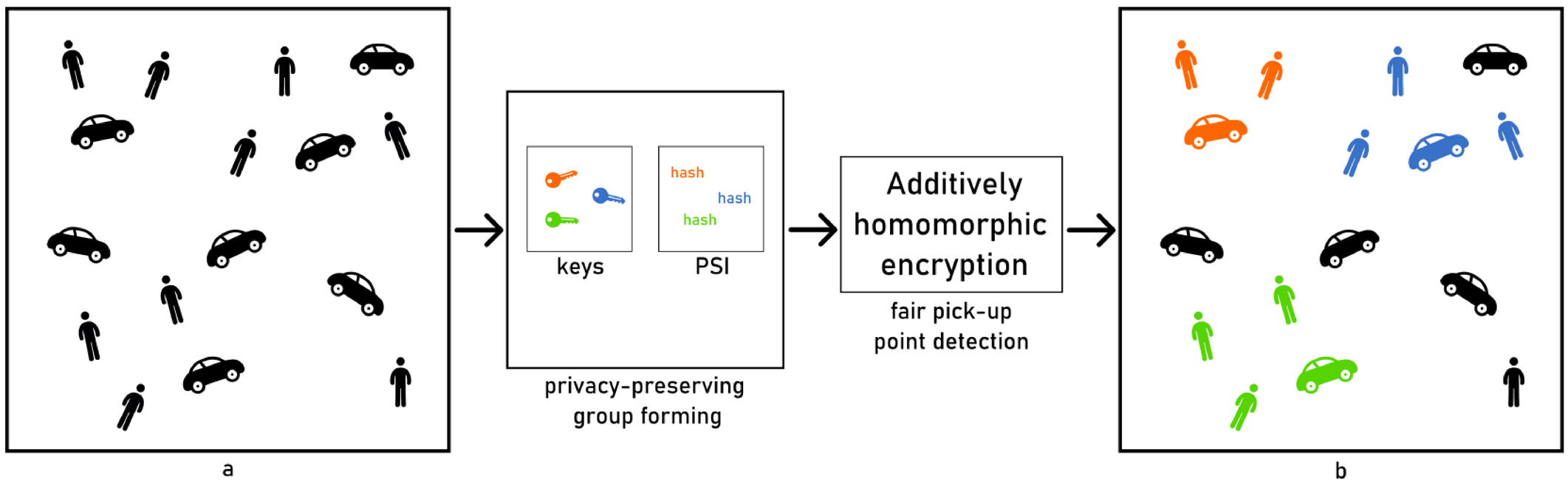
UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE

Sara Ramezanian
Gizem Akman
Mohamed Taoufiq Damir
Valtteri Niemi
Department of Computer Science, University of Helsinki
Helsinki Institute for Information Technology (HIIT)

Privacy-Preserving Ride-Sharing Protocols for Autonomous Cars



A summary of our protocol. Initially, the cars and passengers are not grouped (a). After applying our protocol, the cars are assigned to groups of passengers with similarity in their journeys (b).

