ORide: A Privacy-Preserving yet Accountable Ride-Hailing Service

Context
• Ride-hailing services (RHSs) are used by millions of users in hundreds of cities due to their convenience and safety features.

Privacy problems:
• RHS providers know the exact rides of the riders and drivers, hence being able to infer sensitive information about their activities, e.g., one-night stands.

Our contributions:
• We propose ORide (Oblivious Ride), a privacy-preserving RHS based on somewhat homomorphic encryption (SHE) with optimizations such as ciphertext packing and transformed processing.
• ORide supports the matching of riders and drivers without learning their identities or location information.
• ORide supports key RHSs features such as easy payment, reputation scores, accountability, and retrieval of lost items.

Our solution: ORide

Naïve ride-matching

Optimized ride-matching

• Problems:
  − The SP separately computes the ciphertext distances between the rider and d drivers \( \rightarrow \) computational cost.
  − The SP sends \( d \) ciphertext distances to the rider \( \rightarrow \) bandwidth cost due to huge ciphertext expansion of SHE.

Optimized ride-matching

• Ciphertext packing:

  Pack \( d \) ciphertexts in a single ciphertext by taking advantage of SHE polynomial structure.
  − Each encrypted operation affects all the coefficients in parallel.
  − NTT transformation is applied s.t. products in the encrypted domain are translated into coefficient-wise products in the plaintext domain.

ORide Evaluation

• Datasets: Taxi GPS traces in NYC
• Evaluation criteria:
  – Per-ride computational and bandwidth overhead in three scenarios:
    + S1: Naïve approach
    + S2: Optimized approach and honest drivers.
    + S3: Optimized approach and malicious drivers.
  – Riders’ anonymity and drivers’ bandwidth requirements:
    + Anonymity set of 26,000 and drivers are only required to have a data-connection speed of less than 2 Mbps.
  – Effect on ride matching:
    + The extra driving distance for a driver is less than 0.5 km in more than 75% of the cases evaluated.
• Conclusions
  − ORide enables the SP to choose a balanced trade-off between riders’ anonymity vs. bandwidth requirements for the drivers.
  − It preserves the convenience and accountability features of the current RHSs.

Information observed by the SP during ride set-up procedure w.r.t. different RHS designs