Introduction to Privacy Enhancing Technology

Jointly organized by:

Classic analysis:
Collect the data in one place

VANTAGE
WORKSHOP

Name	Weight	Height
Bahati	20	180
Winifred	80	153

Name	Weight	Height
Charles	50	170
Brandi	45	163

Name	Weight	Height
Bahati	20	180
Winifred	80	153
Charles	50	170
Brandi	45	163

Jointly organized by:
netherlands eScience center
KNL

Data anonymization: Remove sensitive fields

VANTAGE WORKSHOP

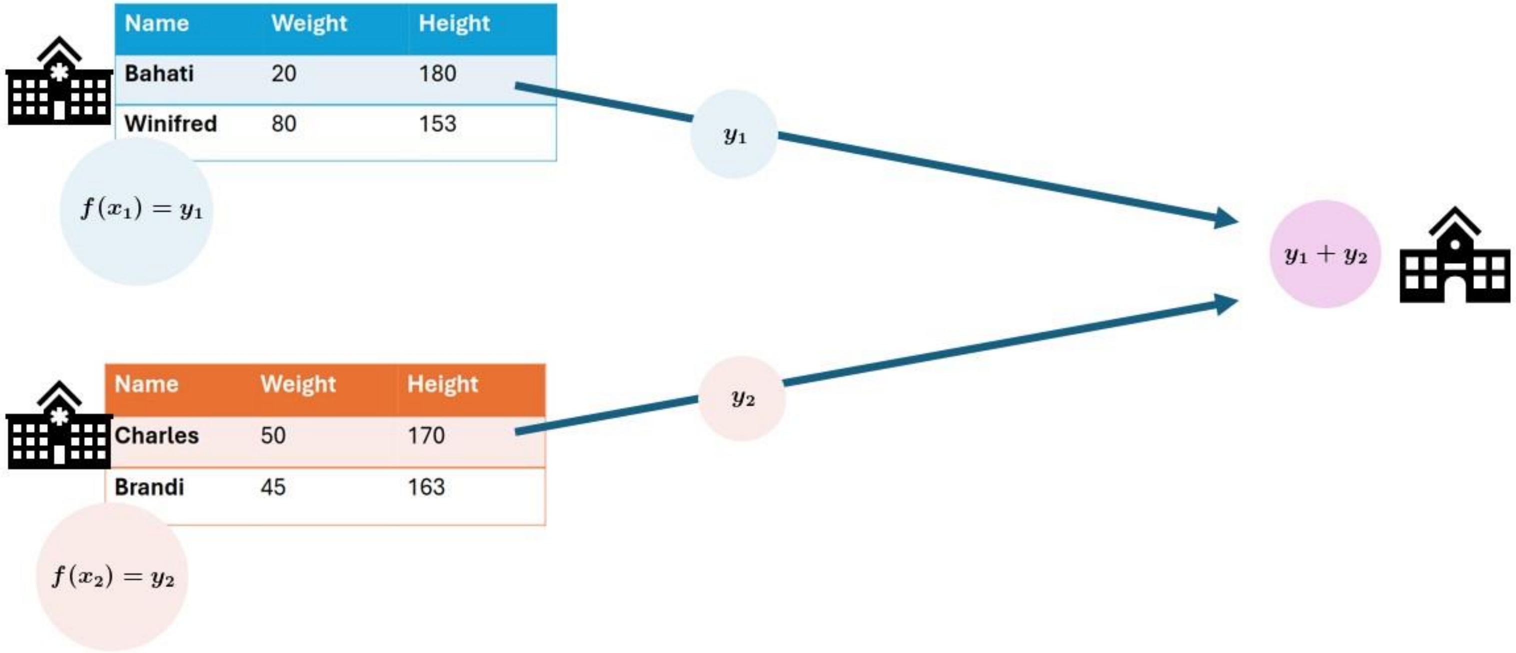
Name	Weight	Height
[redacted]	20	180
[redacted]	80	153

Name	Weight	Height
[redacted]	50	170
[redacted]	45	163

Name	Weight	Height
[redacted]	20	180
[redacted]	80	153
[redacted]	50	170
[redacted]	45	163

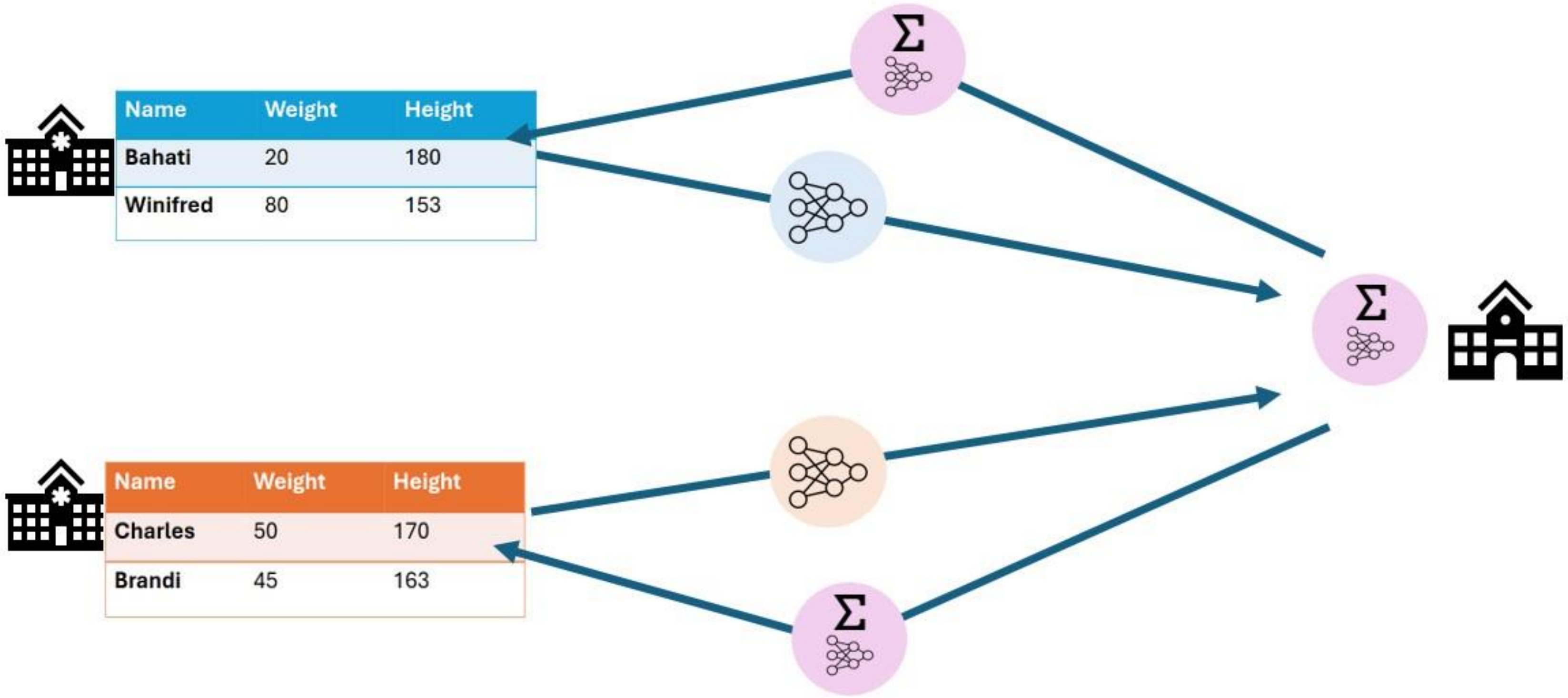
Federated data analysis:
Send analysis to the source, then aggregate

