

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

Anh Pham[1], Italo Dacosta[1], Guillaume Endignoux[1], Juan Ramón Troncoso-Pastoriza[1], Kévin Huguenin[2], and Jean-Pierre Hubaux[1]

[1]EPFL, [2]UNIL

Ride-Hailing Services (RHSs)

- Millions of users, billions of rides, hundreds of cities











Privacy Problems

For riders

Lyft Sued For Violating California Privacy Law

by **Wendy Davis @wendyndavis**, February 12, 2014

News › Business › Business News

Uber employees used app to 'spy on ex-lovers, politicians and celebrities'

Thousands of staff have access to 'God View' mode which can be used to track customers' movements, former security executive alleges

Ben Chapman | Tuesday 13 December 2016 17:15 GMT | 0 comments

NEWS

US Senator Al Franken scrutinizes Lyft's privacy policies

By John Ribeiro

Bangalore Correspondent, IDG News Service | DEC 3, 2014 12:05 AM PT

For drivers

TECH & SCIENCE

UBER DRIVERS HAVE PRIVACY PROBLEMS TOO

BY POLLY MOSENDZ ON 11/19/14 AT 5:12 PM

APPS | TECH | UBER

Uber is tracking its drivers in China, will fire anyone attending taxi protests

27

by Dante D'Orazio | Jun 14, 2015, 10:41am EDT

Uber's 'Hell' program tracked and targeted Lyft drivers

The top-secret program apparently ran for two years.



