Disclosure Risks of Distance Preserving Data Transformations

E. Onur Turgay, Thomas B. Pedersen,
Yücel Saygın, Erkay Savaş, Albert Levi

Sabancı Üniversitesi

SSDBM, Hong Kong
July 9, 2008

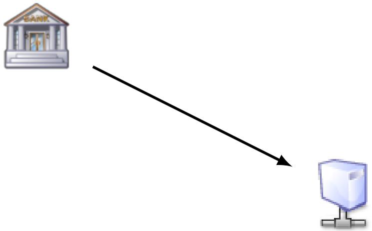
Outline

Outline

Data Analysis and Sharing

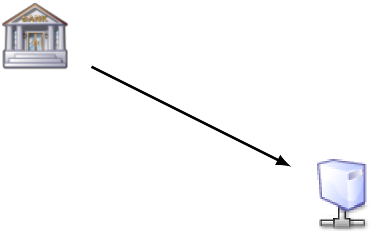
Data Analysis and Sharing

Data Analysis and Sharing



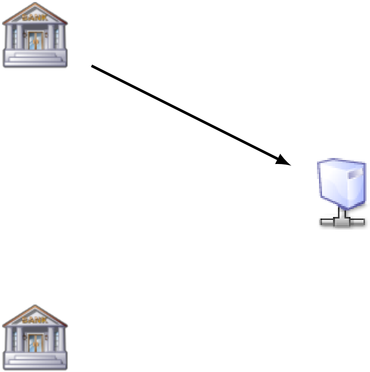
- Outsourcing

Data Analysis and Sharing



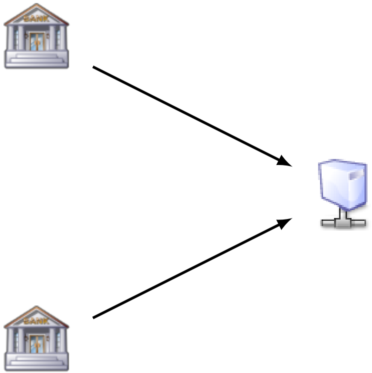
- Outsourcing — can the statistician be trusted?

Data Analysis and Sharing



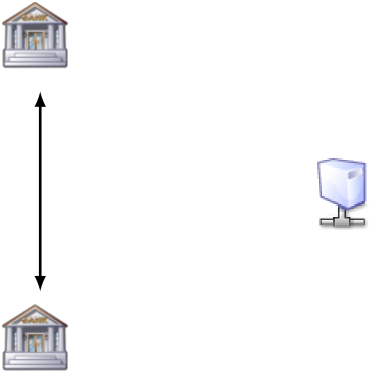
- Outsourcing — can the statistician be trusted?

Data Analysis and Sharing



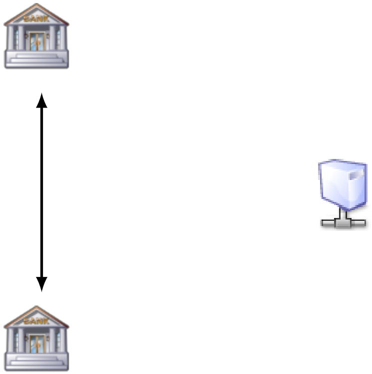
- Outsourcing — can the statistician be trusted?

Data Analysis and Sharing



- Outsourcing — can the statistician be trusted?
- Sharing

Data Analysis and Sharing



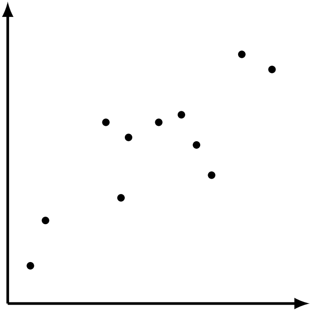
- Outsourcing — can the statistician be trusted?
- Sharing — can they trust each other?

Data Transformations

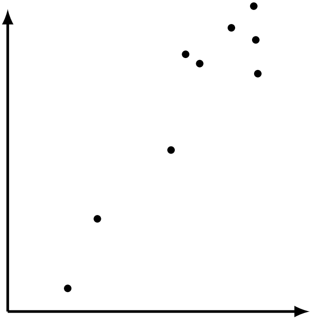
Data Transformations — a way to get rid of trust.

Data Transformations

Data Transformations — a way to get rid of trust.