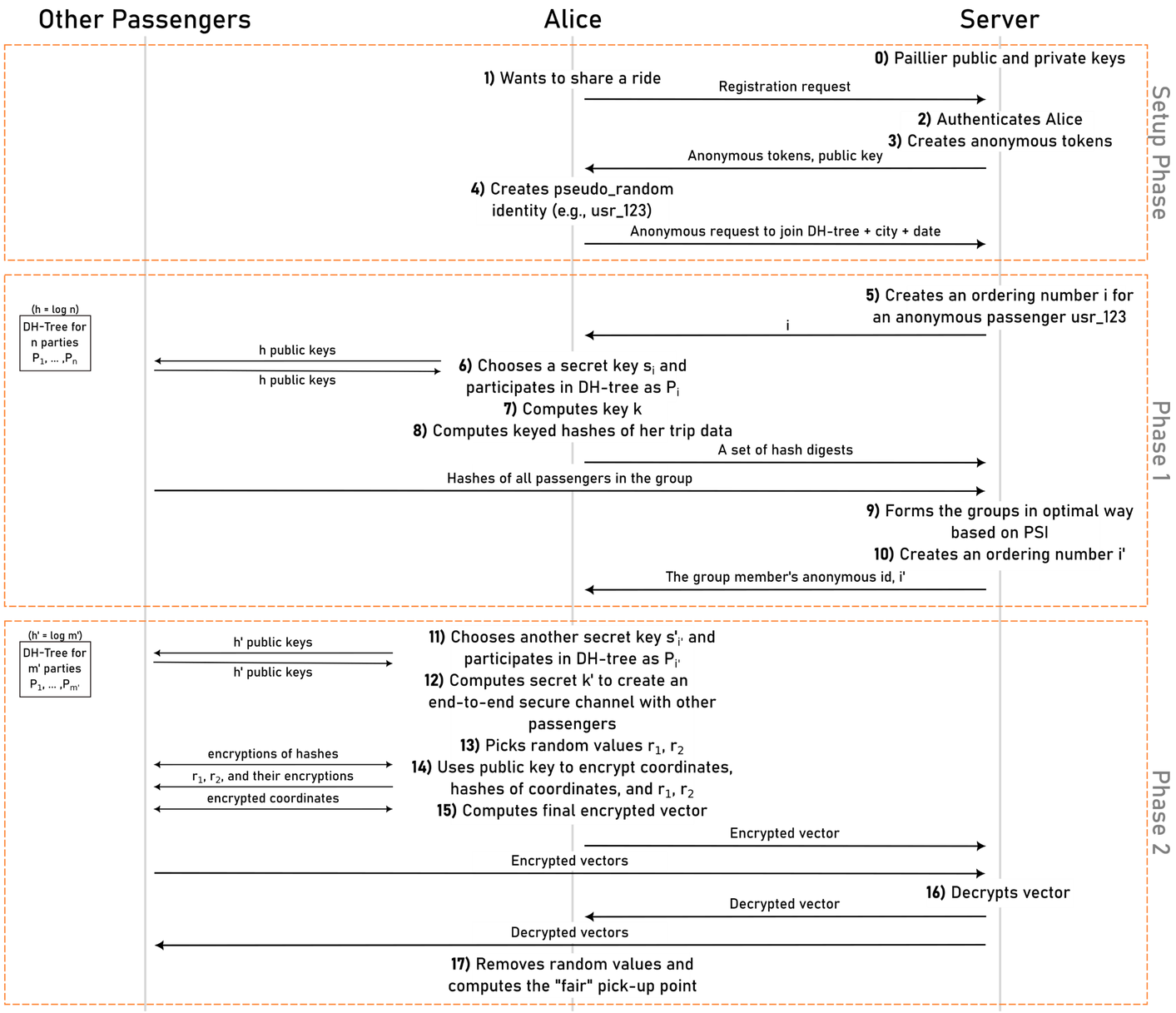
Fair Pick-up point

- A *fair pick-up point* is a location where its distance from all the passengers is fair.
- The pick-up point itself should be convenient, i.e., the point should be reachable easily by an autonomous car.

Protocol

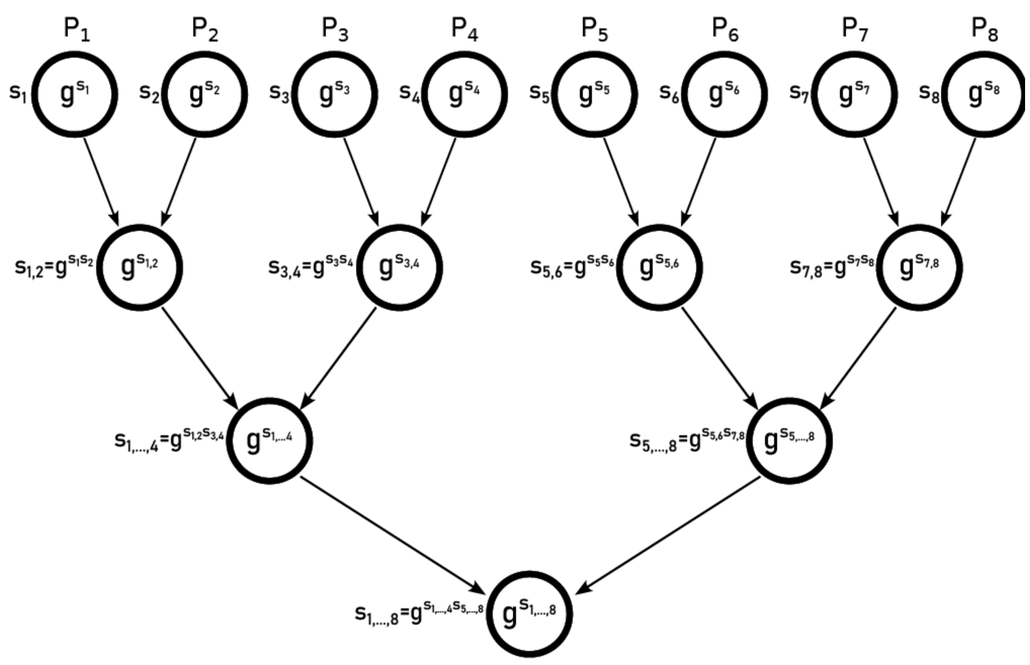
The protocol runs between the server of a company and the customers of that company and consists of three phases:

- Setup Phase
- Phase 1: The privacy-preserving group forming
  - Phase 1.a: Generating a Shared Secret Key
  - Phase 1.b: Private Set Intersection
- Phase 2: The privacy-preserving fair pick-up point selection



A Tree Diffie-Hellman Group Key Exchange

A modification to the DH-tree group key protocol that does not require a server.



Security and Privacy Analysis

- Our model is based on the assumption that the server of the ride-sharing company is honest-but-curious. We also consider both semi-honest and malicious passengers.
- In the setup phase, each passenger reveals the city and the date of their trip to the server while keeping their identity anonymous.
- The passengers do not reveal their identity either to each other or to the server.
- In Phase 1, the server groups the passengers without learning the passengers' exact or approximate locations or times of the planned trips. Moreover, the passengers do not learn any information about each other's journeys.
- Phase 2, the passengers can arrange a fair pick-up point without learning each other's exact or approximate locations and without revealing any information about their trip to the server.

This study is published in Proceedings of the 6th ACM Computer Science in Cars Symposium - CSCS 2022