



DNA: Differential Privacy Neural Augmentation for Contact Tracing

Learning on Graphs - Amsterdam, 26 Nov

github.com/RobRomijnders/DNA

Rob Romijnders, Christos Louizos, Yuki M. Asano, Max Welling



Brain, Behavior, and Immunity

Volume 89, October 2020, Pages 531-542





Review Article

COVID-19 pandemic and mental health consequences: Systematic review of the current evidence

Nina Vindegaard, Michael Eriksen Benros  

Show more 

+ Add to Mendeley  Share  Cite

<https://doi.org/10.1016/j.bbi.2020.05.048> 

[Get rights and content](#) 




























Best Practice & Research Clinical Anaesthesiology

Volume 35, Issue 3, October 2021, Pages 293-306



2

Economic impact of COVID-19 pandemic on healthcare facilities and systems: International perspectives

Alan D. Kaye MD, PhD (Provost & Vice Chancellor of Academic Affairs).^a  ,
Chikezie N. Okeagu MD (Assistant Professor).^b  , Alex D. Pham MD (Resident Physician).^c  ,
Rayce A. Silva (Medical Student).^d  , Joshua J. Hurley MD, PGY-1 (Resident Physician).^e  ,
Brett L. Arron MD (Associate Professor).^f  , Noeen Sarfraz MD MPH (Resident Physician).^g  ,
Hong N. Lee MD (Assistant Professor).^h  , G.E. Ghali DDS, MD, FACS, FRCS(Ed) (Chancellor).ⁱ  ,
Jack W. Gamble (Professor and Chairman).^j  , Henry Liu MD (Professor).^k  ,
Richard D. Urman MD (Associate Professor).^k  ,
Elyse M. Cornett PhD (Assistant Professor).^h  

Show more 

Covid-19: Cities fear 'huge' economic impact of restrictions

 29 September 2020

BBC, Sept 2020

Covid had negative impact on children's reading - Estyn

 4 May

BBC, May 2023

This interactive tool tracks covid-19 travel restrictions by country

Skyscanner's detailed travel map is color-coded in stoplight-style green, yellow and red

Washington Post, December 2020

Privacy is important

“The top reasons against app use were as follows: mistrusting the government, concerns about data security and **privacy**, and doubts about efficacy.” Jones et al. 2021

Privacy is important

“The top reasons against app use were as follows: mistrusting the government, concerns about data security and **privacy**, and doubts about efficacy.” Jones et al. 2021

“The most cited reasons for not downloading were related to **data (...)** **concerns**” Gao et al. 2022

Privacy is important

“The top reasons against app use were as follows: mistrusting the government, concerns about data security and **privacy**, and doubts about efficacy.” Jones et al. 2021

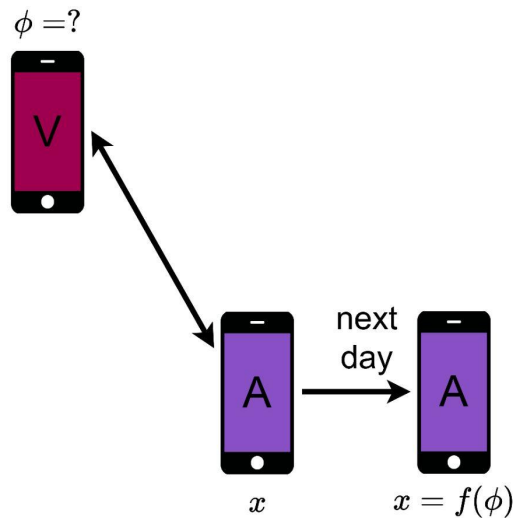
“The most cited reasons for not downloading were related to **data (...)** **concerns**” Gao et al. 2022

“The main reasons for not downloading and using the app were (...) **worries about privacy**” Walrave et al. 2022

Attack Scenario on contact tracing apps

Privacy with respect to
released risk score

V is victim, A is attacker

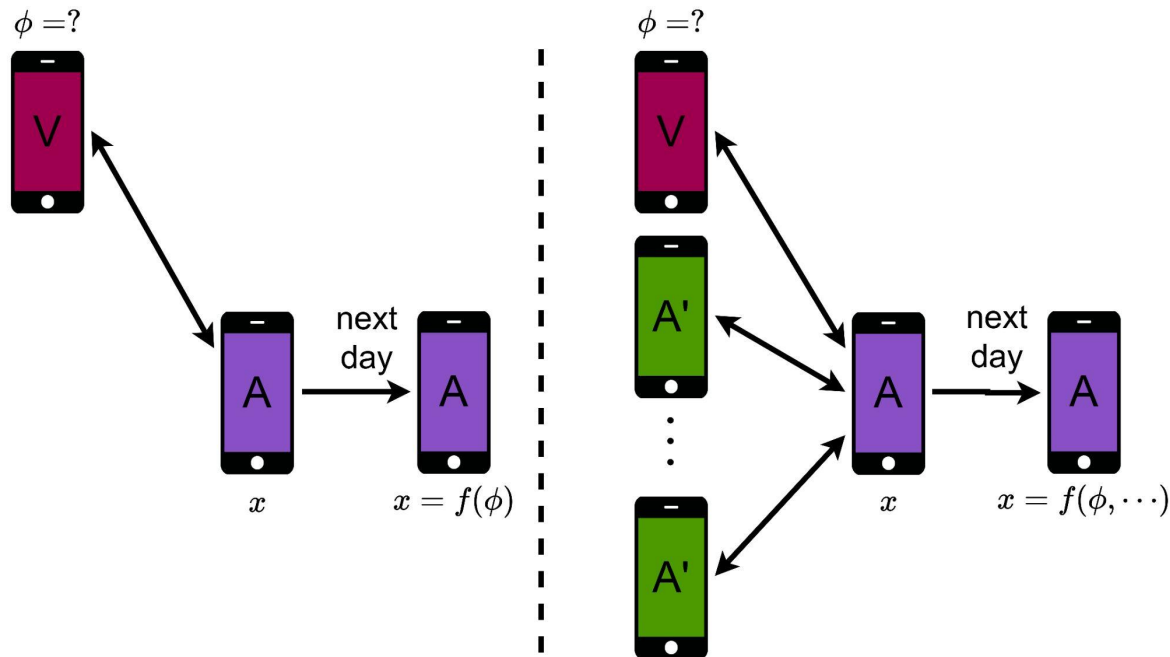


Attack Scenario

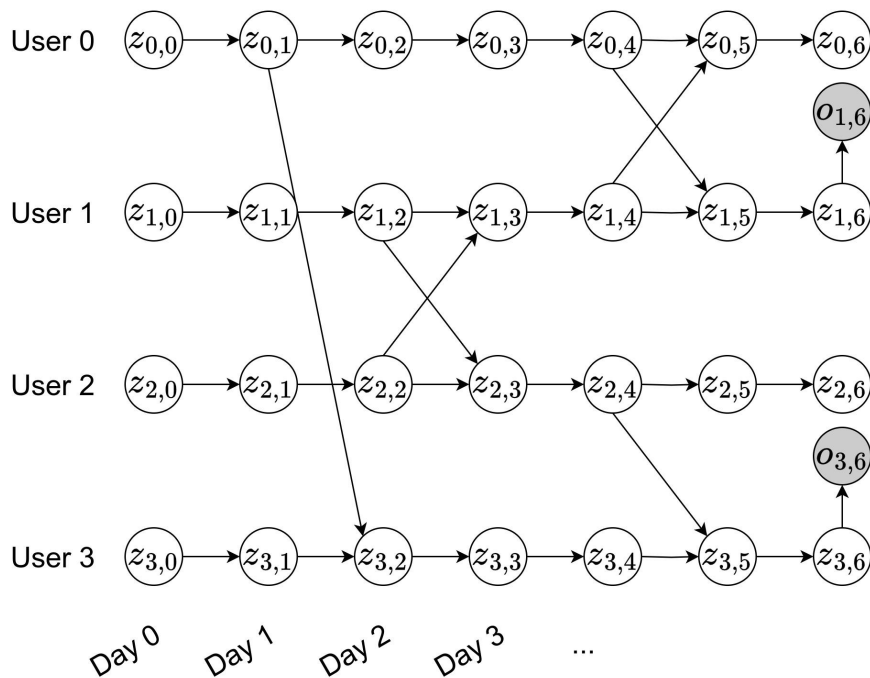
Privacy with respect to
released covidscore