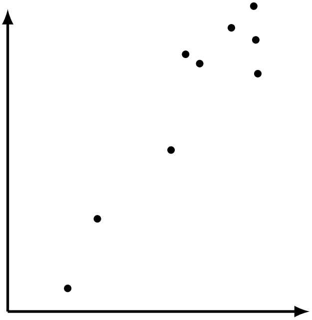


Data Transformations — a way to get rid of trust.



Data Transformations

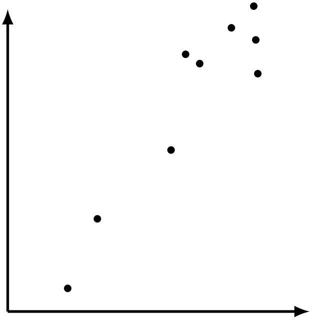
Data Transformations — a way to get rid of trust.



Liu, Giannella, Kargupta: Attack on perturbed data.

Data Transformations

Data Transformations — a way to get rid of trust.

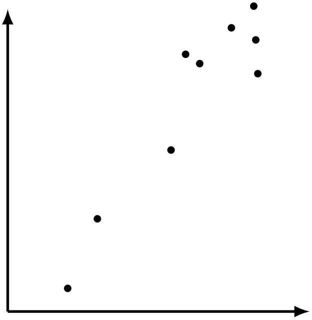


Liu, Giannella, Kargupta: Attack on perturbed data.

Mutual distances:

Data Transformations

Data Transformations — a way to get rid of trust.



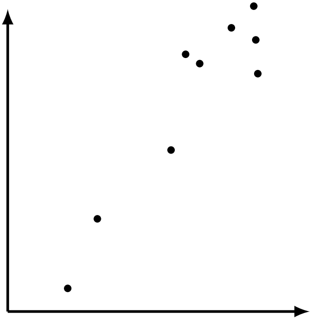
Liu, Giannella, Kargupta: Attack on perturbed data.

Mutual distances:

Fact Are useful in many analytical techniques.

Data Transformations

Data Transformations — a way to get rid of trust.



Liu, Giannella, Kargupta: Attack on perturbed data.

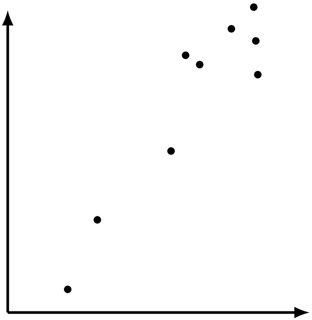
Mutual distances:

Fact Are useful in many analytical techniques.

Claim Do not leak private information.

Data Transformations

Data Transformations — a way to get rid of trust.



Liu, Giannella, Kargupta: Attack on perturbed data.

Mutual distances:

Fact Are useful in many analytical techniques.

Claim Do not leak private information. Wrong!

Attack Scenarios

Things an attacker might know:

Attack Scenarios

Things an attacker might know:

Data sample

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data
- Leaked data

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data
- Leaked data

Probability distribution

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data
- Leaked data

Probability distribution

- National statistical institutes

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data
- Leaked data

Probability distribution

- National statistical institutes
- Previous studies

Attack Scenarios

Things an attacker might know:

Data sample

- Public knowledge
- Own data
- Injected data
- Leaked data

Probability distribution

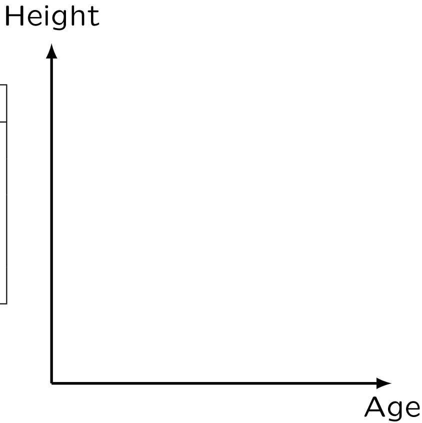
- National statistical institutes
- Previous studies
- Qualified guess

An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-

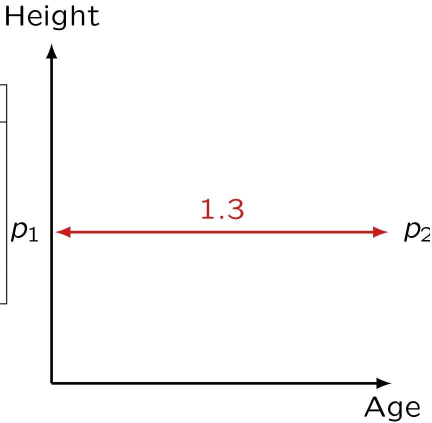
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