Mariella Moon, @mariella_moon
04.13.17 in Transportation

41 Comments

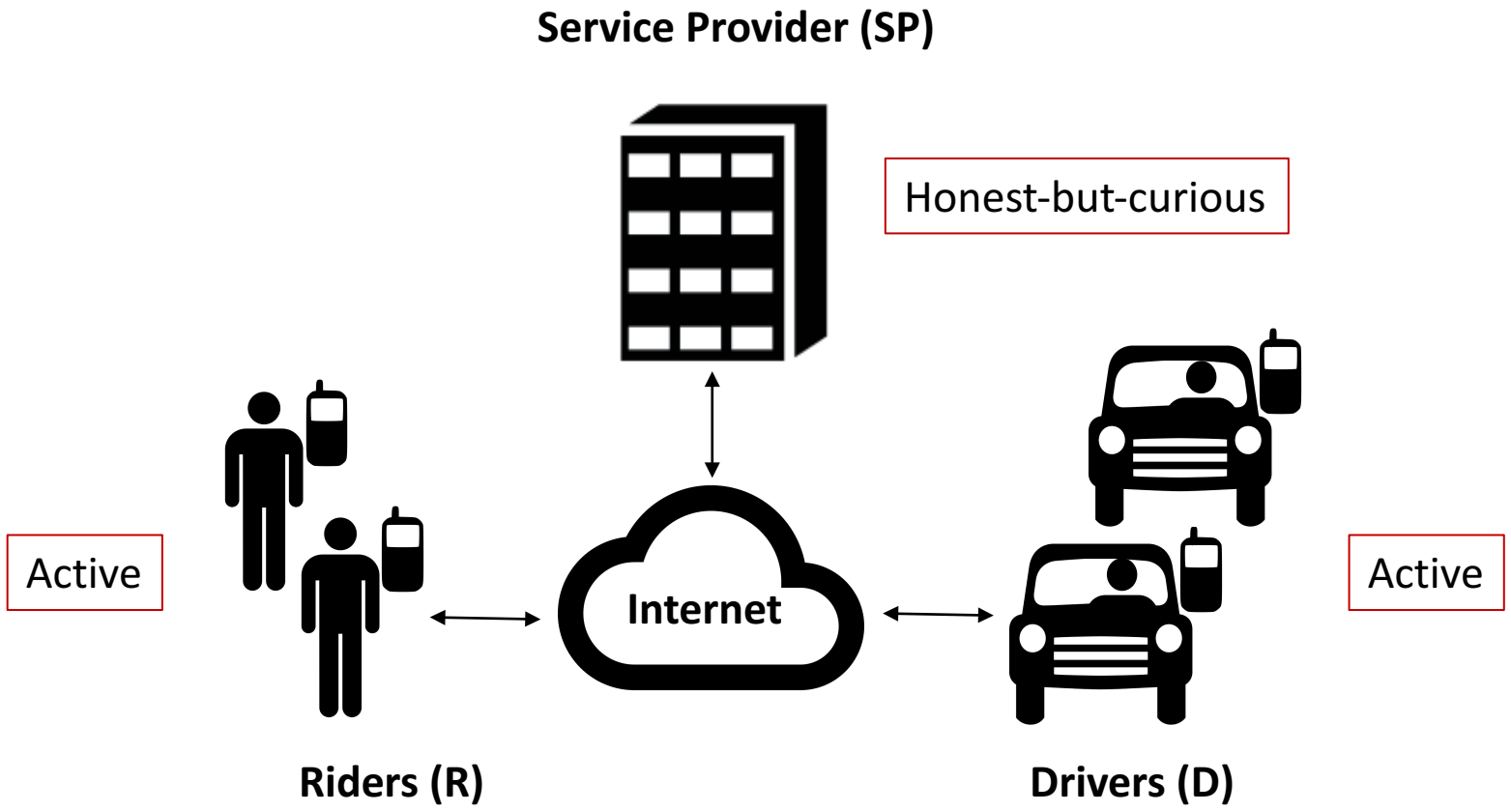
2936 Shares

ORide: Goals

- Privacy for riders and drivers
- Usability and accountability



Adversarial Assumptions

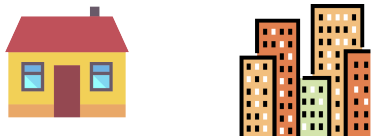


Attacks Considered

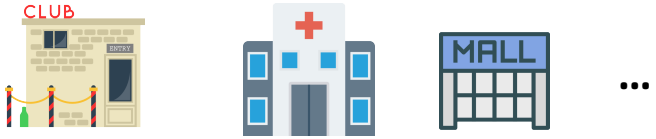
- Riders and drivers might assault each other



- SP might perform large-scale privacy-sensitive inferences



Home/work addresses



Sensitive activities

- SP might perform targeted attacks



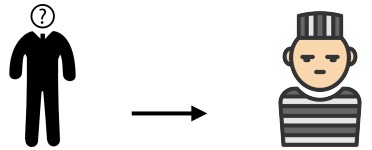
Pick-up loc. and time



Drop-off loc.

Desired Usability and Accountability Features

- Riders and drivers are accountable for their behaviors
  - The SP can identify misbehaving users
  - Even in extreme cases: e.g., kidnapping



- Usability:
  - Easy payment
  - Reputation ratings for riders and drivers
  - Retrieval of lost items



ORide Overview

Notations:
ACs: Anonymous credentials
cert: Digital certificate

Rider (anonymous)

cert_R
ACs



SP



Drivers (anonymous)