V is victim, A is attacker

Green phones, A' are
co-attackers

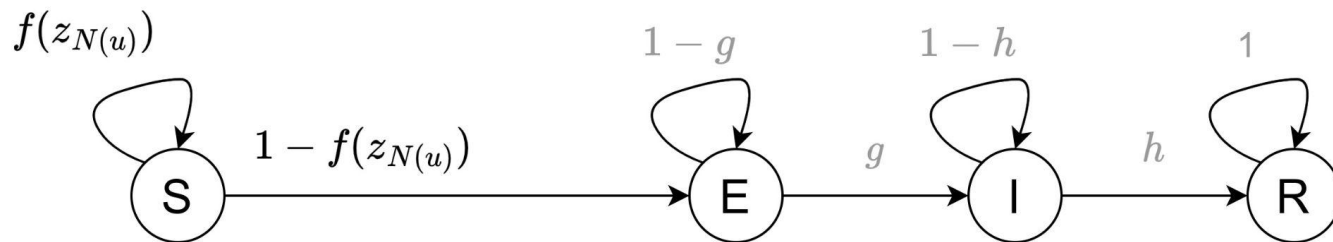


Example of graphical model of 4 users in 6 days



Statistical model for contact tracing

Susceptible - Exposed - Infected - Recovered



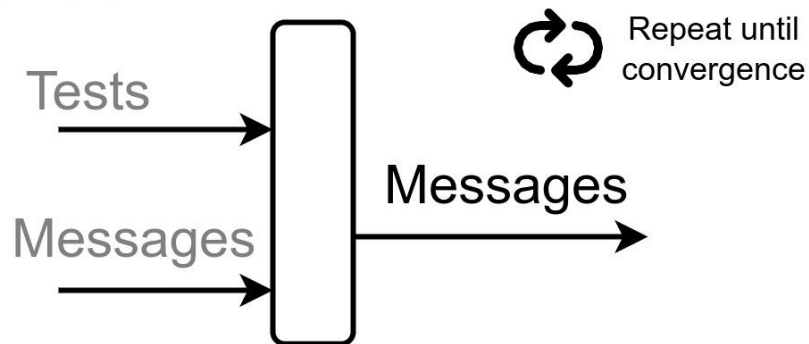
$$f(z_{N(u)}) = (1 - p_0)(1 - p_1)^{|\{z \in z_{N(u)} : z=I\}|}$$

Modular view

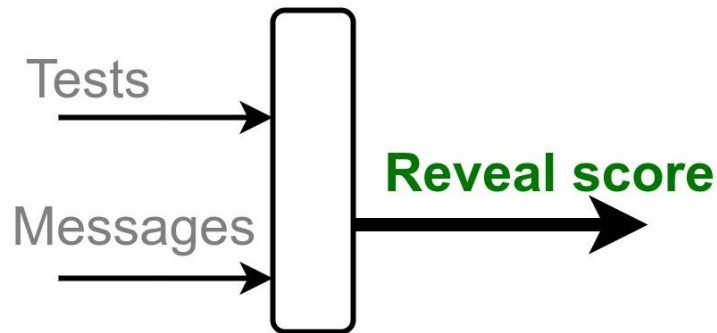
Do approximate inference by
either Belief Propagation or
Factorized Neighbors

$$\begin{aligned} b_u(z_u) &= \sum_{z_{N(u)}} P(z_u | z_{N(u)}, \mathcal{O}) B_{N(u)}(z_{N(u)}) \\ &= E_{B_{N(u)}(z_{N(u)})} [P(z_u | z_{N(u)}, \mathcal{O})]. \end{aligned}$$

Inference



Predict



Practical use of Differential Privacy

- Emoji suggestions at **Apple**
- QuickType suggestions at **Apple**
- **US Census** releases data under DP
- Executive order US gov. mentions Differential Privacy multiple times
- **Governments** releasing birth rate data
- **Facebook** releases mobility data of users during covid pandemic
- **Google GBoard** language next word prediction
- **LinkedIn** user analytics
- Telemetry on **Windows**

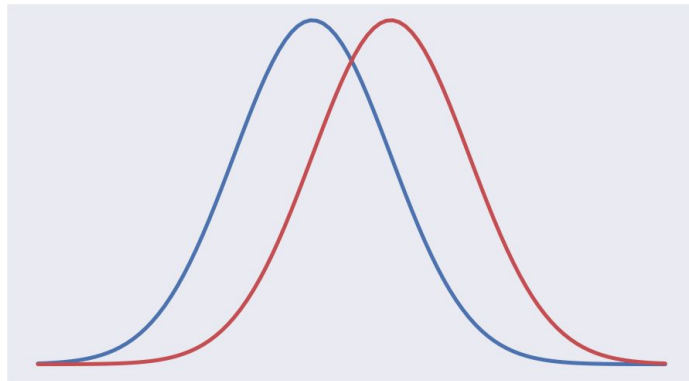
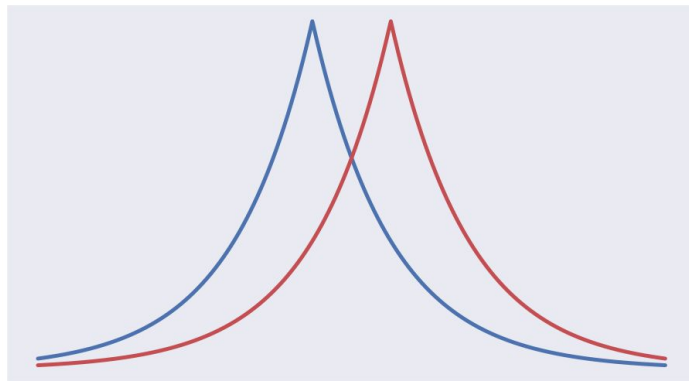
Differential privacy