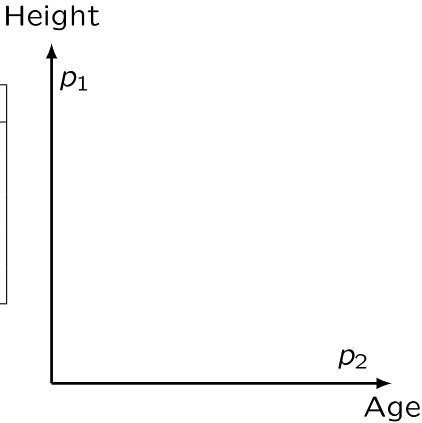
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



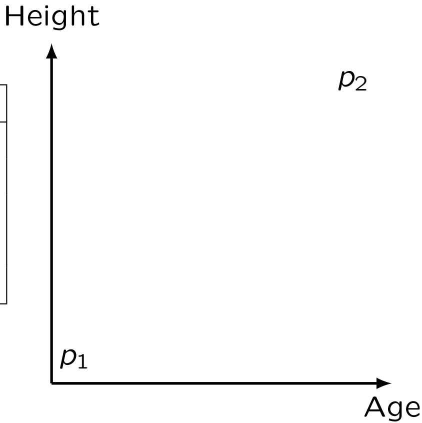
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



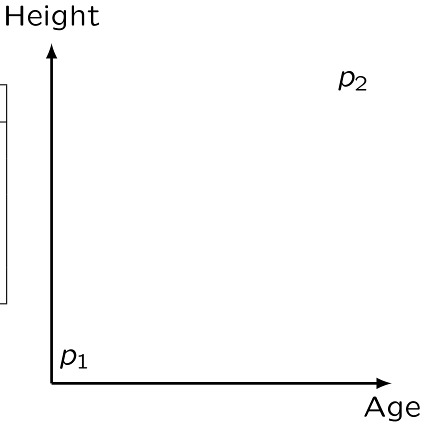
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



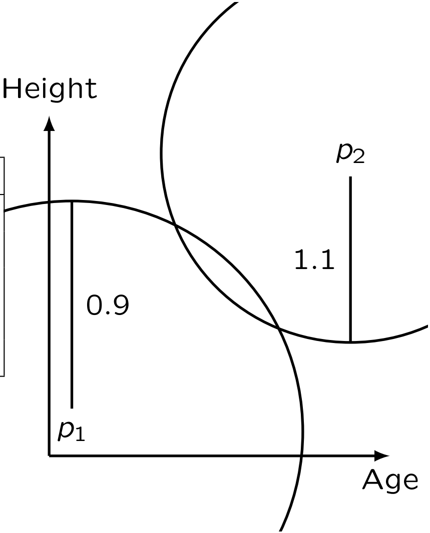
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



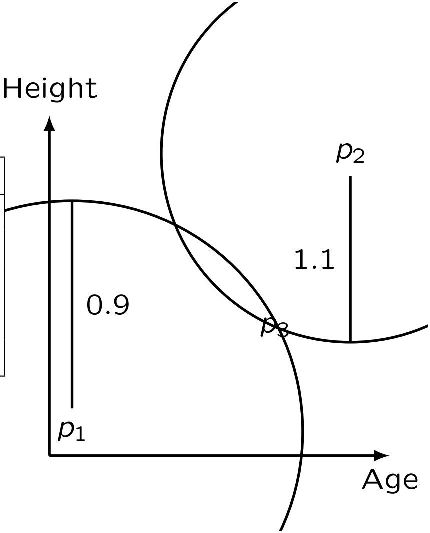
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



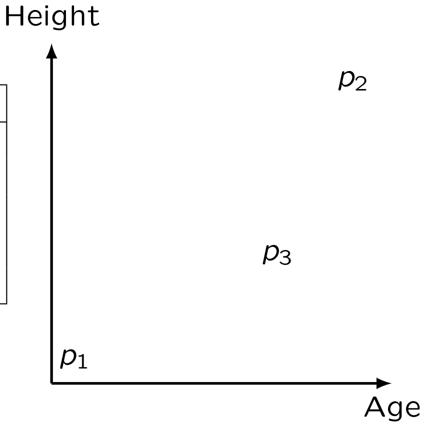
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



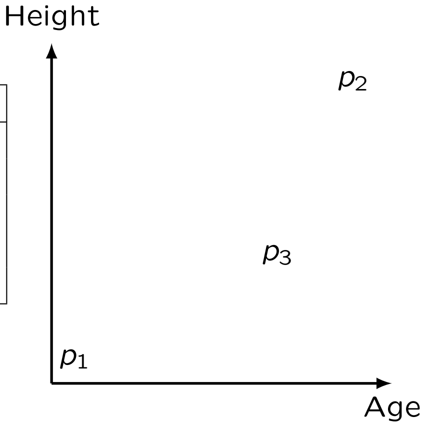
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



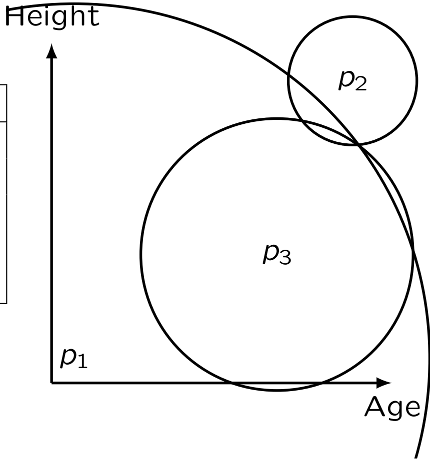
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



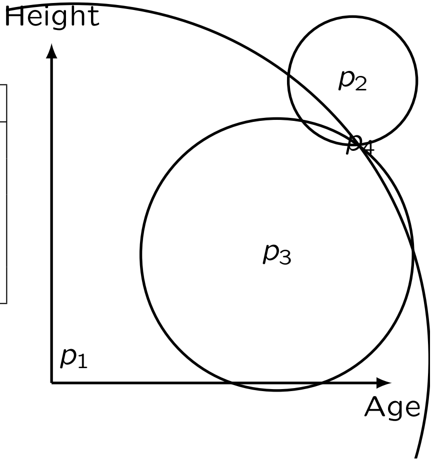
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



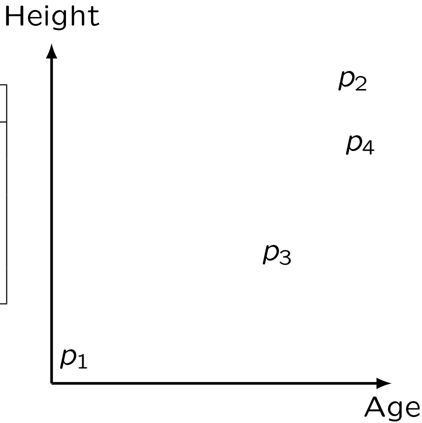
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



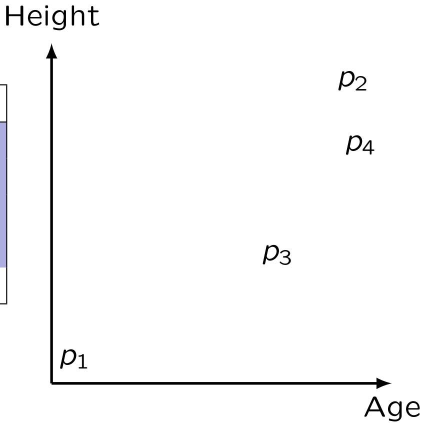
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



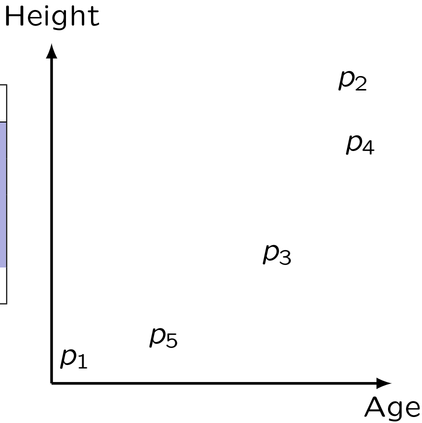
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



