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

CWC 21.05.13

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

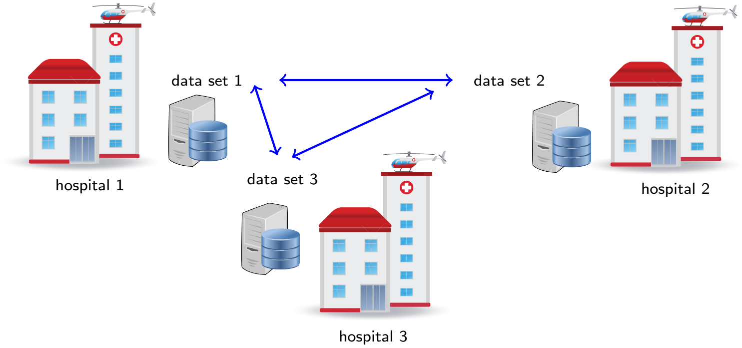
Motivation – Why Privacy/Security ?

- 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 ⇒ inference for better diagnosis
  - larger data sets ⇒ 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

candidate 1 **candidate 2**

X	X				X	X
		X	X	X		

vote 1 vote 2 . . . . vote N

Real World

- **example 4**
  - millionaires' problem [Yao82], i.e., check $b_1 \leq b_2$
  - **challenge:** neither b_1 nor b_2 should be revealed

Alice

b_1 **€**

Bob

b_2 **€**

Secured Multiparty Computation

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

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

- $\mathbf{A}_i$ is the private data belonging to party i
- $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_n)$ 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

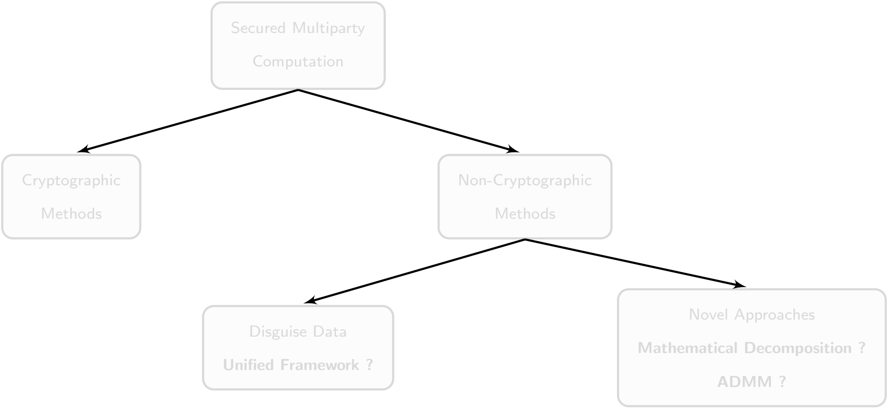
- solve, **in a secured manner**, the n-party problem of the form:

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

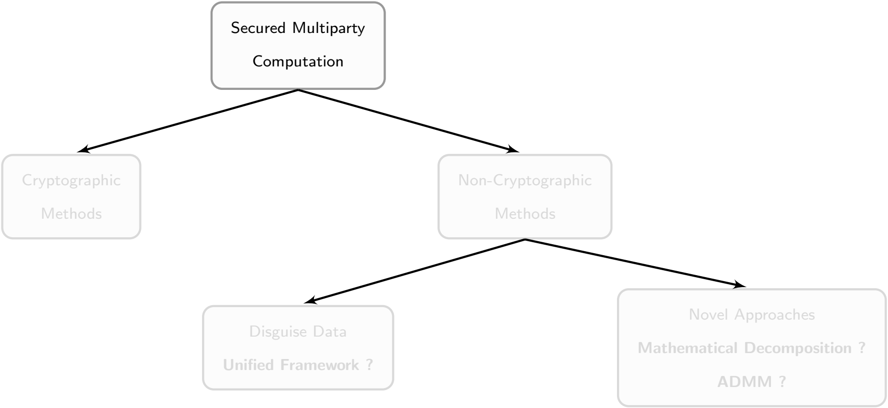
  - $\mathbf{A}_i$ is the private data belonging to party i
  - $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is the decision variable
  - $f_0(\cdot)$ is the global objective function
  - $\mathbf{g}(\cdot)$ is the vector-valued constraint function
  - $f(\cdot)$ is the desired optimal value

