IAIK TU Graz

KNOW Center

TU Graz
SCIENCE
PASSION
TECHNOLOGY

Privately Connecting Mobility to Infectious Diseases via Applied Cryptography

Alexandros Bampoulidis[4] Alessandro Bruni[3] Lukas Helminger[1,2] Daniel Kales[1] Christian Rechberger[1] Roman Walch[1,2]

[1]TU Graz, [2]Know-Center, [3]KU Leuven, [4]RSA FG

What It Is, and What It Is Not

	Contact Tracing Apps	Our Approach
Feature phones	✗	✓
Data available	✗/✓	✓
Contact tracing	✓	✗

Human mobility is a critical factor in infectious disease

- Increased contacts between susceptible and infected individuals.
- Introduction of pathogens into new geographical regions.

understanding human mobility
↓
understanding dynamic of pandemic

Connecting mobile phone data to infectious diseases

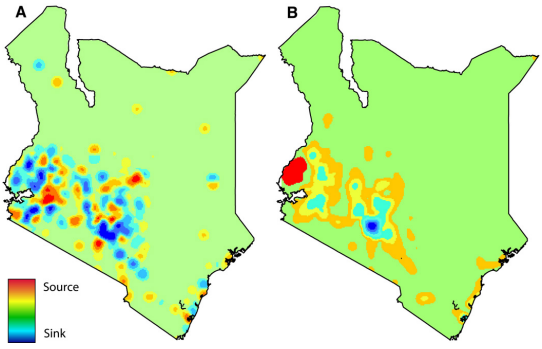


Fig.: Quantifying the Impact of Human Mobility on Malaria [WET$^+$12], **Science Magazine 2012**

Go one step further

So far:

- Aggregated mobility data of all subscribers
  - ⇝ issues when relatively few cases or mass-gatherings.

Our proposition:

- Aggregated mobility data of infected individuals
  - ⇝ likely more accurate epidemiological models, BUT

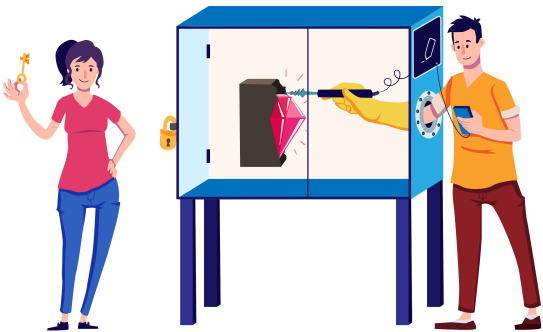
Why was this not done so far?

Privacy?!

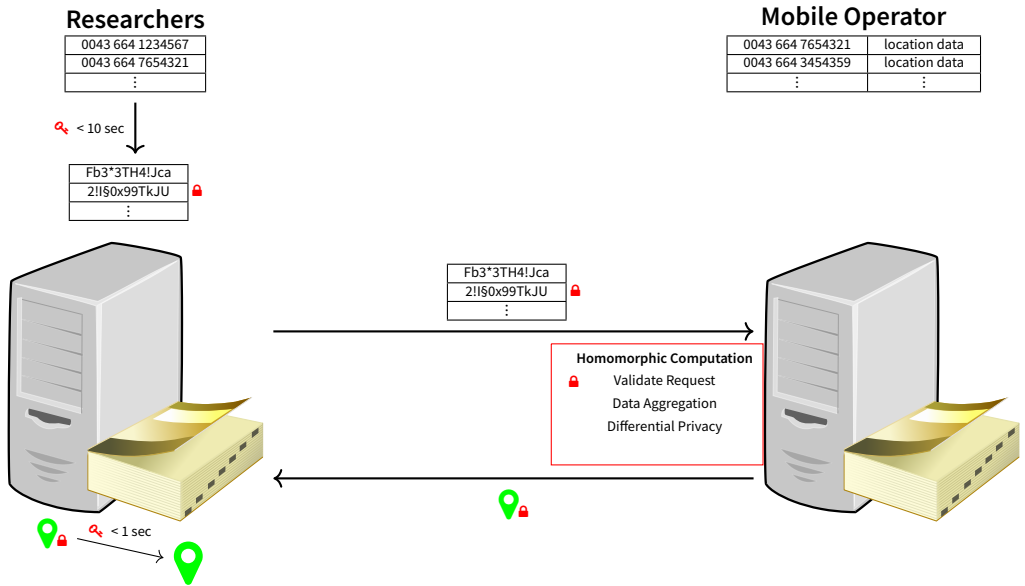
Two options:

- Sending mobile operator patients' identifiers
- Researchers get access to non-anonymized data records

Solution: Cryptography



- Homomorphic encryption protects patients' identifiers
- Zero-knowledge proof techniques ensure minimum cardinality of identifiers' set.
- Differential privacy protects highly sensitive output.


Researchers
0043 664 1234567
0043 664 7654321
< 10 sec
Fb3*3TH4!Jca
2!I§0x99TkJU
Mobile Operator
0043 664 7654321
location data
0043 664 3454359
location data
Fb3*3TH4!Jca
2!I§0x99TkJU
Homomorphic Computation
Validate Request
Data Aggregation
Differential Privacy
< 1 sec

Data Aggregation

$$\begin{matrix} id_1 & id_2 & id_3 \end{matrix}\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \times \begin{matrix} ct_1 & ct_2 & ct_3 \end{matrix}\begin{pmatrix} 2 & 0 & 3 \\ 3 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix}\begin{matrix} id_1 \\ id_2 \\ id_3 \end{matrix} = \begin{matrix} ct_1 & ct_2 & ct_3 \end{matrix}\begin{pmatrix} 3 & 4 & 6 \end{pmatrix}$$

Matrix-vector multiplication: Baby-Step Giant-Step algorithm

Validation of Request

$$\begin{pmatrix} 3 & 4 & 6 \end{pmatrix} + mask, \quad \text{where} \quad mask = \begin{cases} 0 & \text{if honest} \\ \text{random} & \text{else} \end{cases}$$

$$\begin{aligned} mask_{\texttt{bin}} &\leftarrow \langle \boldsymbol{c}, \boldsymbol{c} - \mathbf{1} \rangle \\ mask_{\texttt{HW}} &\leftarrow \langle \boldsymbol{c}, \mathbf{1} \rangle - w \\ mask &\leftarrow \mu_{\texttt{bin}} + \mu_{\texttt{HW}} \end{aligned}$$

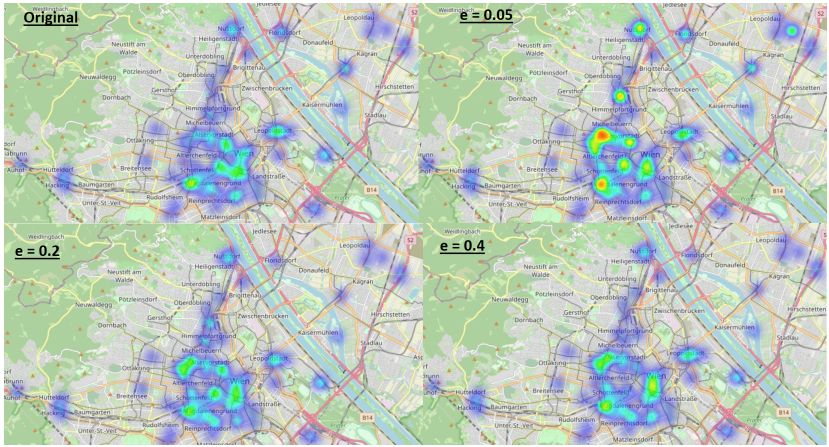
Adding Noise (Differential Privacy)

$$\begin{matrix} ct_1 & ct_2 & ct_3 \\ (\ 3 & 4 & 6\ ) \end{matrix} + \begin{matrix} \text{Noise} \\ (\ -1 \quad 0 \quad 1) \end{matrix} = \begin{matrix} ct_1 & ct_2 & ct_3 \\ (\ 2 & 4 & 7\ ) \end{matrix}$$

Producing noise: Laplace distribution with privacy parameter ϵ

Larger $\epsilon \rightsquigarrow$ less noise $\rightsquigarrow$ less privacy

Differential Privacy Experiments



Legal Analysis

- Patients' ids:

$$\text{Encryption} \rightsquigarrow \text{Anonymization}$$

(when decryption key is not given away)

$$\Rightarrow \text{not personal data (GDPR)}$$

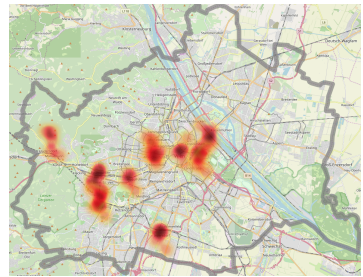
- Mobility data:

$$\text{DP and orthogonal technical measures}$$

$$\rightsquigarrow \text{risk of de-identification highly unlikely}$$

Is this feasible/affordable in practice for whole countries?

$< 2h \triangleq 10\$$ (e.g. Austria, Singapore, NY City)



- Optimized C++ implementation using SEAL
- 96 Threads
- 1GiB data

Security

Homomorphic encryption $\Rightarrow$ semi-honest security.

Is semi-honest security enough for medical records and location data?

NO

- Medical records: Private against malicious adversaries.
- Location data: DP protection against malicious researchers.

Our Message

Even in times of crisis where it is tempting to (temporarily) lower data protection standards for purposes of big data analytics, there are technical methods to keep data protection standards high. And those technical methods are practical and available.

https://covid-heatmap.iaik.tugraz.at/en/
https://eprint.iacr.org/2020/522

References I

[WET+12] Amy Wesolowski, Nathan Eagle, Andrew J Tatem, David L Smith, Abdisalan M Noor, Robert W Snow, and Caroline O Buckee.

Quantifying the impact of human mobility on malaria.

Science, 338(6104):267–270, 2012.