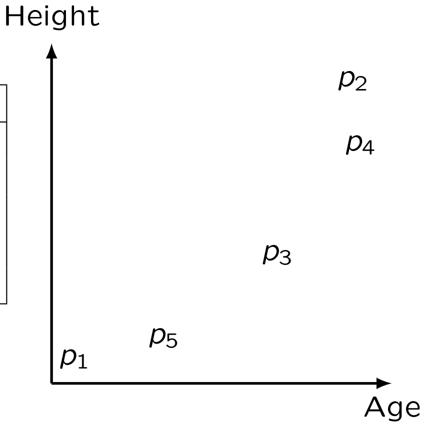
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



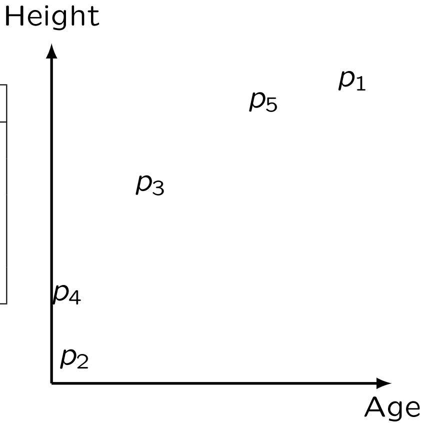
An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



An Example

	p_1	p_2	p_3	p_4	p_5
p_1	-	1.3	0.9	1.2	0.3
p_2	1.3	-	1.1	0.2	1.0
p_3	0.9	1.1	-	0.5	0.5
p_4	1.2	0.2	0.5	-	0.9
p_5	0.3	1.0	0.5	0.9	-



Outline

Motivation

The Attack

Conclusion

Attack Outline

Database n objects with d attributes

Attack Outline

Database n objects with d attributes

Published Distances between objects

Attack Outline

Database	n objects with d attributes
Published	Distances between objects
Attacker	Knows probability distribution

Attack Outline

Database n objects with d attributes

Published Distances between objects

Attacker Knows probability distribution

The attack:

Attack Outline

Database n objects with d attributes

Published Distances between objects

Attacker Knows probability distribution

The attack:

1. Guess $d + 1$ objects.

Attack Outline

Database n objects with d attributes

Published Distances between objects

Attacker Knows probability distribution

The attack:

1. Guess $d + 1$ objects.
2. Use lateration to fix remaining objects.

Attack Outline

Database n objects with d attributes

Published Distances between objects

Attacker Knows probability distribution

The attack:

1. Guess $d+1$ objects.
2. Use lateration to fix remaining objects.
3. Rotate and mirror to fit known distribution.

Hyper-lateration

Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

Hyper-lateration

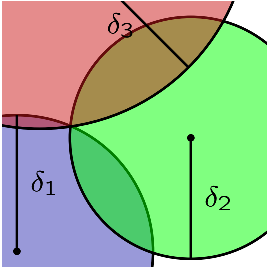
Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

Unknown point $\overline{x}$ at distance $\|\overline{x} - \overline{p}_i\| = \delta_i$

Hyper-lateration

Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

Unknown point $\overline{x}$ at distance $\|\overline{x} - \overline{p}_i\| = \delta_i$



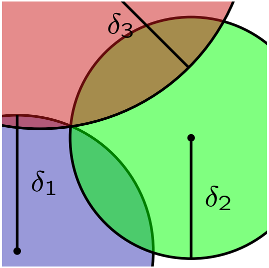
Hyper-lateration

Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

Unknown point $\overline{x}$ at distance $\|\overline{x} - \overline{p}_i\| = \delta_i$

n quadratic equations:

$$\delta_i^2 = \sum_{j=1}^{d} (x_j - p_{ij})^2 = \sum_{j=1}^{d} x_j^2 - 2x_j p_{ij} + p_{ij}^2$$



Hyper-lateration

Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

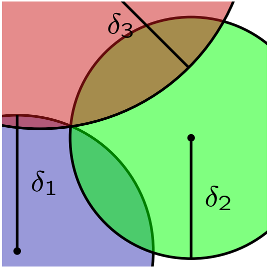
Unknown point $\overline{x}$ at distance $\|\overline{x} - \overline{p}_i\| = \delta_i$

n quadratic equations:

$$\delta_i^2 = \sum_{j=1}^{d} (x_j - p_{ij})^2 = \sum_{j=1}^{d} x_j^2 - 2x_j p_{ij} + p_{ij}^2$$

$n - 1$ linear equations:

$$\delta_i^2 - \delta_0^2 = \sum_{j=1}^{d} 2x_j(p_{0j} - p_{ij}) + p_{ij}^2 - p_{0j}^2$$