Definition of (ε, δ) differential privacy (Dwork and Roth 2014):
for every $\varepsilon > 0$, $\delta \in [0, 1)$, a mechanism $f(\cdot)$, for any outcome Φ in the range of $f(\cdot)$, and any two adjacent data sets D, D' that differ in at most one element, satisfies the constraint:

$$p(f(D) \in \Phi) \leq e^\varepsilon p(f(D') \in \Phi) + \delta$$

Gaussian Mechanism:

$$\sigma > \frac{\Delta}{\varepsilon} \left(2 \log \left(\frac{1.25}{\delta} \right) \right)^{\frac{1}{2}}$$



Desiderata

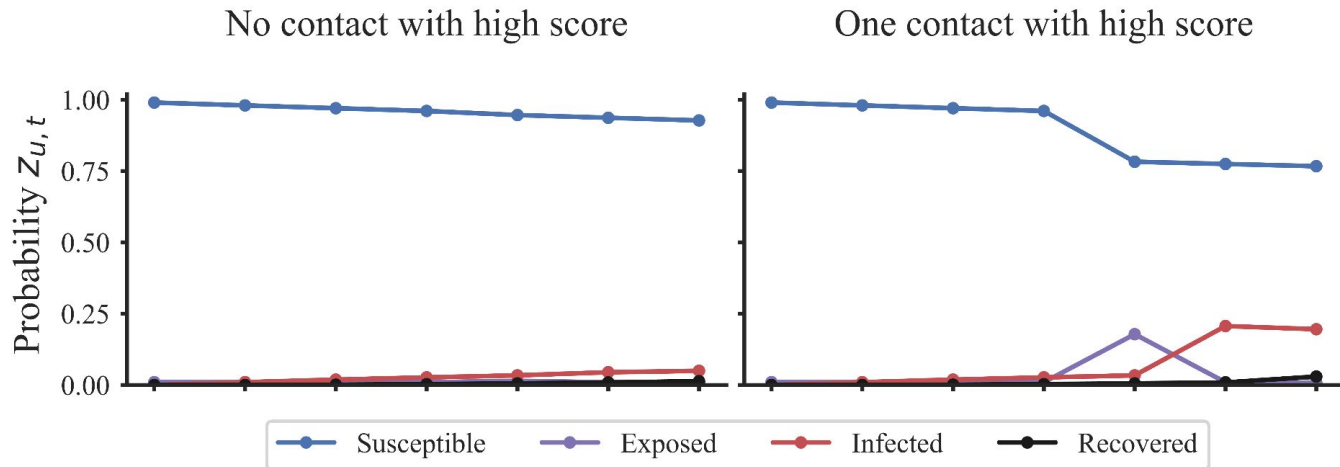
Plausible deniability

Privacy

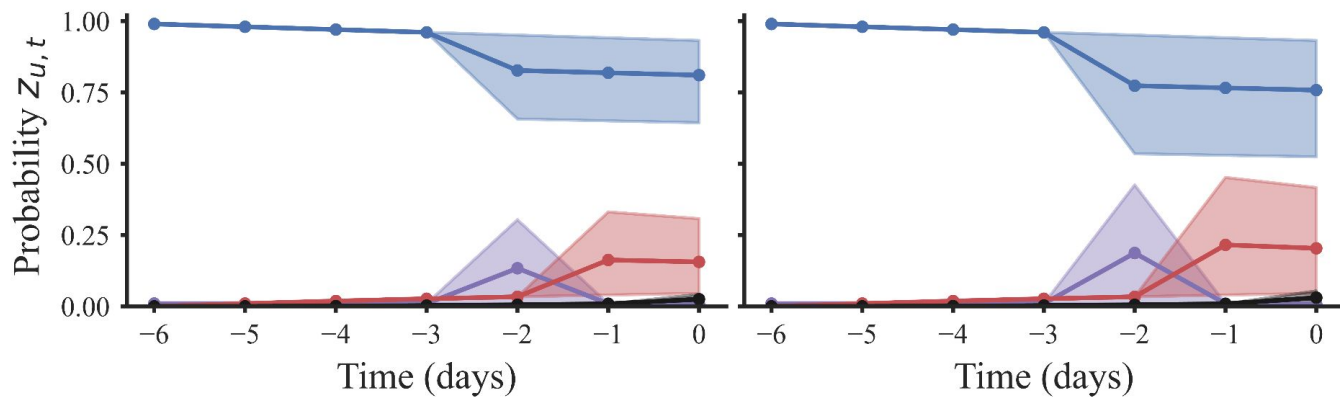
and

High utility

Without DP



$(\epsilon = 1)$ -DP



Privacy bound, definition of adjacent datasets

Dataset:

