

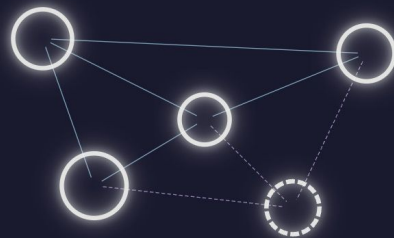


Thesis defense

Rob Romijnders

October 12th, 2026

Learning from Private Data:
Algorithms for Decentralized and
Differentially Private Machine Learning



We live in a period of data-hungry AI

AI has rapid adoption among consumers

33% of general EU population used AI chatbots in 2025 (and 64% of 16-24 y.o.)

AI is trained on lots of data, and gets better with more data

Frontier models are trained on 30+ trillion tokens and see returns from more data

Yet the majority of data is private and behind firewalls

Studies estimate that 50% to 90% of data is private and unused

if only this data could be accessed without compromising privacy

<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20260210-1>

Villalobos et al. ICML 2024; Kaplan et al. 2020

<https://www.cycloneinteractive.com/sites/cyclone/assets/File/idc-digital-universe-infobrief.pdf>

<https://www.ibm.com/think/topics/ai-ready-data>

<http://www.ibmbigdatahub.com/blog/big-data-challenge-transformation-manufacturing-industry>

if only this data could be accessed without compromising privacy

This thesis presents six studies towards this goal:

“Learning from Private Data”

(1) Decentralized contact tracing

(4) Differential privacy in 2-layer perceptrons

(2) Contact tracing under differential privacy

(5) Differential privacy in Mixture-of-Experts models

(3) Neural augmentation differential privacy

(6) Privacy in the use of Large Language models

Illustration

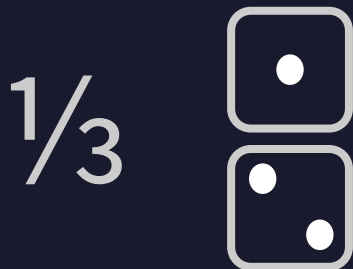
Privacy-sensitive questions:

- “Did you vote for this party in the election, yes or no?”
- “Do you live at this GPS location, yes or no?”
- “Do you have medical condition x, yes or no?”
- “Do you like this product, yes or no?”

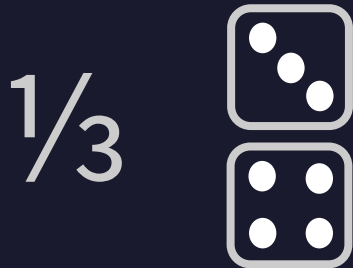
These are example yes/no questions and serve as illustration for bigger tasks such as real-valued scores, or neural network weights.

Plausible deniability

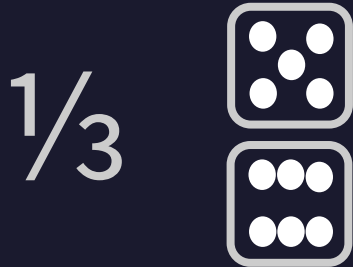
Noisy answer to yes/no question



Fixed to “yes”



Fixed to “no”



Tell the **local answer**

Noisy response to yes/no question

$1/3$



Fixed to “yes”

126 out of 200 responded YES

$1/3$



Fixed to “no”

What does that tell us?

$1/3$



Tell the local answer

Still, everyone has “plausible deniability”

Noisy response to yes/no question

$1/3$



Fixed to “yes”

126 out of 200 responded YES

$1/3$



Fixed to “no”

What does that tell us?

$1/3$



Tell the local answer

Estimate of 89%

and everyone has “plausible deniability”

Elements of a “noisy thing” in this thesis

Chapters 2, 3, and 4: the “noisy thing” is the risk score of COVID19

Chapters 5 and 6: the “noisy thing” are the weights of a neural network

Chapter 7: the “noisy thing” is the response from a Large Language Model

A case for decentralization

- **Centralization of information is often not necessary**
- **Centralization carries risk of data breaches and hacks**

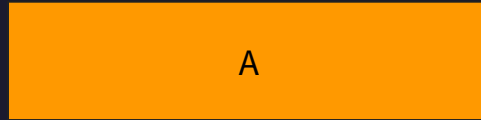
-> Illustrated on the next slide with an example

“What is the **average heartrate** in this room?”

*Central hub
not required!*



Step 1: send data among others



Step 2: sum with others



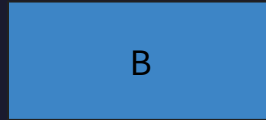
Step 3: average

“What is the **average heartrate** in this room?”

*Central hub
not required!*



Step 1: send data among others



Step 2: sum with others



Step 3: average

“What is the **average heartrate** in this room?”

*Central hub
not required!*



Step 1: send data among others



Step 2: sum with others



Step 3: average

Decentralized and privacy-preserving contact tracing

Economic impact of COVID 19 pandemic was enormous

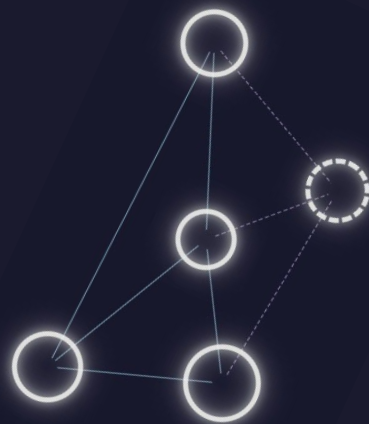
Studies estimate a trillion USD economic loss and mental-health consequences

The main cited reason for low adoption is privacy concerns

Among population studies in three countries totaling 7,000+ respondents

We propose a decentralized algorithm with DP guarantees

Study received oral presentation at AAAI-24 conference



Overview

Beyond current open data,



Web



Books



Videos

*there is **untapped data** to
further improve AI systems:*



Files



E-mails



Records



Purchases



Locations



and more



This raises challenges



***towards which we make the
following contributions:***

Trust & Safety

Decentralized contact tracing

Ch. 2

... with differential privacy

Ch. 3

... and general purpose neural networks

Ch. 4

Efficiency

Privately learning models without revealing intermediate steps

Ch. 5

Privacy in LLMs

Modular LLM with private knowledge transfer

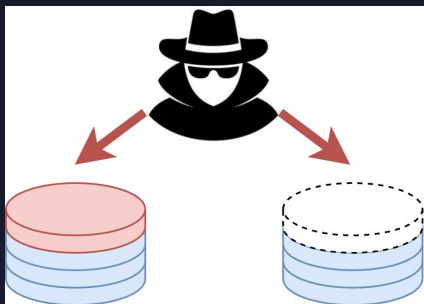
Ch. 6

Private in-context learning for LLMs

Ch. 7

Appendix slides

Slides after this are supplementary



What does DP mean?