cert_D
ACs

Ride set-up

Oblivious ride matching

Accountability mechanisms

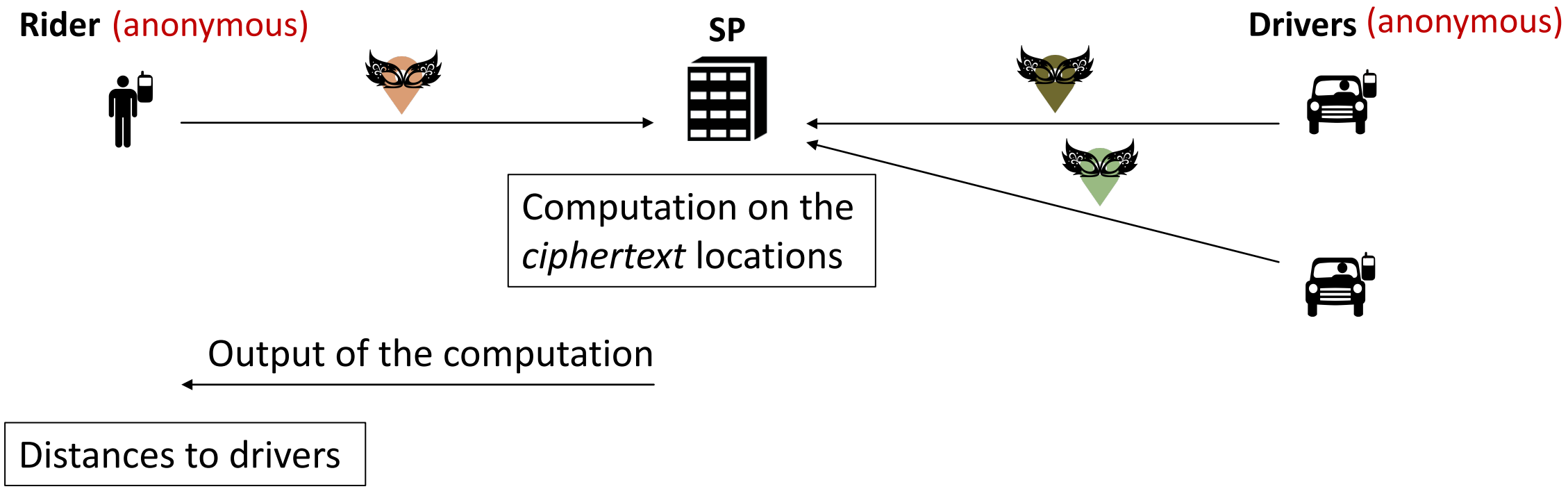
Ride termination

Payment

Reputation rating

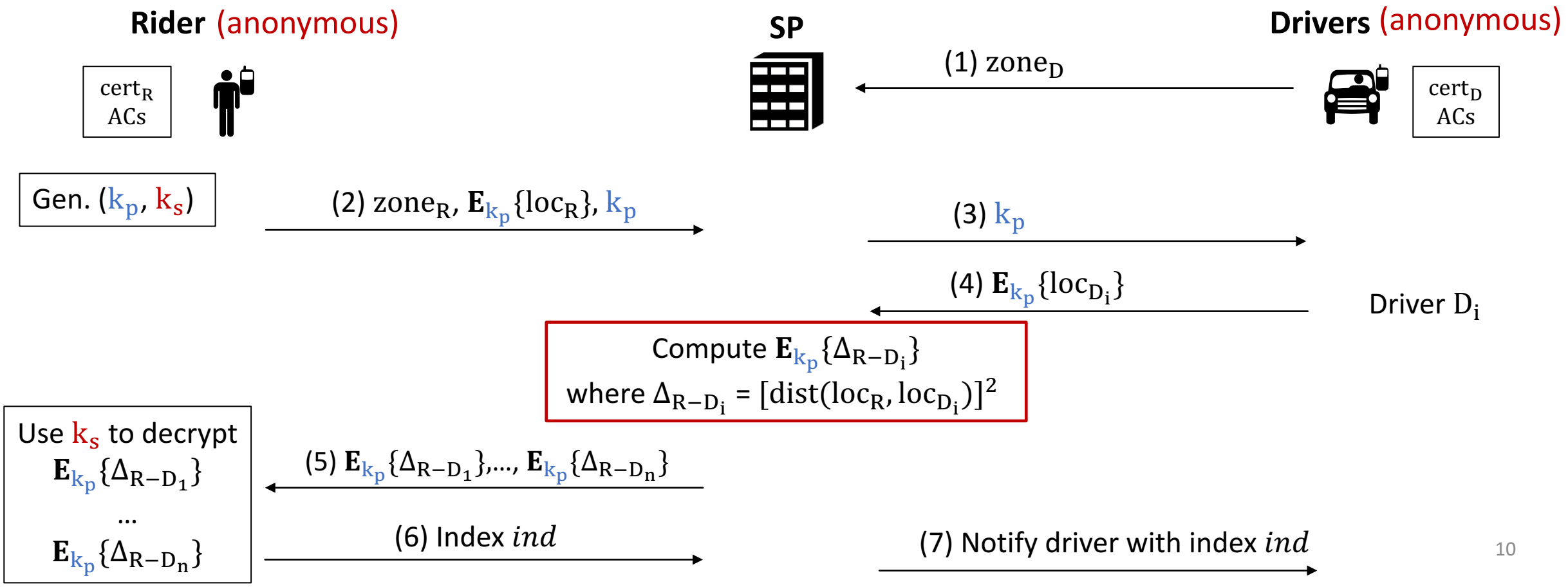
Oblivious Ride Matching - Intuition

- **Goal:** Rider can select the closest driver without revealing their locations to the SP



Oblivious Ride Matching

- **Goal:** Rider can select the closest driver without revealing their locations to the SP