$$D = \{(\mu_i, t_i)\}_{i=1}^C$$

Sensitivity:

$$\Delta = \max_{\mu_1, \mu'_1 \in [0, \gamma_u]} |F((\mu_1, t_1) \cup D) - F((\mu'_1, t_1) \cup D)| \leq p_1 \gamma_u \quad \forall D.$$

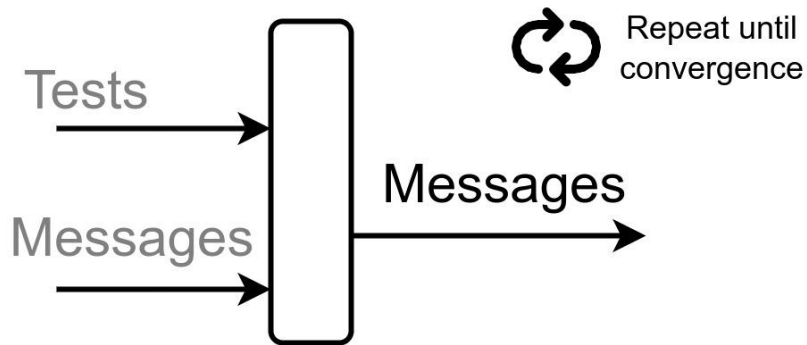
p_1 around 0.05, and gamma around 0.7

Neural Augmentation

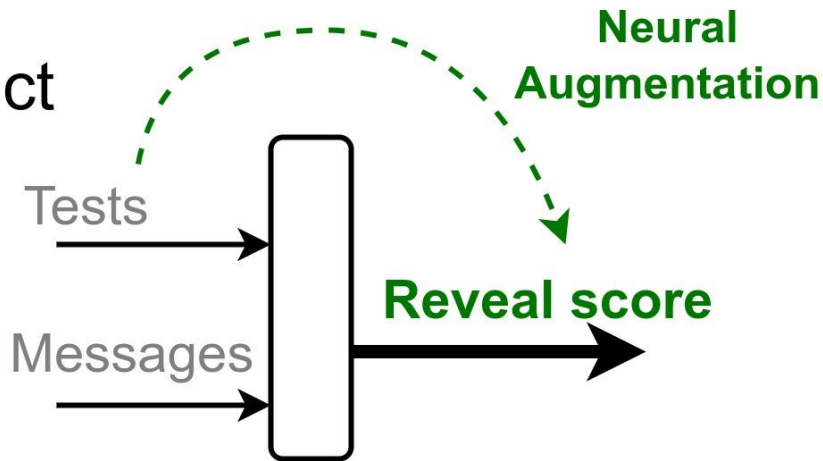
Neural augmentation known from:

- MRI reconstruction
(Lønning et al. Medical image analysis, 2019)
- Enhanced belief propagation
(Satorras et al., AISTATS 2021)
- Fast sparse coding
(Gregor et al. ICML 2010)

Inference



Predict



Lipschitz-bounded Neural Network

$$\phi = G_{\theta}(\{(\mu_i, t_i)\}_{i=1}^{C_T}) = g_{\theta}^{(2)}\left(\frac{1}{C} \sum_i g_{\theta}^{(1)}([\mu_i, t_i]^T)\right)$$

During training: estimate Lipschitz constant with power iterations $O(p^2)$

During testing: calculate Spectral norm exactly once $O(p^3)$

Make Lipschitz function DP with Gaussian noise

Algorithm 1 DNA: Differentially private Neural Augmentation

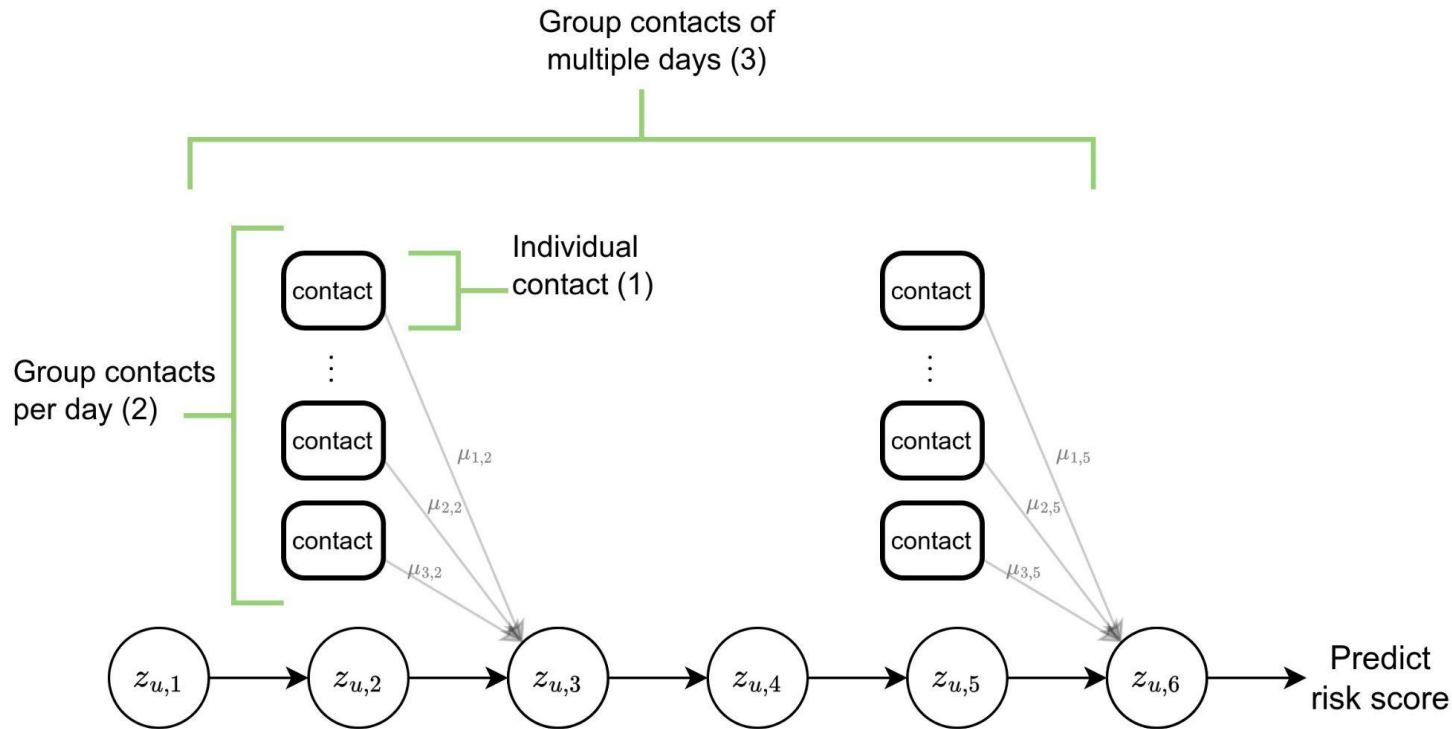
Require: Dataset $D = \{(\mu_i, t_i)\}_{i=1}^{C_T}$, constants $p_1, \gamma_u \in (0, 1)$;

$$\mu_i \leftarrow \min(\mu_i, \gamma_u)$$

$$\bar{\phi} \leftarrow F(\{(\mu_i, t_i)\}_{i=1}^{C_T}) + p_1 \times G_{\theta}(\{(\mu_i, t_i)\}_{i=1}^{C_T})$$

$$\phi \leftarrow \bar{\phi} + \mathcal{N}(0, \frac{2}{\varepsilon^2}(\gamma_u p_1(1 + \frac{1}{C_T}))^2 \log(\frac{5}{4\delta}))$$

Privacy hierarchy



Different algorithms to compare on simulator

- Traditional contact tracing (Baker et al. 2021)
- Per-message, level 1 (Romijnders et al. 2023)
- Per-day, DPFN, level 2 (Romijnders et al. 2024)
- Per-window, DPFN-S, level 3 (Ours)
- Per-window, DNA, level 3+ (Ours)

