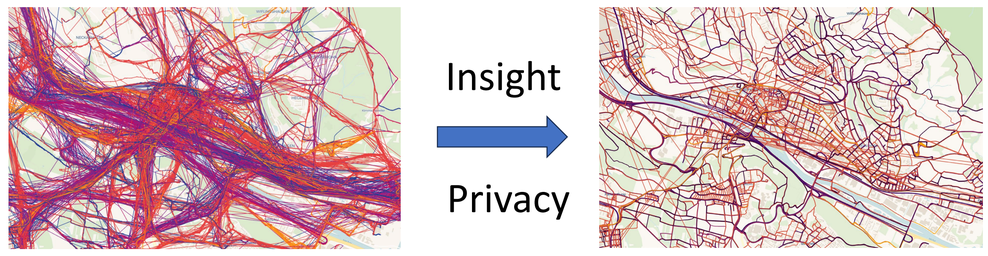
AnoMoB

(Anonymisierte Erfassung und Nutzung von **Mo**bilitäts- und **B**ewegungsdaten)

Enhancing Local Differential Privacy of Trajectories Using Homomorphic Encryption

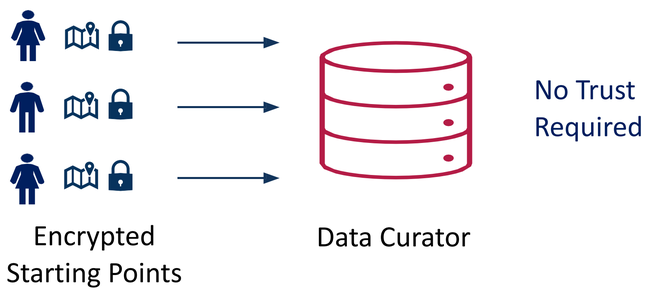
Di Hu, Clemens Krüger, Gabriele Gühring, Dominik Schoop (Hochschule Esslingen)

Goal:
Insights from mobility data without compromising privacy



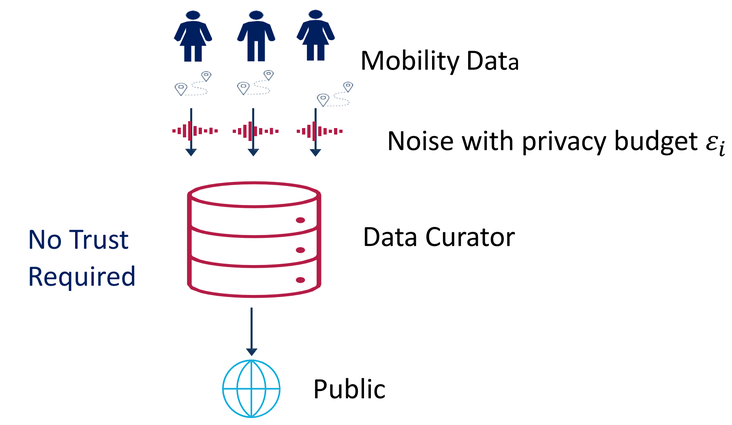
Data collection

- Clients encrypt the starting points of their trajectories locally using fully homomorphic encryption (CKKS scheme [3])
- Data curator collects all encrypted starting points as well as a tessellation of regions (e.g. city districts)



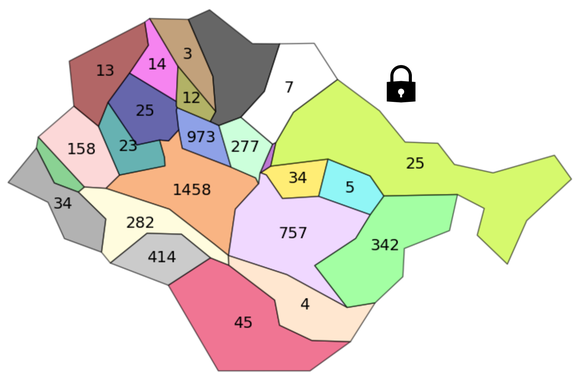
Data collection

- Clients send features of their trajectories
- Every feature i is send with a privacy budget ε_i



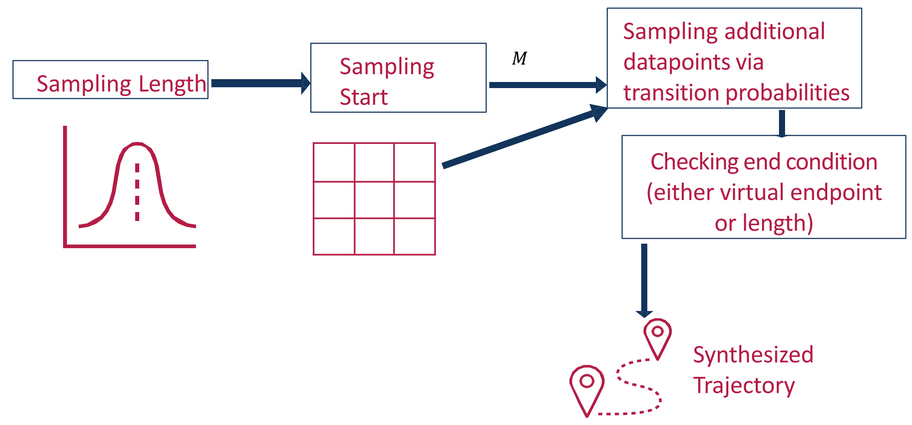
Encrypted processing

- Data curator executes an encrypted point-in-polygon algorithm to determine the number of starting points in each region
- **Input privacy**: Data curator cannot read any starting points