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

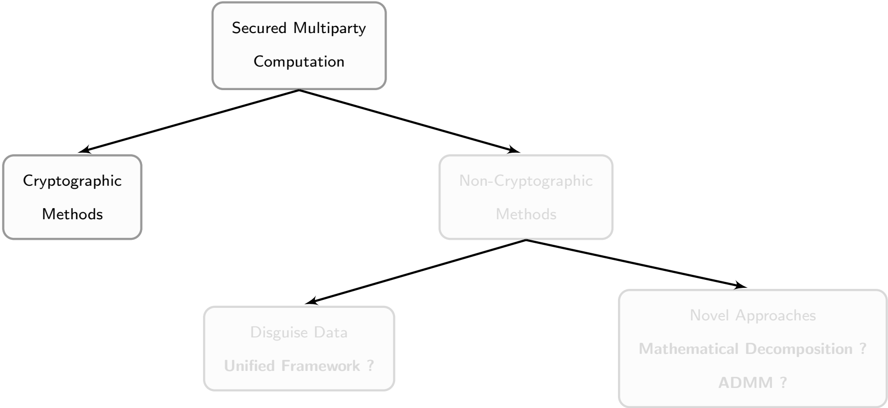
Overview


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

Overview

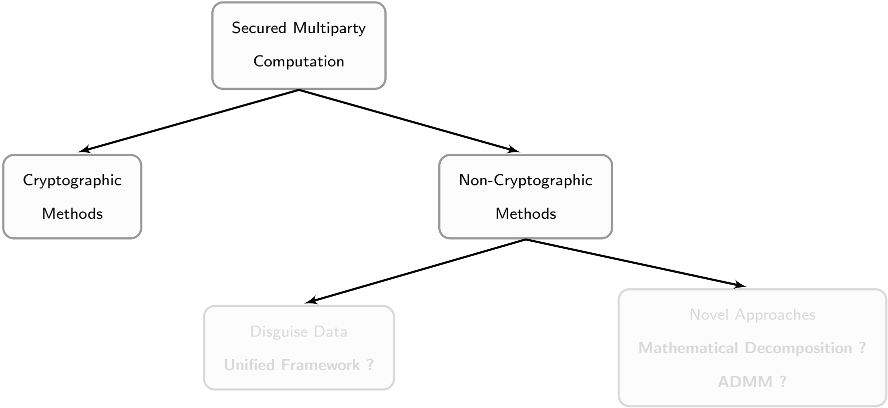

Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

Overview

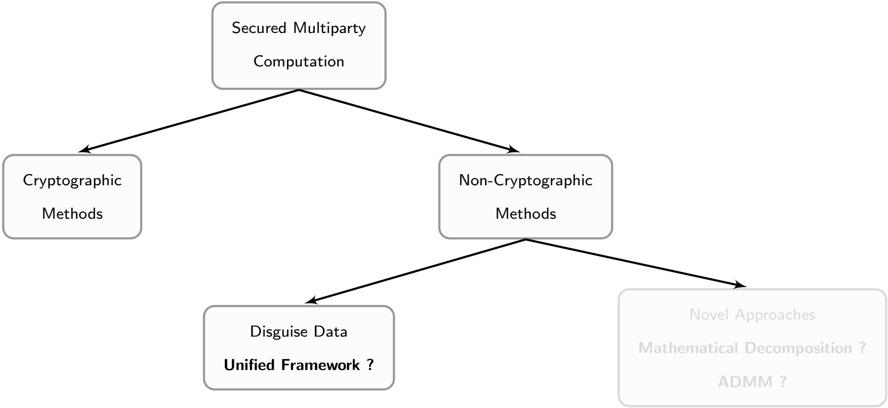


Secured Multiparty Computation
Cryptographic Methods
Non-Cryptographic Methods
Disguise Data
Unified Framework ?
Novel Approaches
Mathematical Decomposition ?
ADMM ?