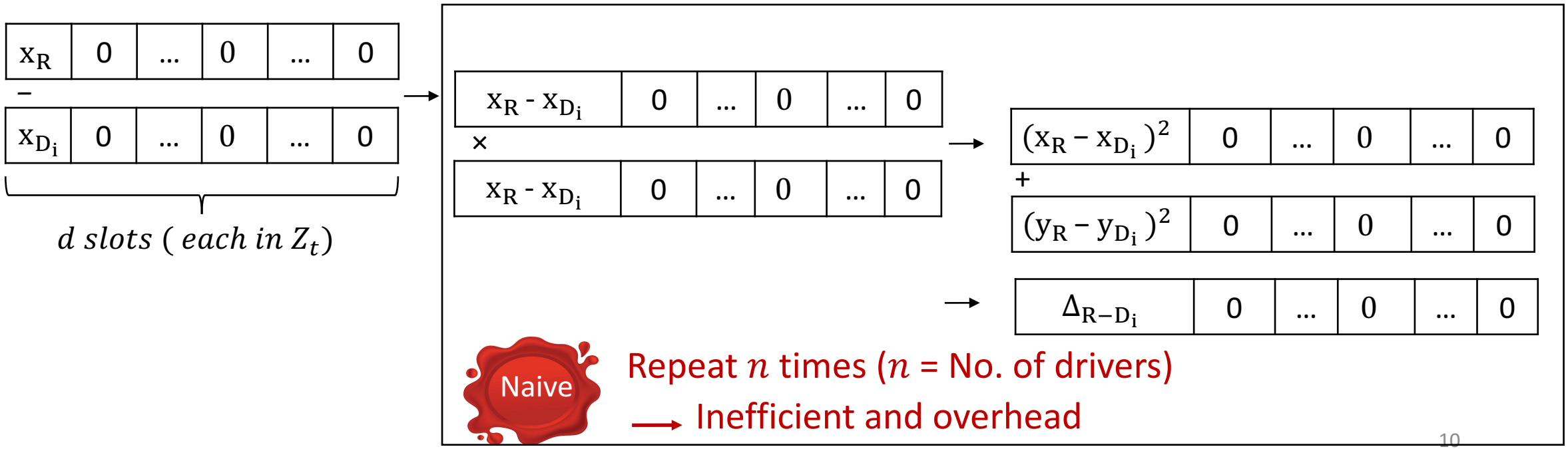
SP Computes $\mathbf{E}_{k_p}\{\Delta_{R-D_i}\}$

with $\Delta_{R-D_i} = [\text{dist}(loc_R, loc_{D_i})]^2 = (x_R - x_{D_i})^2 + (y_R - y_{D_i})^2$

- Use Somewhat-Homomorphic Encryption (SHE) scheme by Fan and Vercauteren

$$\begin{cases} R_t = Z_t[X]/(X^d + 1) & \text{Plaintexts} \\ R_q = Z_q[X]/(X^d + 1) & \text{Ciphertexts and keys} \end{cases}$$

- How?



SP Computes $\mathbf{E}_{k_p}\{\Delta_{R-D_i}\}$

with $\Delta_{R-D_i} = [\text{dist}(loc_R, loc_{D_i})]^2 = (x_R - x_{D_i})^2 + (y_R - y_{D_i})^2$

- **Optimization Goal:** 1 computation/request for R and SP

Naïve

Δ_{R-D_0}	0	…	0	…	0
⋮					
Δ_{R-D_i}	0	…	0	…	0
⋮					
$\Delta_{R-D_{n-1}}$	0	…	0	…	0

Optimized

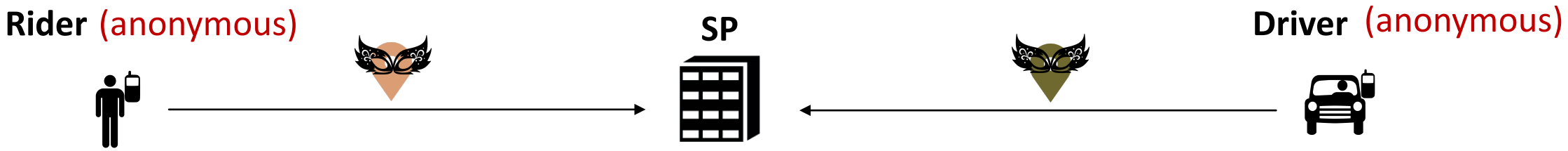
Δ_{R-D_0}	…	Δ_{R-D_i}	…	$\Delta_{R-D_{n-1}}$	0	…	0