VANTAGE WORKSHOP



Federated learning: Train models locally, then aggregate

VANTAGE WORKSHOP



Name	Weight	Height
Bahati	20	180
Winifred	80	153

Name	Weight	Height
Charles	50	170
Brandi	45	163

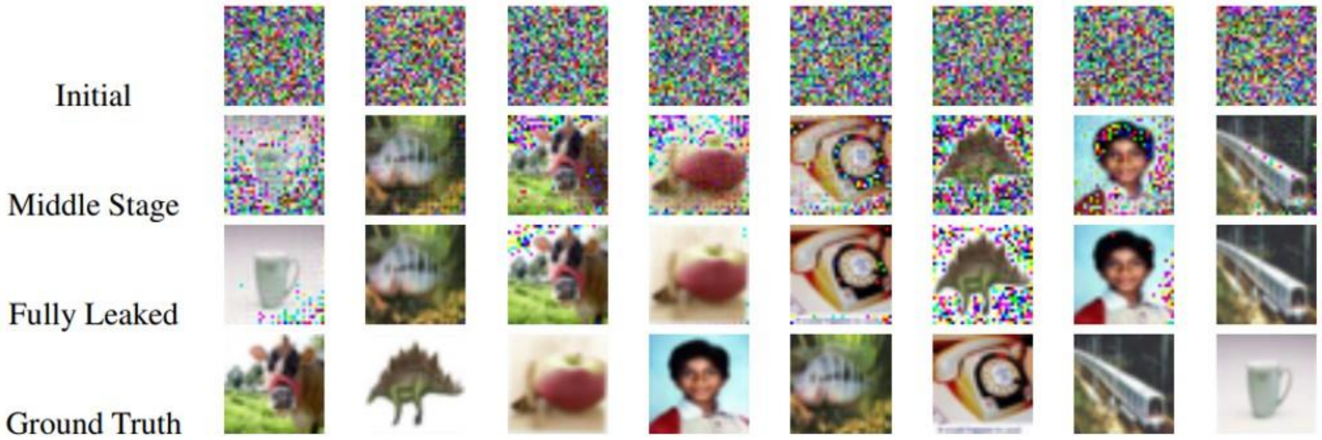
Jointly organized by:

netherlands eScience center

KNL

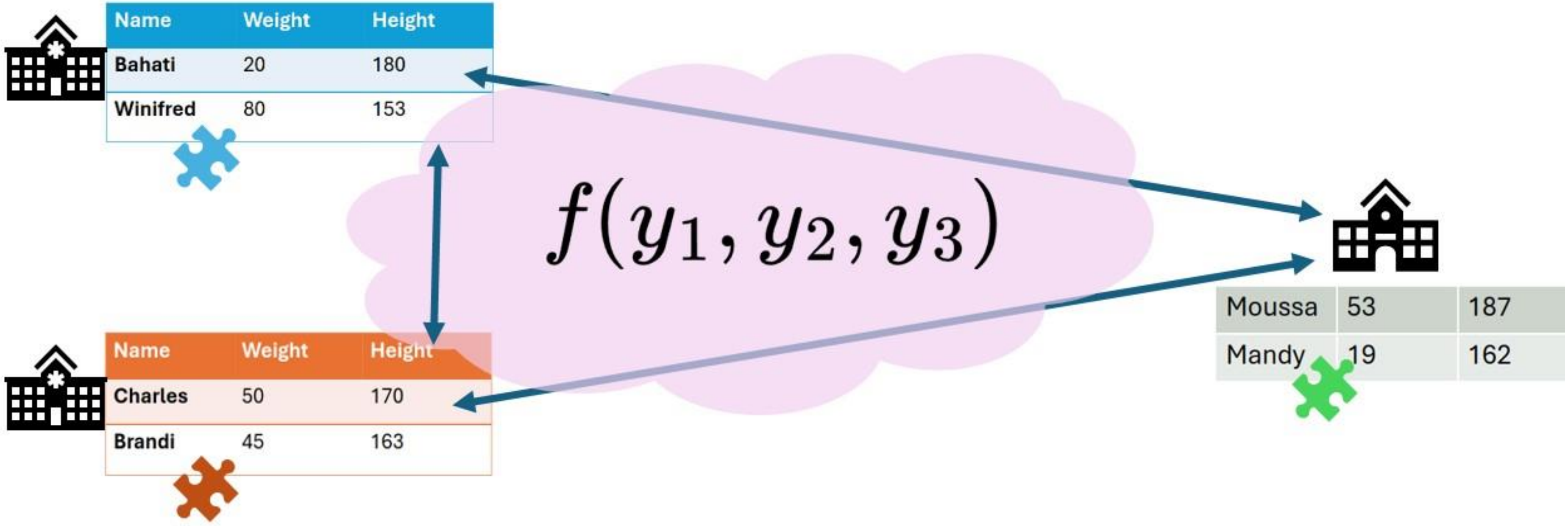
Federated learning and analysis can still leak data!