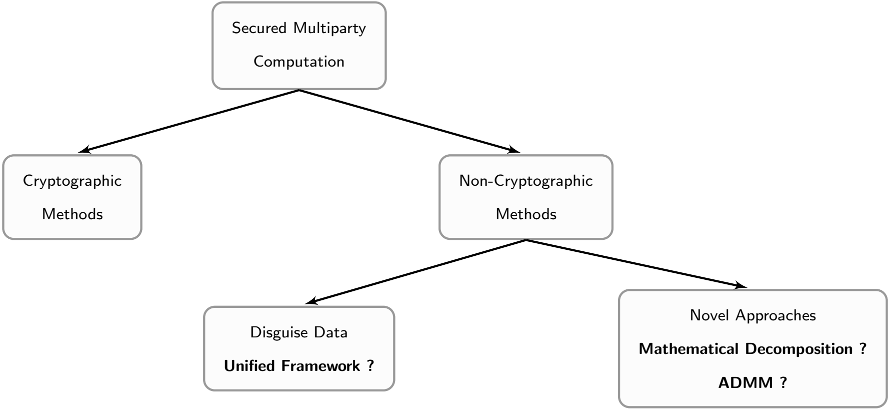
Overview


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

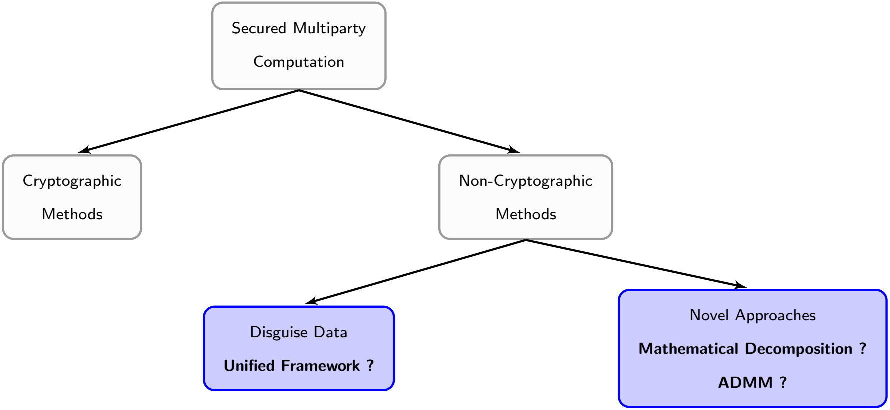
Overview


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

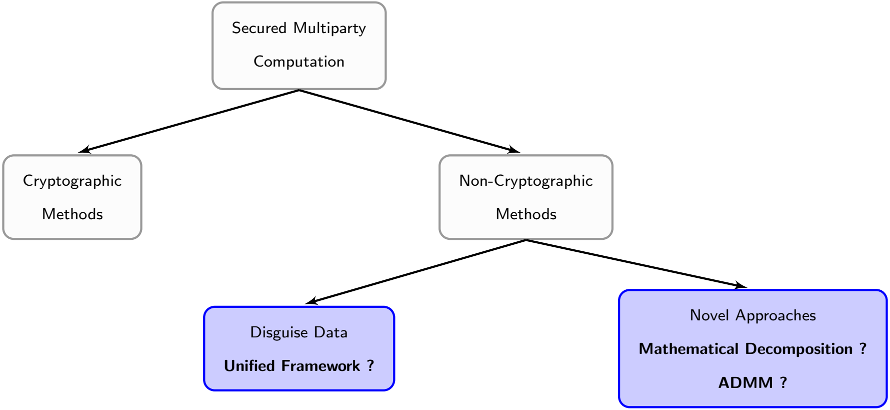
Overview


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

Overview


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

Our Contributions



Our Contributions

- **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.
- **maneuvering decomposition methods, ADMM**
- **general definition** for privacy $\Rightarrow$ 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

General Formulation

we pose the design or decision making problem

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

- optimization variable is $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$.
- $f_i,\ i = 0, \ldots, q$ are *convex*
- $\mathbf{C} \in \mathbb{R}^{p \times n}$ with 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:*

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

- $\mathbf{x}^\star$ *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:*

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

- $\mathbf{x}^\star$ *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

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

Example of Change of Variables

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

- **original problem:**

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

  - 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

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

- **original problem:**

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

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

- **equivalent problem:**

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

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

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*

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

  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

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*

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

  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*

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

privacy is via the function compositions:

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

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

Example of Transformation of Objective

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

Example of Transformation of Objective

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

- **original problem:**

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

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

Example of Transformation of Objective

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

- **original problem:**

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

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

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

Quantify Privacy

ROYAL INSTITUTE OF TECHNOLOGY

Definition (Attacker model, Passive adversary)

- an entity involved in solving the global problem
- 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
- 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 $f_c(c, \mathbf{k}) \leq \mathbf{0}$
- 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

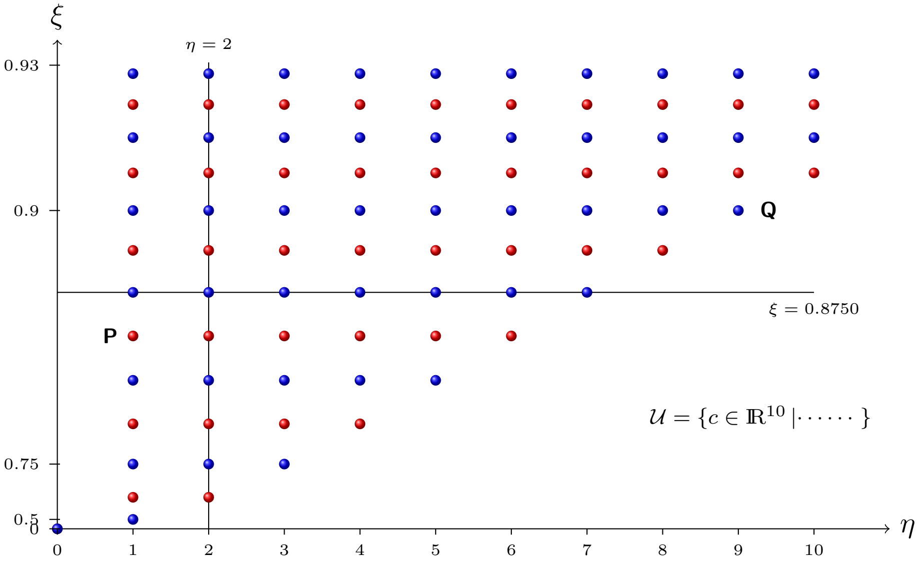
$$\xi = 1 - 1/N_{\mathcal{K}}\ , \quad N_{\mathcal{K}} \text{ is the cardinality of } \mathcal{U} \tag{7}$$

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

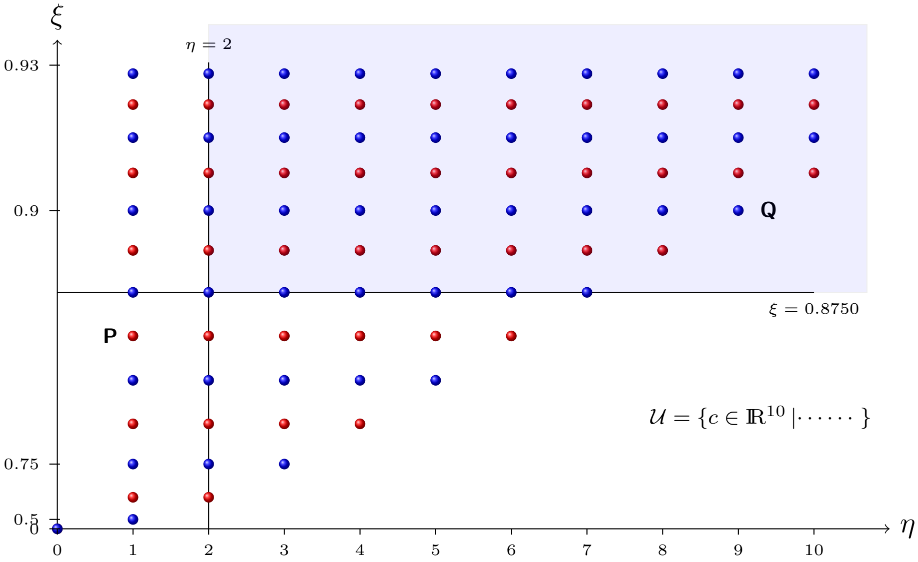
ξ : a measure of probability that the adversary guesses wrong

