Privacy-Preserving Determination of Fair Meeting Point

UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE

Gizem Akman
Valtteri Niemi
Mohamed Taoufiq Damir
University of Helsinki
Kuan Eeik Tan
Huawei Technologies Finland

Contributions

A novel privacy-preserving protocol for determining a fair meeting point for a group of n participants
(1) who want to gather at a meeting point that is fair and convenient
(2) without revealing their initial locations to each other or anyone else, and
(3) without revealing the meeting location to anyone other than the participants themselves.

Solution doesn't rely on Trusted Third Parties (TTPs), instead uses secure Multi-Party Computation (MPC).

PMP: Potential Meeting Point

Phase 1: Group Creation
- Create a group chat
- Share public keys
- Share transportation methods (walk,bike,car)

Phase 2: Weighted Centroid
Alice's perspective for $n = 3$ people:
- $(X_A, Y_A) = (X_{A1} + X_{A2} + X_{A3}, Y_{A1} + Y_{A2} + Y_{A3})$
- Send $\mathrm{E}_{\mathrm{pk_B}}(\mathrm{X}_{A2}, Y_{A2})$ to Bob and $\mathrm{E}_{\mathrm{pk}_C}(\mathrm{X}_{A3}, Y_{A3})$ to Charlie
- Compute $(X'_A, Y'_A) = (w_A X_{A1} + w_B X_{B1} + w_C X_{C1}, w_A Y_{A1} + w_B Y_{B1} + w_C Y_{C1})$ and send to others
- Compute $(X_{Centroid}, Y_{Centroid}) = (X'_A + X'_B + X'_C, Y'_A + Y'_B + Y'_C)/(w_A + w_B + w_C)$

Phase 3: Circle around centroid
Draw a circle around the centroid whose size depends on slowest participant.

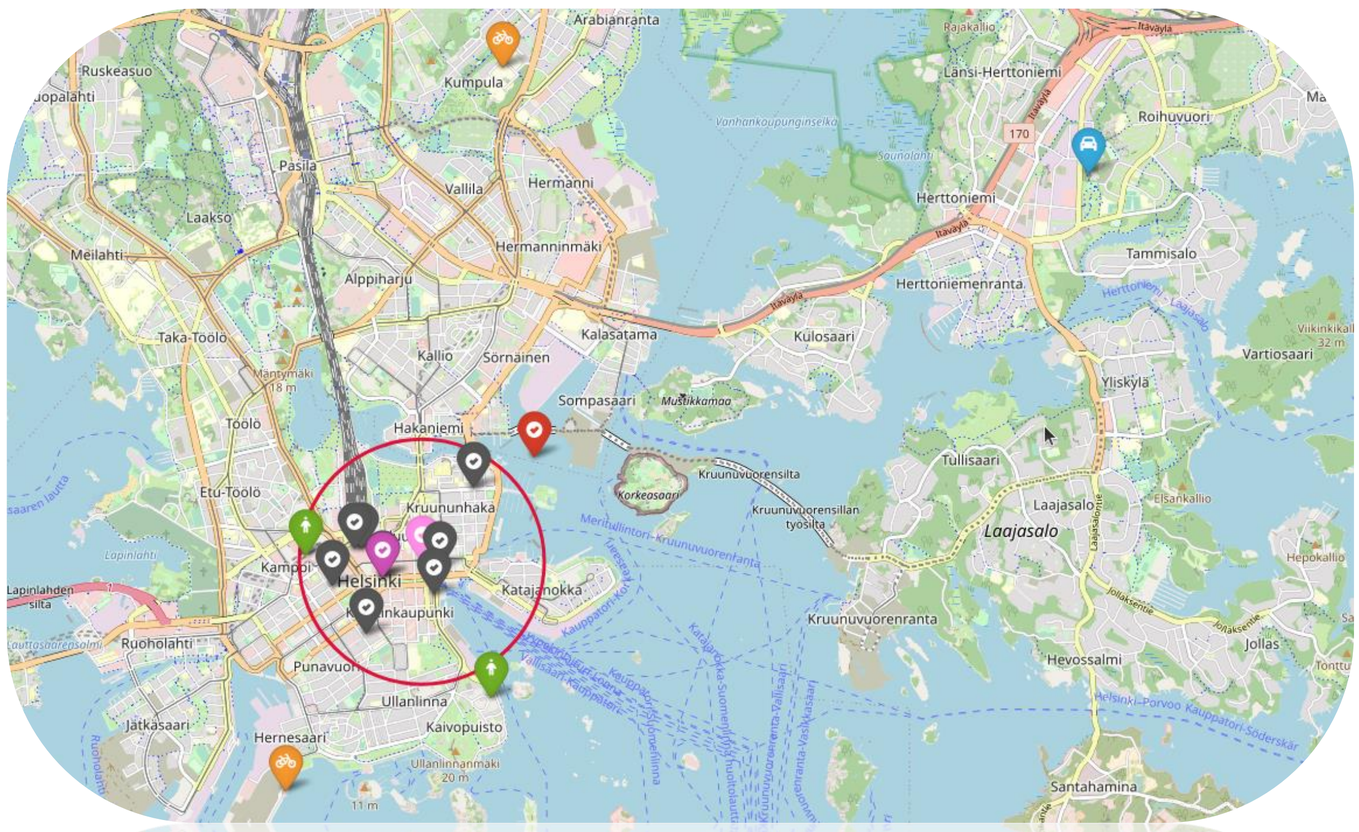
Phase 4: Choosing PMPs
Each participant suggests a few PMPs that reside inside the circle.

Phase 5: Navigating to PMPs
Each participant computes network distance and travel time to each PMP.

Phase 6: Ranking PMPs
Each participant ranks each PMP 1 to t; t is highest rank and 1 is lowest.

Phase 7: Sum of Votes
Participants compute the sum of votes with MPC similarly as in Phase 2.

Phase 8: ETM Determination
Participants run privacy-preserving Dutch auction:
- Descending series of potential ETMs.
- Participant rejects the ETM if ETM<ETA.



This work was presented in the Privacy Symposium 2026, Venice, Italy.

Security Analysis

- Communication is protected from the outsiders after forming secure group chat.
- **Location privacy** is provided due to additive secret sharing, unless there are $n - 1$ dishonest participants.
- **Meeting point privacy** is provided because it is decided at the end of the protocol and revealed only to the participants.
- **ETM secrecy** is provided due to the use of privacy-preserving Dutch auction.
- **Unlinkability** is provided because the integrity and confidentiality of the exchanged data is protected with secure group chat.
- **Preference privacy** is provided because MPC is used for computing the sum of votes.

Dynamic Setup

- A protocol extension to provide
  - updating ETM, e.g., due to traffic, on the way to the meeting
  - updating meeting location when meeting is later than the protocol run
    - due to new member joining or old member leaving
    - existing members change initial locations

Performance Analysis

- Communication cost for n participant: $2n^2 + 3n + 3$ exchanged messages.
- Choice of cryptosystems:
  - Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM-512)
  - Elliptic Curve Integrated Encryption Scheme (ECIES) - P-256 curve
- Communication cost per participant:
  - ML-KEM-512
    - $n = 3 \Rightarrow 4\ KB$
    - $n = 10 \Rightarrow 11\ KB$
  - ECIES P-256 has significantly less cost.