Coefficient i contains $[\text{dist}(loc_R, loc_{D_i})]^2$

- How?
  - Ciphertext packing: to pack drivers' ciphertexts into 1 ciphertext
  - Number-Theoretic Transform (NTT): to support coefficient-wise multiplication

Oblivious Ride Matching ☑

- Rider R selected driver D without revealing their locations to the SP



- How R and D share their locations w/ each other?
- Accountability?
  - R and D might assault each other
  - R might not want to pay for the ride
  - Dispute on the fare





Accountability Mechanisms



Secure channel
Proximity channel

- **Goal:** Rider and driver are accountable for their behaviors

Rider (anonymous)

cert_R
ACs



SP



Keep locally or share with trusted peers

Driver (anonymous)



cert_D
ACs

(8) Secure channel: exchange rep_R, rep_D, loc_R, loc_D, cert_R and cert_D, gen. a PIN

(9) loc_D in real time

(10) Proximity check & validation of secure channel



In proximity of loc_R

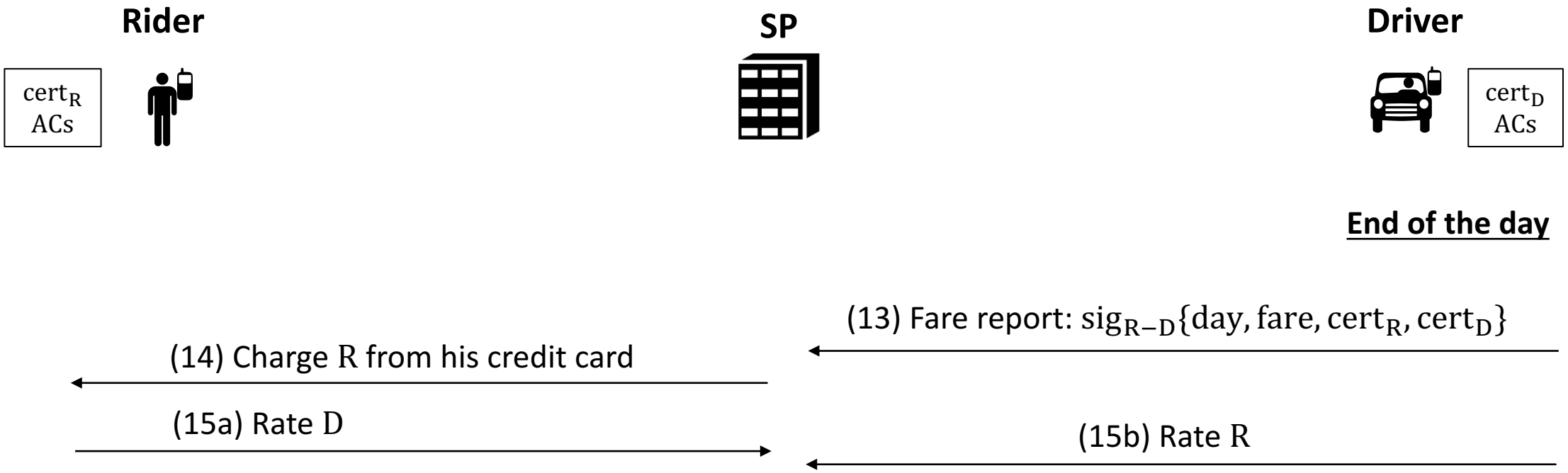
(11) Driver's info: plate number and profile photo

(12) Fare report: $\text{sig}_{\text{R}-\text{D}}\{\text{day}, \text{fare}, \text{cert}_\text{R}, \text{cert}_\text{D}\}$