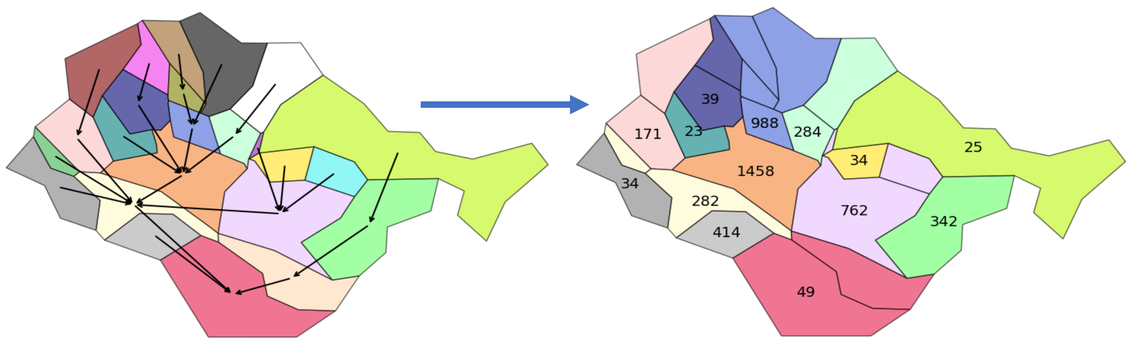
Sampling from different distributions

- I. e. length, transition matrix, mode, …
- Synthesized trajectories are created [1]



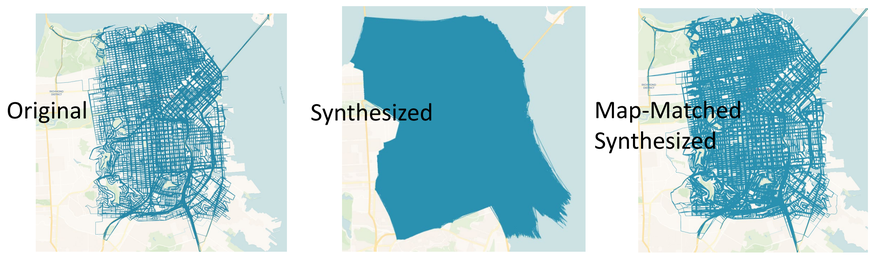
Privacy

- In sparsely populated areas some individuals could possibly be re-identified → needs to be resolved before decryption
- Challenge: Algorithm needs to be static, because encrypted data cannot influence program flow → Aggregate regions with too few data points according to a static, hierarchical path

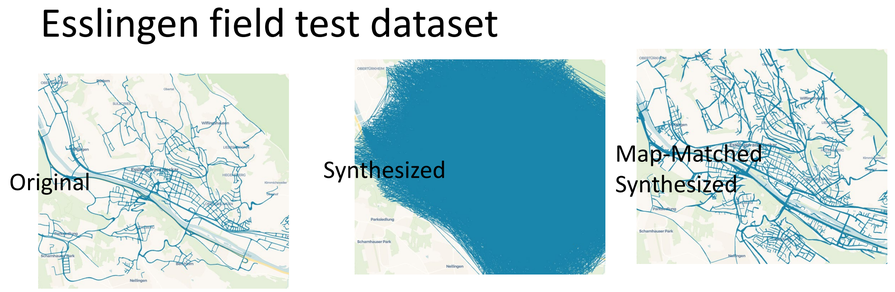


Synthesized trajectories and privacy

- San Francisco Cab Spotting Dataset [2]



- Esslingen field test dataset



- Stuttgart E-Scooter, Rome Taxi data, ….

Kontaktdaten

- Prof. Dr. Dominik Schoop
- +49 711 397-4467
- Dominik.Schoop@hs-esslingen.de

Quellenangaben

[1] Du, Yuntao, Yujia Hu, Zhikun Zhang, Ziquan Fang, Lu Chen, Baihua Zheng and Yunjun Gao: LDPTrace: Locally Differentially Private Trajectory Synthesis. 2023. PVLDB, 16(8): 1897 - 1909, 2023. https://doi.org/10.14778/3594512.3594520

[2] Hu, Di, Heinrich, Andreas, Gühring Gabriele (2025) A Toolchain for for Anonymized Data for Mobility Trajectory Optimization, 8th International Conference on Future Smart Cities (FSC), 15.-16. Oct 2025

[3] Cheon, Jung Hee, et al. "Homomorphic encryption for arithmetic of approximate numbers." International conference on the theory and application of cryptology and information security. Cham: Springer International Publishing, 2017.

Finanziert von der Europäischen Union NextGenerationEU

Gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt