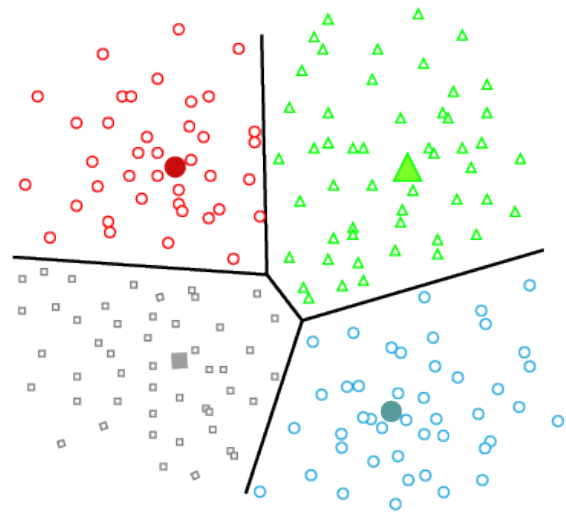


Bachelor's Thesis *or* Master's Thesis

# A Clustering Trajectory Protection Mechanism with Actual Privacy Guarantees

**Did you know that knowing just four location points is enough to identify 95% of the population?** While trajectory data is great for analysis, it contains very **sensitive information**. It can be used to learn where you've been and at what time, when you left home, and when you meet up with friends. So it's really important to make sure that the personal information in a trajectory database is protected.

To keep trajectory data safe, we can use a mechanism that satisfies **differential privacy** ( $\epsilon$ -DP), the go-to privacy notion. For example, we see proposals that claim to introduce a DP clustering mechanism for trajectories. However, **none of the DP trajectory clustering mechanisms proposed in the literature actually satisfy DP as they claim.**



**Thesis Task** In this thesis, you'll learn how to identify and fix the problems with existing clustering mechanisms, and you'll also be **the first to develop new clustering mechanisms that correctly satisfy DP**. You'll also be able to test your mechanisms on real-world data and scenarios.

**If you're interested in closing this gap in the field of trajectory protection and keeping your data safe, this thesis is for you.**

**Prerequisites** Primary interest in the topic. Coding skills in Python or similar languages, basic software development practices (e.g., Git), and English communication skills are required.

**If you are interested in this topic or have further questions, please contact Àlex Miranda-Pascual ([alex.pascual@kit.edu](mailto:alex.pascual@kit.edu)).**

25th June 2024