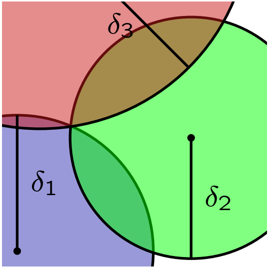


Known points $\overline{p}_1, \ldots, \overline{p}_n \in \mathbb{R}^d$

Unknown point $\overline{x}$ at distance $\|\overline{x} - \overline{p}_i\| = \delta_i$

n quadratic equations:

$$\delta_i^2 = \sum_{j=1}^{d} (x_j - p_{ij})^2 = \sum_{j=1}^{d} x_j^2 - 2x_j p_{ij} + p_{ij}^2$$



$n - 1$ linear equations:

$$\delta_i^2 - \delta_0^2 = \sum_{j=1}^{d} 2x_j(p_{0j} - p_{ij}) + p_{ij}^2 - p_{0j}^2$$

If $n > d$ and $span\{\overline{p}_i\}_i = \mathbb{R}^d$, solution is unique.

Principal Component Analysis

Hyper-lateration Unique up to orthogonal transform.

Principal Component Analysis

Hyper-lateration Unique up to orthogonal transform.

PCA Recognizes orientation of data

Principal Component Analysis

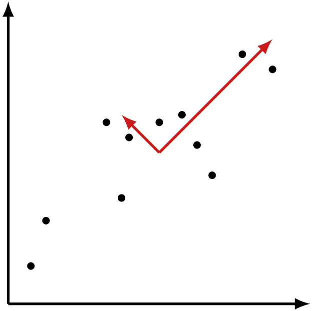
Hyper-lateration: Unique up to orthogonal transform.

PCA: Recognizes orientation of data (does not recognize mirroring).

Principal Component Analysis

Hyper-lateration Unique up to orthogonal transform.

PCA Recognizes orientation of data (does not recognize mirroring).



Principal Component Analysis

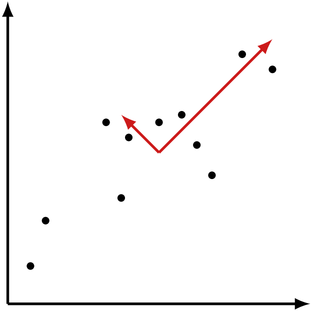
Hyper-lateration Unique up to orthogonal transform.

PCA Recognizes orientation of data (does not recognize mirroring).

Covariance matrix:

$$\Sigma = \begin{bmatrix} Cov(A_1, A_1) & \cdots & Cov(A_1, A_d) \\ \vdots & & \vdots \\ Cov(A_d, A_1) & \cdots & Cov(A_d, A_d) \end{bmatrix},$$

$$Cov(A, B) = E[(A - \mu)(B - \nu)].$$



Principal Component Analysis

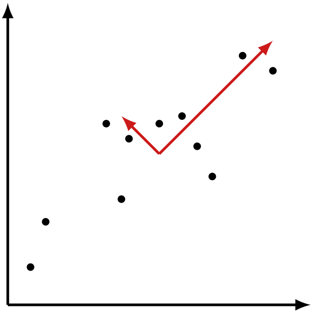
Hyper-lateration Unique up to orthogonal transform.

PCA Recognizes orientation of data (does not recognize mirroring).

Covariance matrix:

$$\Sigma = \begin{bmatrix} Cov(A_1, A_1) & \cdots & Cov(A_1, A_d) \\ \vdots & & \vdots \\ Cov(A_d, A_1) & \cdots & Cov(A_d, A_d) \end{bmatrix},$$

$Cov(A, B) = E[(A - \mu)(B - \nu)]$.
Eigenvectors, and values:
$(\overline{e}_1, \lambda_1), \ldots, (\overline{e}_d, \lambda_d)$.



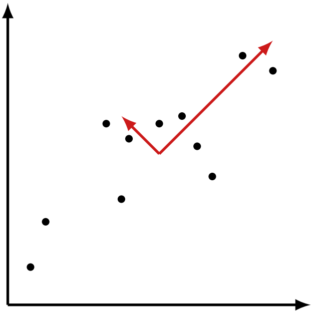
Principal Component Analysis

Hyper-lateration Unique up to orthogonal transform.

PCA Recognizes orientation of data (does not recognize mirroring).

Covariance matrix:

$$\Sigma = \begin{bmatrix} Cov(A_1, A_1) & \cdots & Cov(A_1, A_d) \\ \vdots & & \vdots \\ Cov(A_d, A_1) & \cdots & Cov(A_d, A_d) \end{bmatrix},$$



$Cov(A, B) = E[(A - \mu)(B - \nu)]$.
Eigenvectors, and values:
$(\overline{e}_1, \lambda_1), \ldots, (\overline{e}_d, \lambda_d)$.

Do this for both hyper-laterated points and sample drawn from known distribution.

The Attack

1. Guess first d objects

The Attack

1. Guess first d objects
   (unique up to rotation and mirroring)

The Attack

1. Guess first d objects
   (unique up to rotation and mirroring)
2. Find remaining objects with lateration

The Attack

1. Guess first d objects
   (unique up to rotation and mirroring)
2. Find remaining objects with lateration
3. Find principal components

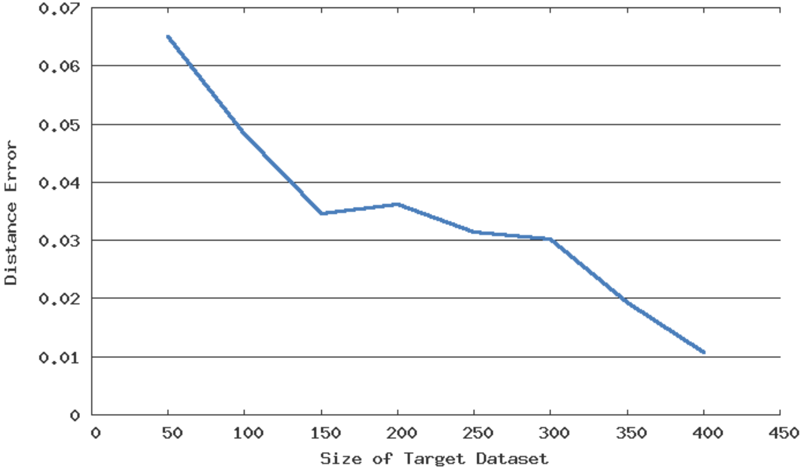
The Attack

1. Guess first d objects
   (unique up to rotation and mirroring)
2. Find remaining objects with lateration
3. Find principal components
4. Rotate to match principal components of known probability distribution

The Attack

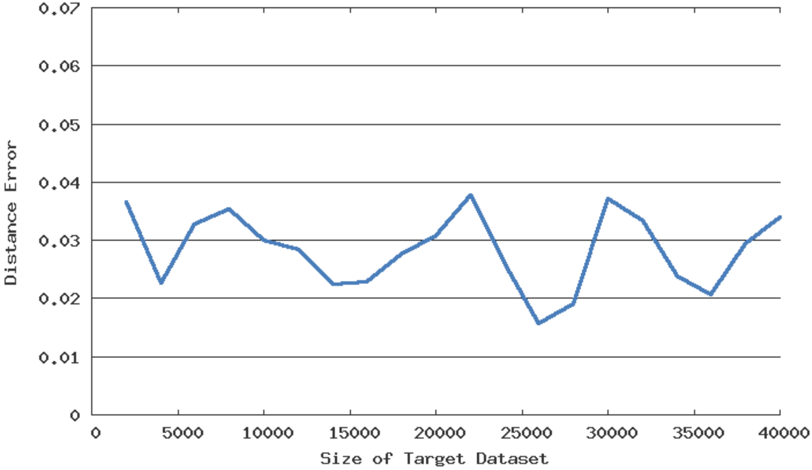
1. Guess first d objects
   (unique up to rotation and mirroring)
2. Find remaining objects with lateration
3. Find principal components
4. Rotate to match principal components of known probability distribution
5. Find best mirroring (optimized)

Attack Accuracy (1)



Auto Miles per Gallon (using 5 attributes)

Attack Accuracy (2)



US Adult Census (using 4 attributes)

Outline

Motivation

The Attack

Conclusion

Conclusion

Known	**Leaked**
Sample of $d+1$ objects	Everything
Probability distribution	Everything with high fidelity

Conclusion

Known	**Leaked**
Sample of $d+1$ objects	Everything
Probability distribution	Everything with high fidelity

Never publish distances between data points!

Conclusion

Known	Leaked
Sample of $d+1$ objects	Everything
Probability distribution	Everything with high fidelity

Never publish distances between data points!

Thank You