Gradient leakage



Zhu, Ligeng, Zhijian Liu, and Song Han. "Deep leakage from gradients." Advances in neural information processing systems 32 (2019).

Secure multiparty computation: Send around encrypted puzzle pieces

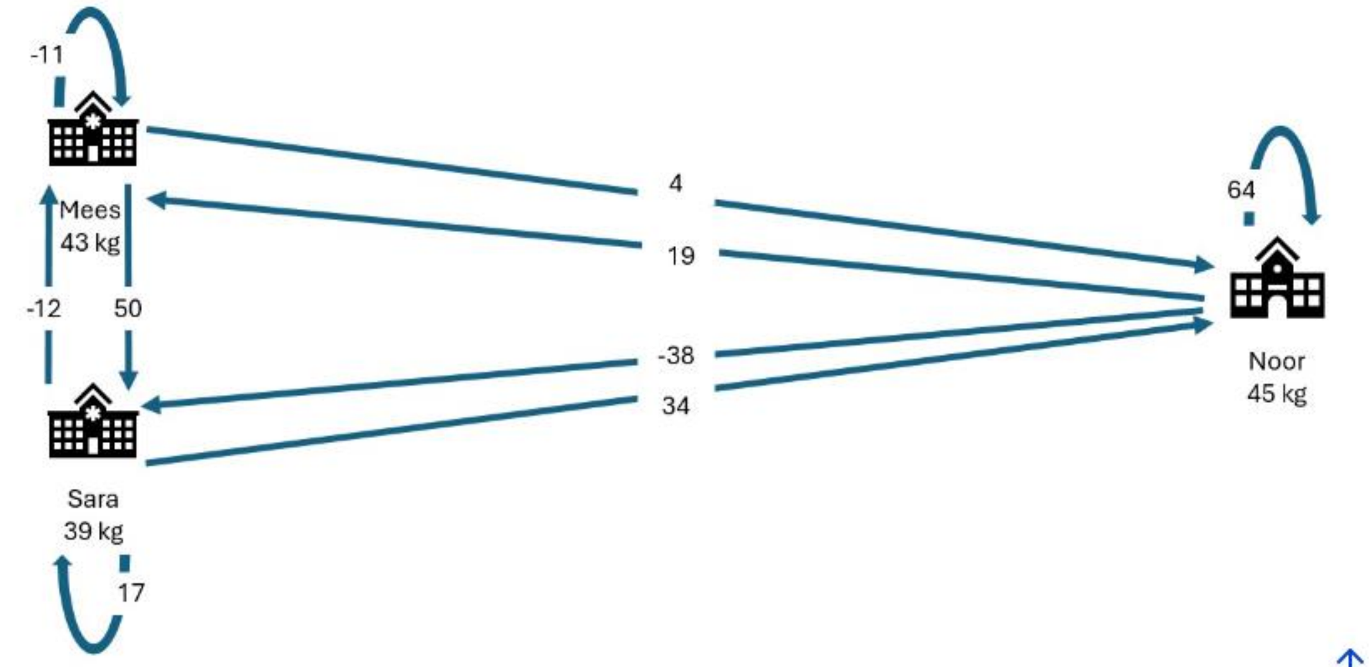


Secret sharing: an example

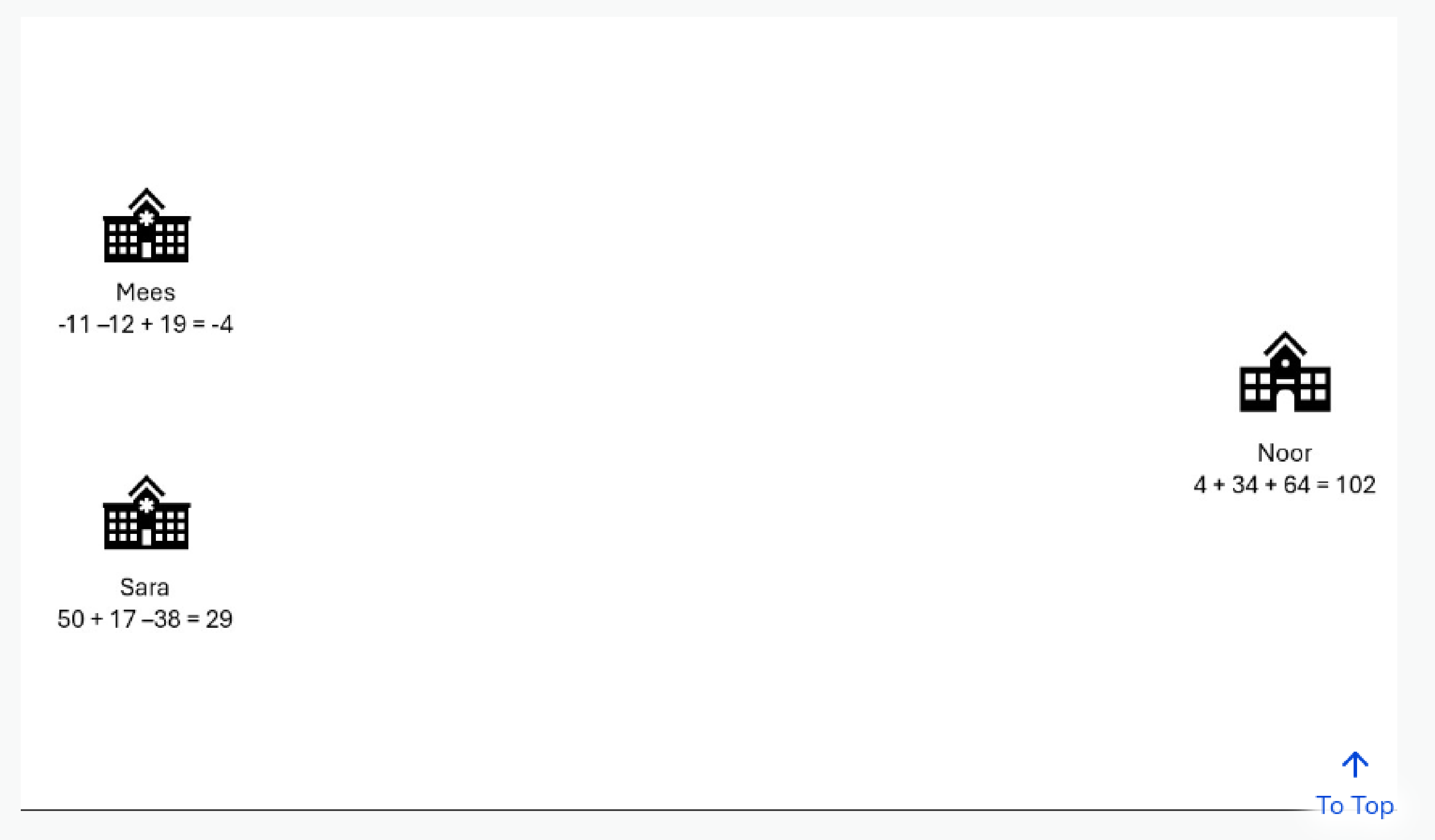
SECRET SHARING, AN EXAMPLE

Mees, Sara and Noor want to know how much they weigh in total. Mees weighs 43 kg, Sara weighs 39, Noor weighs 45. All three they think of 2 random numbers r_1 and r_2 so that $weight = r_1 + r_2 + x$. Finally they compute x by $x = weight - r_1 - r_2$

After computing the secret shares, they distribute these “cryptographical puzzle pieces” among their peers.