η : indicates how effective the transformation disguises the private data

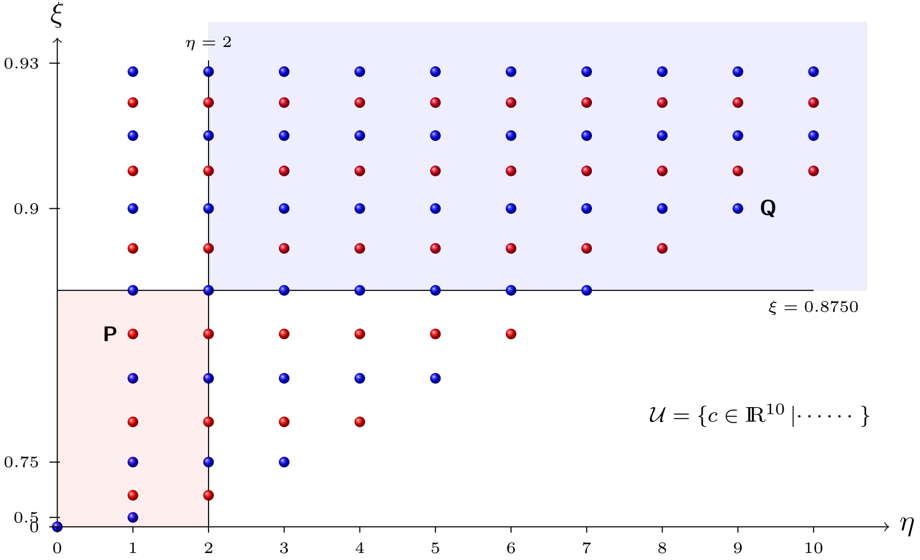
Quantify Privacy



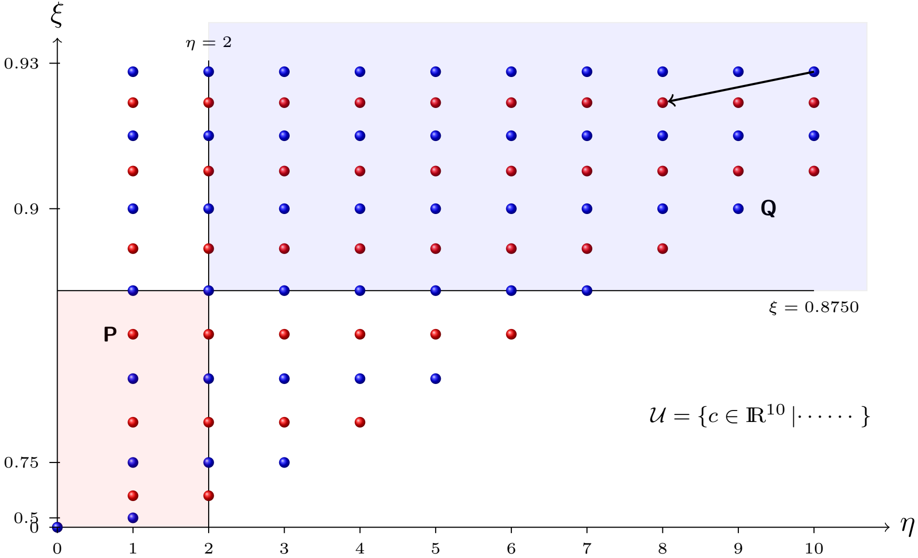
Quantify Privacy



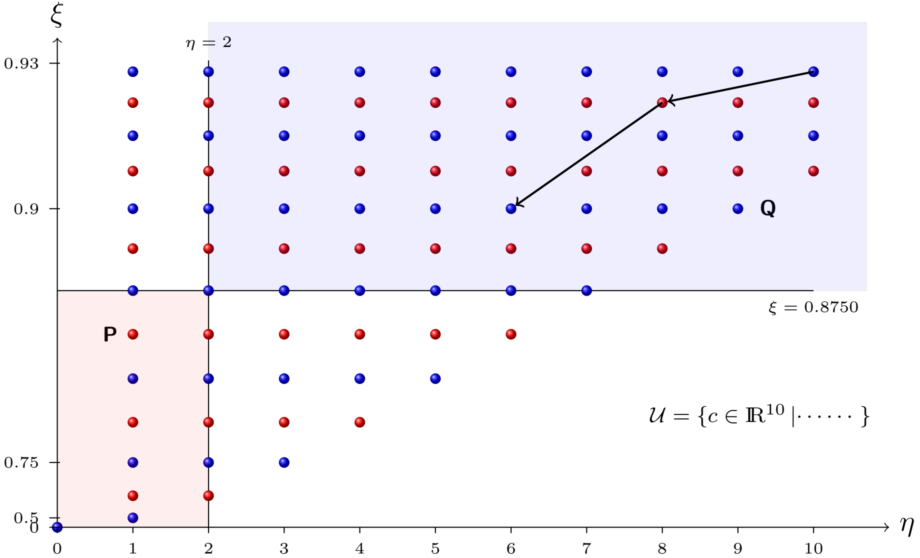
Quantify Privacy



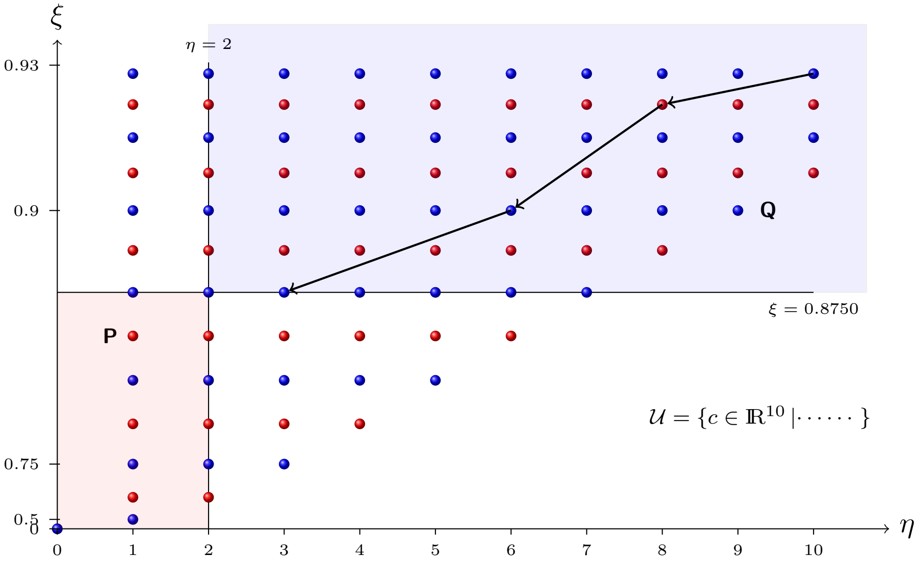
Quantify Privacy



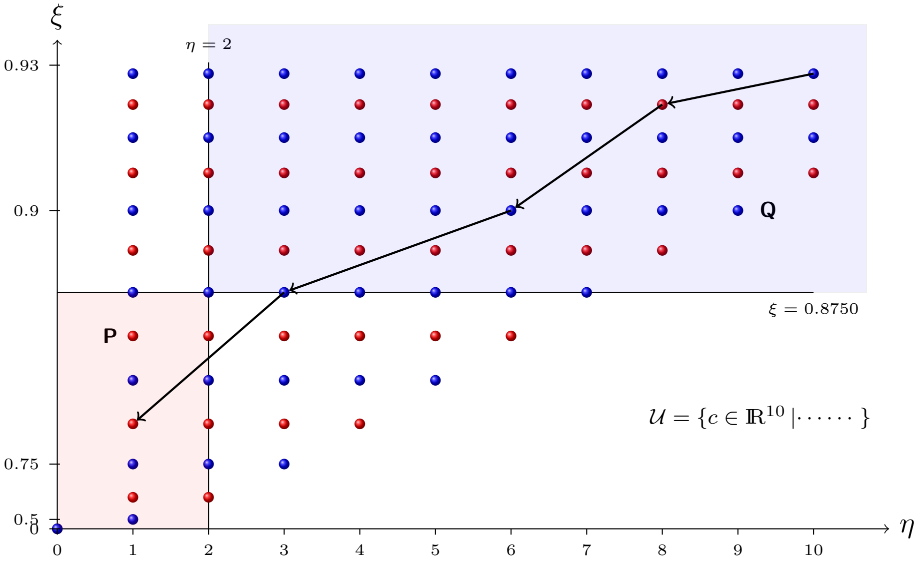
Quantify Privacy



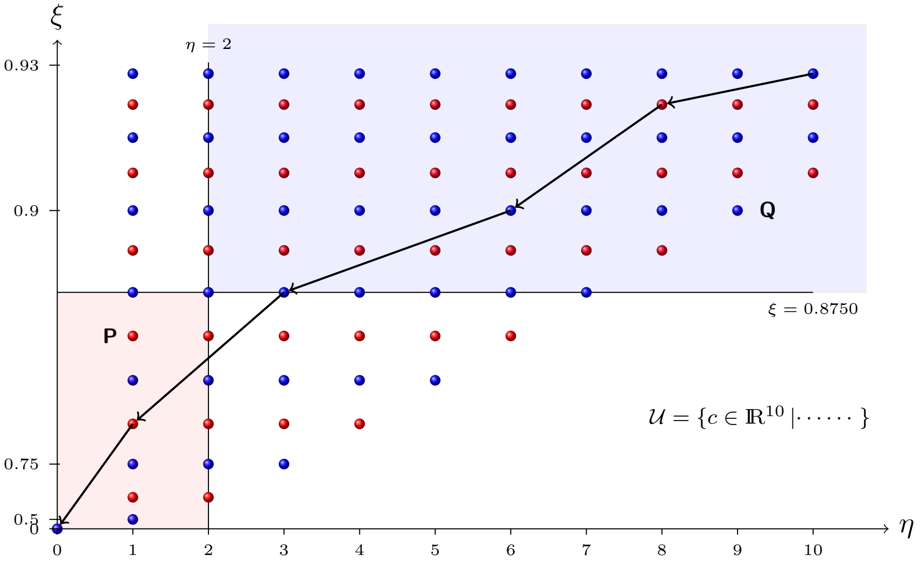
Quantify Privacy



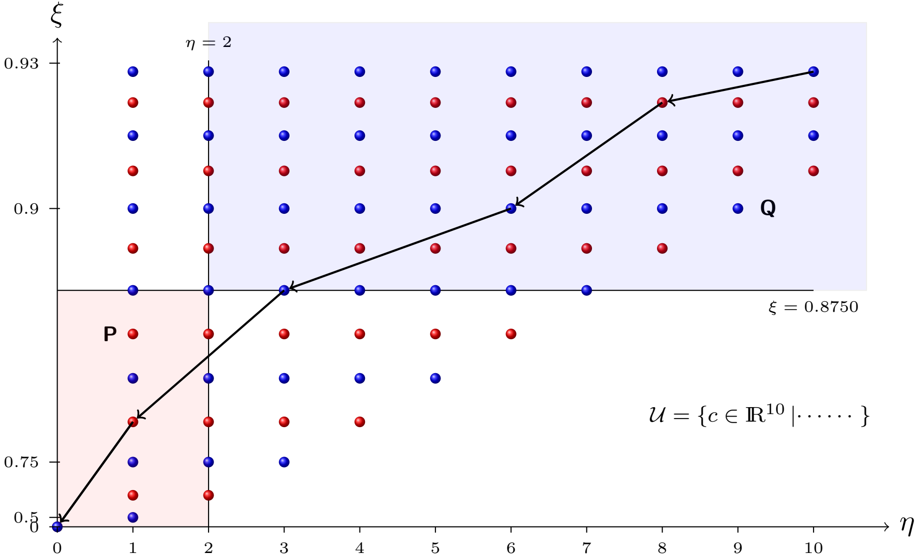
Quantify Privacy



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 i owns $\mathbf{a}_i, \mathbf{b}_i$, $i = 1, 2$

- **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 i owns $\mathbf{a}_i, \mathbf{b}_i$, $i = 1, 2$

- **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

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

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

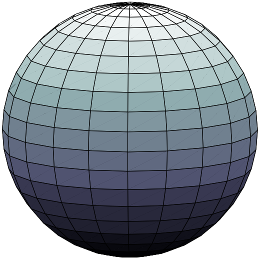
$$\mathcal{U} = \Big\{ \mathbf{a}_1 \;\Big|\; r_1 = \mathbf{a}_1^\intercal \mathbf{a}_1, s_1 = \mathbf{b}_1^\intercal \mathbf{a}_1, \mathbf{b}_1 \in \mathbb{R}^3 \Big\}$$

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

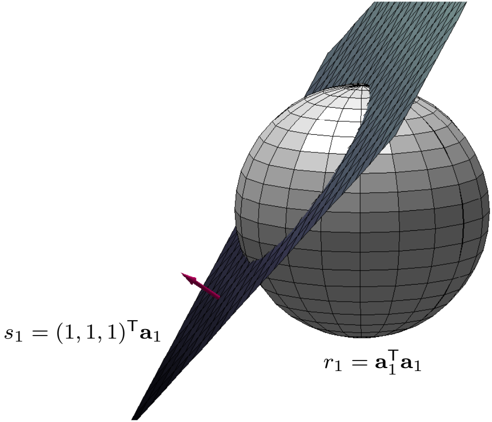


$$r_1 = \mathbf{a}_1^\mathsf{T}\mathbf{a}_1$$

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

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

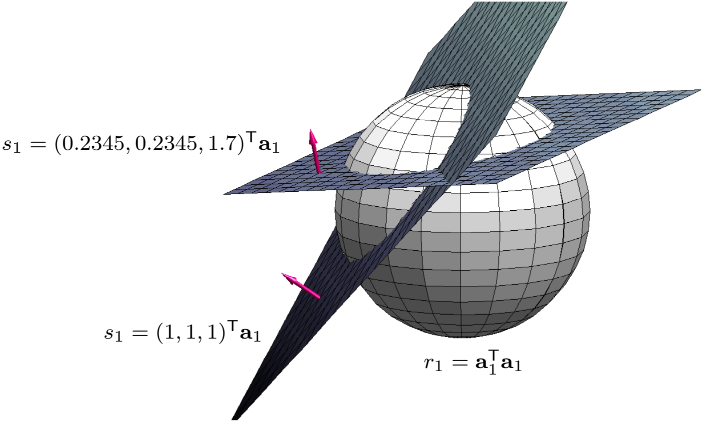
Privacy Index in a Least-Squares Problem



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

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

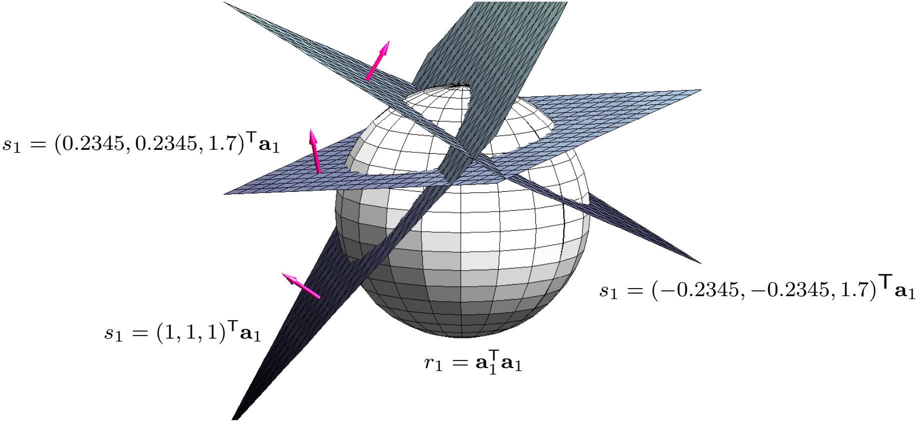
Privacy Index in a Least-Squares Problem



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

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

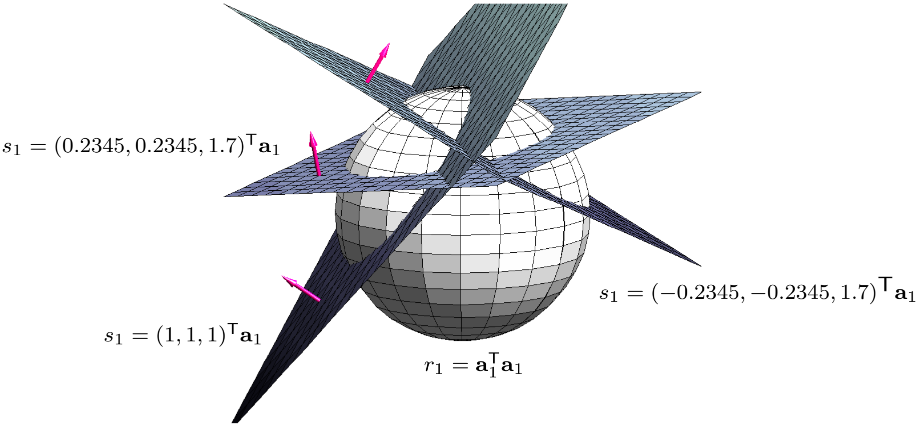
Privacy Index in a Least-Squares Problem



- 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: $(\xi, \eta) = (1, 3)$

Cryptographic vs Non-Cryptographic Methods

Cryptographic methods	Non-Cryptographic methods
• large circuit representations (1000s 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 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

ROYAL INSTITUTE OF TECHNOLOGY

Cryptographic methods	Non-Cryptographic methods
• large circuit representations (1000s 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 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

ROYAL INSTITUTE OF TECHNOLOGY

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

ROYAL INSTITUTE OF TECHNOLOGY

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

ROYAL INSTITUTE OF TECHNOLOGY

> 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 is **inefficient**
- **alternatives** for cryptographic approaches: **less investigated**
- we believe that **substantial research is required**

ROYAL INSTITUTE OF TECHNOLOGY

Thank you

ROYAL INSTITUTE OF TECHNOLOGY

Hydrobionets

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

CWC 21.05.13

[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`.

[Yao82] A. C. Yao.
Protocols for secure computations.
In *Proc. IEEE Symp. Found. of Comp. Science*, pages 160–164, Chicago, USA, November 1982.