbf{a}_1$:

$$\mathcal{U} = \left\{ \mathbf{a}_1 \;\middle|\; r_1 = \mathbf{a}_1^\mathsf{T} \mathbf{a}_1, s_1 = \mathbf{b}_1^\mathsf{T} \mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \right\}$$

# Privacy Index in a Least-Squares Problem




$\mathbf{b}_1$ is known: $(\xi, \eta) = (1, 2)$

$\mathbf{b}_1$ is arbitrary: $(\xi, \eta) = (1, 3)$

KTH VETENSKAP OCH KONST
ROYAL INSTITUTE OF TECHNOLOGY

# Cryptography
# Vs
# Non-Cryptographic methods

# Cryptographic vs Non-Cryptographic Methods

| Cryptographic methods | Non-Cryptographic methods |
|---|---|
| • large circuit representations ($1000$s of bits) to compute $f(\mathbf{A}_1, \dots, \mathbf{A}_n)$ | no such restrictions |
| • not scalable | scalable |
| • finite field restriction for $\mathbf{A}_i$ | no such restrictions |
| • hardly handle non-integer valued $\mathbf{A}_i$ (overflow, underflow, round-off, and truncations errors) | no such restrictions<br>HQ implementations (LAPACK,BLAS) |
| • $f_0$ and $\mathbf{g}$ are often restricted | no hard restrictions |
| • mechanism influences the algorithm iterations | mechanism is transparent to the solver |
| • theory for general $f_0$ and $\mathbf{g}$ are not promising | there exist a rich and a promising theory, e.g., convex optimization |
| • privacy guaranties for $\mathbf{A}_i$ are broadly studied | to be investigated |

# Cryptographic vs Non-Cryptographic Methods

| Cryptographic methods | Non-Cryptographic methods |
|---|---|
| • large circuit representations ($1000$s of bits) to compute $f(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ | no such restrictions |
| • not scalable | scalable |
| • finite field restriction for $\mathbf{A}_i$ | no such restrictions |
| • hardly handle non-integer valued $\mathbf{A}_i$ (overflow, underflow, round-off, and truncations errors) | no such restrictions<br>HQ implementations (LAPACK,BLAS) |
| • $f_0$ and $\mathbf{g}$ are often restricted | no hard restrictions |
| • mechanism influences the algorithm iterations | mechanism is transparent to the solver |
| • theory for general $f_0$ and $\mathbf{g}$ are not promising | there exist a rich and a promising theory, e.g., convex optimization |
| • **privacy guaranties for $\mathbf{A}_i$ are broadly studied** | **to be investigated** |

# Cryptographic Vs Non-Cryptographic Methods

encrypting simplex algorithm iterations...a quote from Toft [Tof09]

- start with **32-bit numbers**
- **after ten iterations** these have grown to **32 thousand bits**
- **after twenty iterations** they have increased to **32 million**
- even small inputs ⇒ basic operations ⇒ mod. exponentiations with a million bit modulus"

# Cryptographic Vs Non-Cryptographic Methods

encrypting simplex algorithm iterations...a quote from Toft [Tof09]

- start with **32-bit numbers**
- **after ten iterations** these have grown to **32 thousand bits**
- **after twenty iterations** they have increased to **32 million**
- even small inputs ⇒ basic operations ⇒ mod. exponentiations with a million bit modulus"

INEFFICIENT

# Conclusions

If you think cryptography is
the answer to your problem,
then you dont know what
your problem is.

-Peter G. Numann
Principal Scientist, SRI International
Menlo Park, CA, 94025 USA

# Conclusions

If you think cryptography is
the answer to your problem,
then you dont know what
your problem is.

-Peter G. Numann
Principal Scientist, SRI International
Menlo Park, CA, 94025 USA

- cryptography can be **inefficient** in many useful problems
- **alternatives** for cryptographic approaches: **less investigated**
- we believe that **substantial research is required**

# Thank you

# On the application of optimization methods for secured multiparty computations

**C. Weeraddana**⋆, G. Athanasiou⋆, M. Jakobsson⋆, C. Fischione⋆, and J. S. Baras⋆⋆

⋆KTH Royal Institute of Technology, Stockholm, Sweden
⋆⋆University of Maryland, MD, USA
{chatw, georgioa, mjakobss, carlofi}@kth.se; baras@umd.edu

ACCESS ISS 18.09.13

[Du01] W. Du.
*A Study of Several Specific Secure Two-Party Computation Problems*.
PhD thesis, Purdue University, 2001.

[Tof09] T. Toft.
Solving linear programs using multiparty computation.
*Financ. Crypt. and Data Sec. LNCS*, pages 90–107, 2009.

[Vai09] J. Vaidya.
Privacy-preserving linear programming.
In *Proc. ACM Symp. on App. Comp.*, pages 2002–2007, Honolulu, Hawaii, USA, March 2009.

[WAJ+13] P. C. Weeraddana, G. Athanasiou, M. Jakobsson, C. Fischione, and J. S. Baras.
Per-se privacy preserving distributed optimization.
*arXiv, Cornell University Library*, 2013.
[Online]. Available: http://arxiv.org/abs/1210.3283.