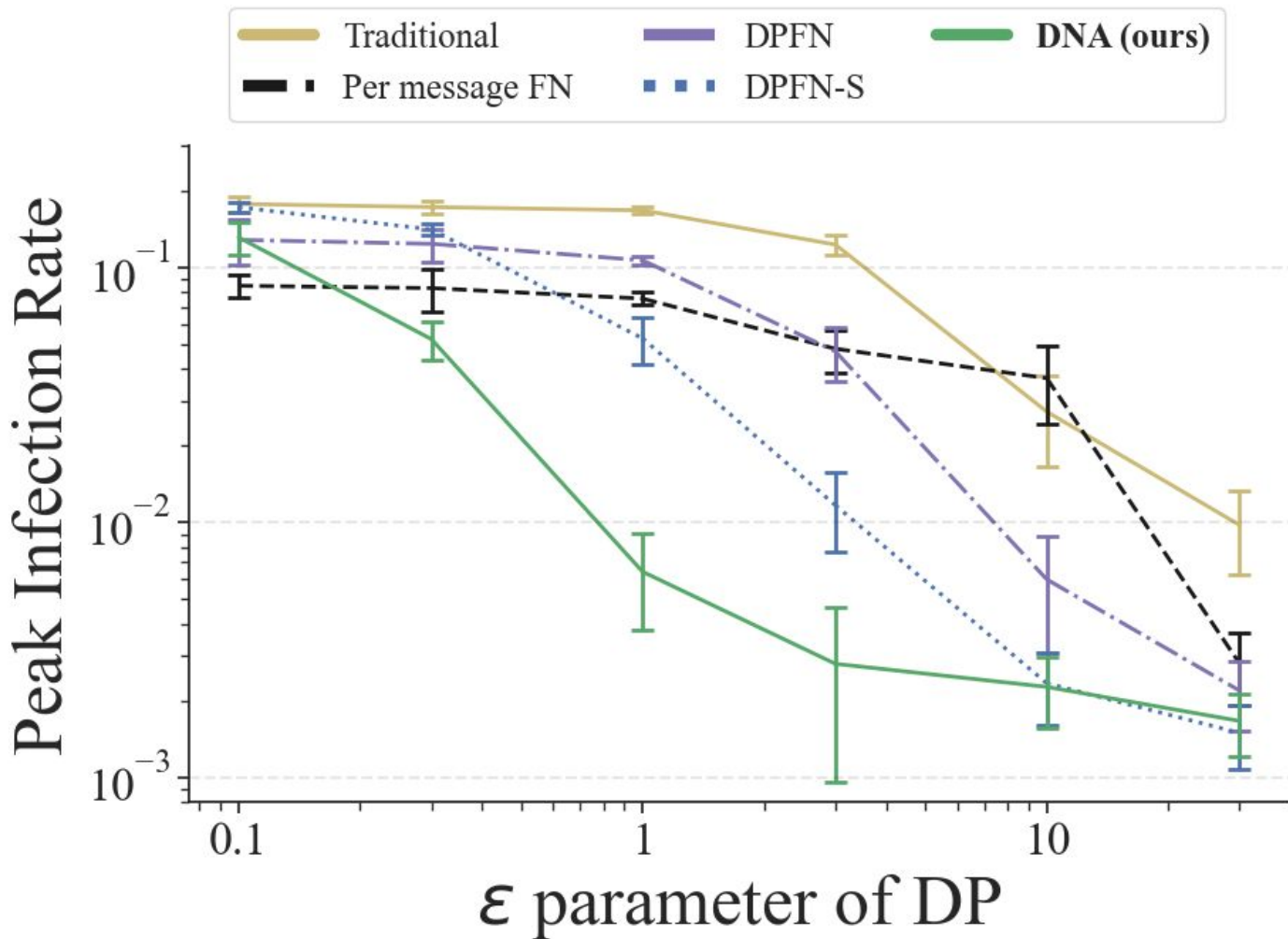
Simulator for experiments

Need simulator as better predictions interact with agents

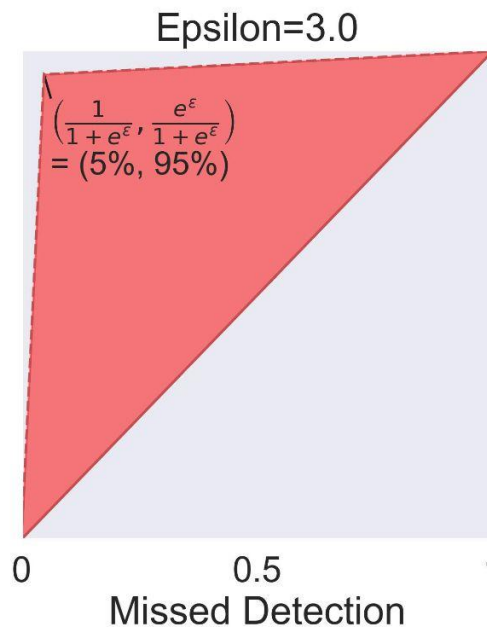
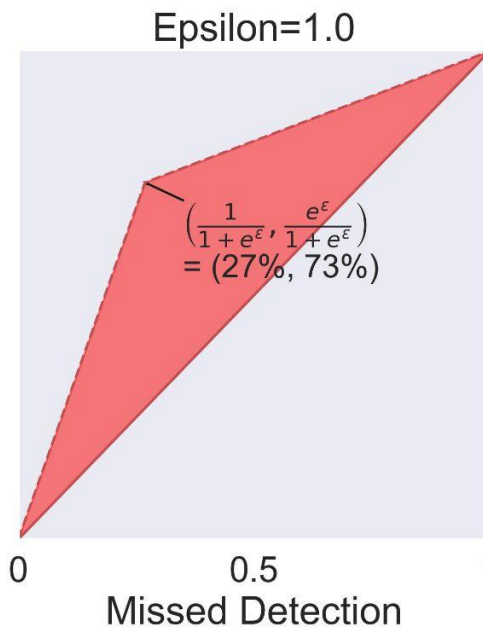
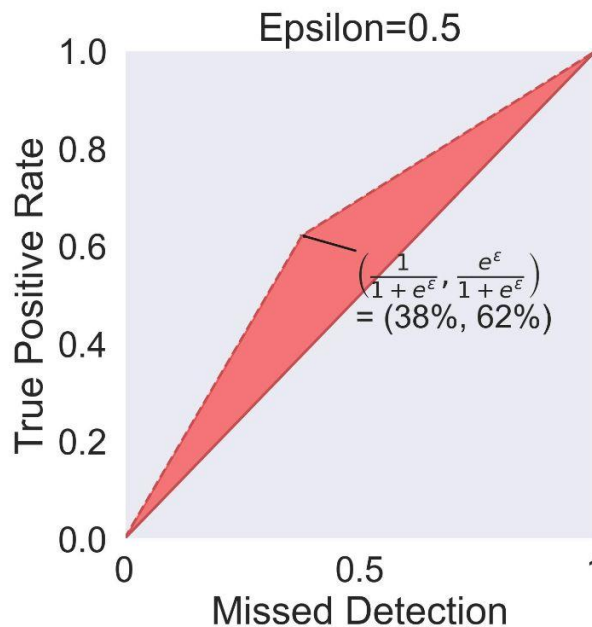
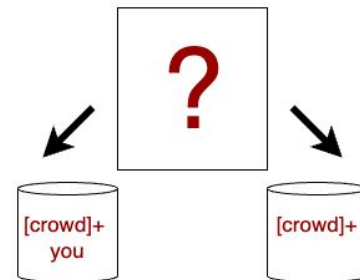
OpenABM (Hinch et al. 2021)

- Stratifying for
 - 9 age categories
 - 3 occupations
 - 6 household types
- In total 150 parameters calibrated against a typical city in the UK

Experimental results



What does DP mean?



DNA has better utility under various noise scenarios

Even when up to 50% of the agents don't follow the protocol, or when the tests become more noisy, the DNA method **achieves lower infection rate**, compared to the same method without neural augmentation