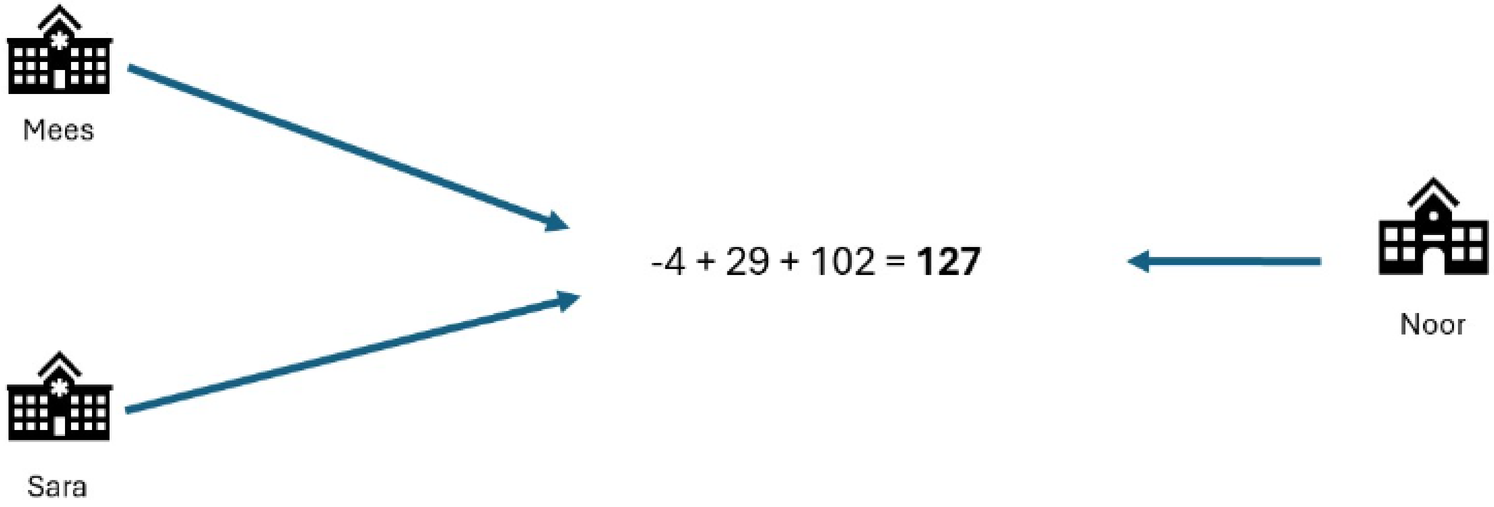


Secret sharing: an example



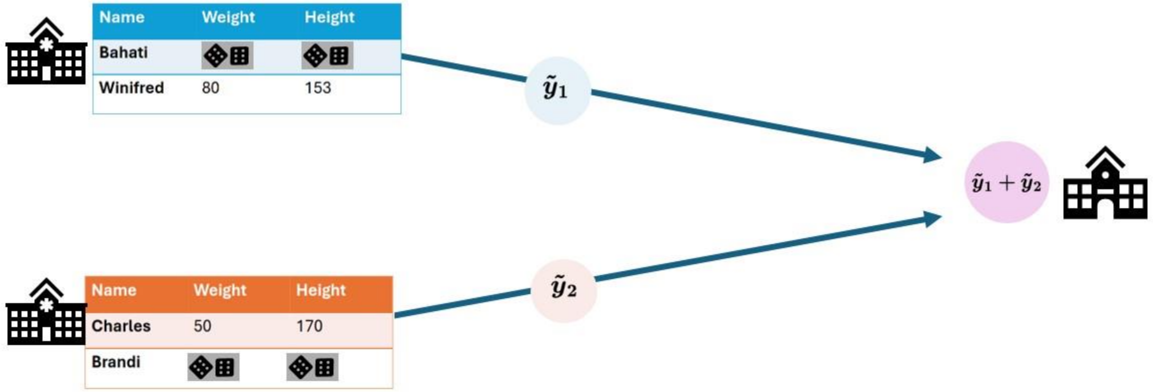
Secret sharing: an example

They add their sums together: -4 + 29 + 102 = 127 In this way, they have aggregated their data without sharing their individual data with anyone else.



To Top

Differential privacy: Add noise



Data partitioning

VANTAGE WORKSHOP

Horizontal partitioning

Name	Weight	Height
Charles	50	170
Brandi	45	163

Name	Weight	Height
Jez	33	193
Deonne	25	168

Vertical partitioning

Name	Weight
Bahati	20
Winifred	80
Ben	62
Zayden	18

Name	Height
Bahati	180
Winifred	153
Ben	198
Zayden	182

Projects usually combine techniques

Jointly organized by:

netherlands eScience center KNL

Technology doesn't solve everything!

VANTAGE WORKSHOP

- Privacy enhancing technology is only a small part of the data sharing puzzle
- Some other factors
  - Trust
  - Regulations (either general or specific to the location)
  - Data harmonization