Units are number of infections per thousand agents, \pm standard deviation

FPR/FNR = False Positive/Negative Rate

	DPFN-S (‰)	DNA (‰)
<i>Follow protocol</i>		
100%	52.7 ± 10.9	6.4 ± 2.6
80%	60.4 ± 9.6	6.4 ± 2.2
50%	100.1 ± 4.4	27.2 ± 8.6
<i>Noisy tests</i>		
FPR 1%, FNR .1%	52.7 ± 10.9	6.4 ± 2.6
FPR 10%, FNR 1%	81.3 ± 2.6	19.5 ± 2.5
FPR 25%, FNR 3%	130.4 ± 1.5	81.3 ± 1.8

Conclusion

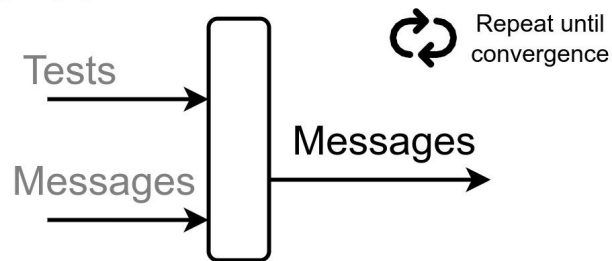
- Novel view of Lipschitz Neural Augmentation as providing Differential Privacy w.r.t. input
- Neural augmentation increases sensitivity, but compares favourably with better predictions
- Future work:
 - Decentralized reinforcement learning, partial adoption

DNA: DP Neural Augmentation for Contact Tracing

Questions

r.romijnders@uva.nl; romijndersrob@gmail.com
github.com/robromijnders/dna

Inference



Predict