The ride begins

Payment and Reputation Rating ✅

- **Goal:** The two operations do not break the anonymity of the ride



Protocol Analysis

- Information observed by the SP

Ride DB

Zone of the pick-up	**Obfuscated** pick-up time

Payment DB

Rider's ID	Driver's ID	Fare	Day of the ride

- Targeted attacks by the SP



Pick-up loc. and time of a specific rider



Drop-off location

Drop-off locations and times are never reported to the SP

Protocol Analysis

- Information observed by the SP

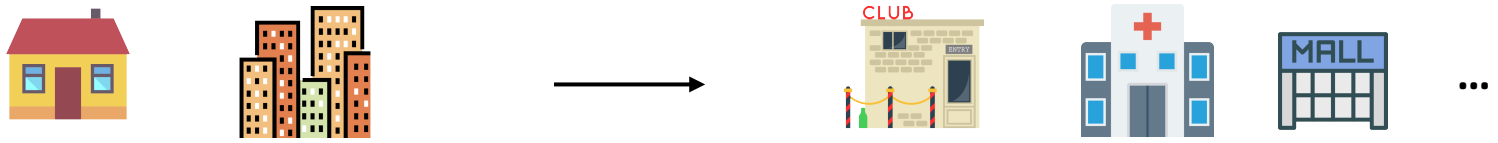
Ride DB

Zone of the pick-up	**Obfuscated** pick-up time

Payment DB

Rider's ID	Driver's ID	Fare	Day of the ride

- Large-scale inferences by the SP

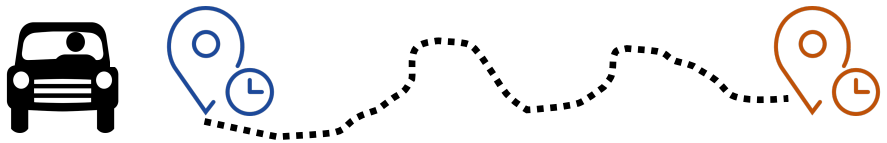


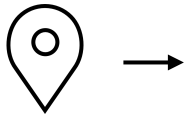
Home/work addresses → Sensitive activities

Lower-bound anonymity set = No. of rides from the same zone on the same day

Evaluation

- Data-set: taxi rides in NYC in Oct. 2013 (15 millions rides)

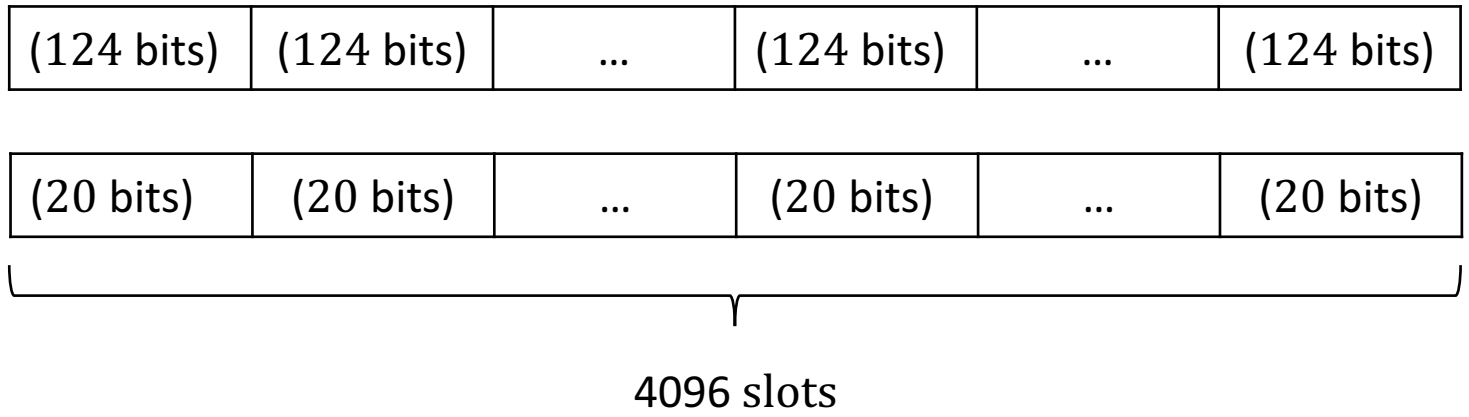


 → Census Tracts (CT) and Neighborhood Tabulation Areas (NTA)

- How practical and efficient is ORide?
  - Per-ride overhead
  - Riders' anonymity vs. drivers' bandwidth
  - Effect of Euclidean distance on ride-matching optimality

Implementation

- Feature the oblivious ride matching algorithm
- SHE parameters: > 112 bits of security
  - Ciphertexts and keys
  - Plaintexts



- In C++ using NFLlib
- No SSE or AVX optimizations

Per-Ride Overhead

S1: Naïve approach
S2: Optimized approach

- Measured on Intel i5-4200U, 2.6 GHz, 6 GB RAM
- Bandwidth overhead

Setting	Rider		Driver	
Algorithm	Upload (KB)	Download (KB)	Download (KB)	Upload (KB)
S1	372	761856	124	248
S2	372	186	124	248

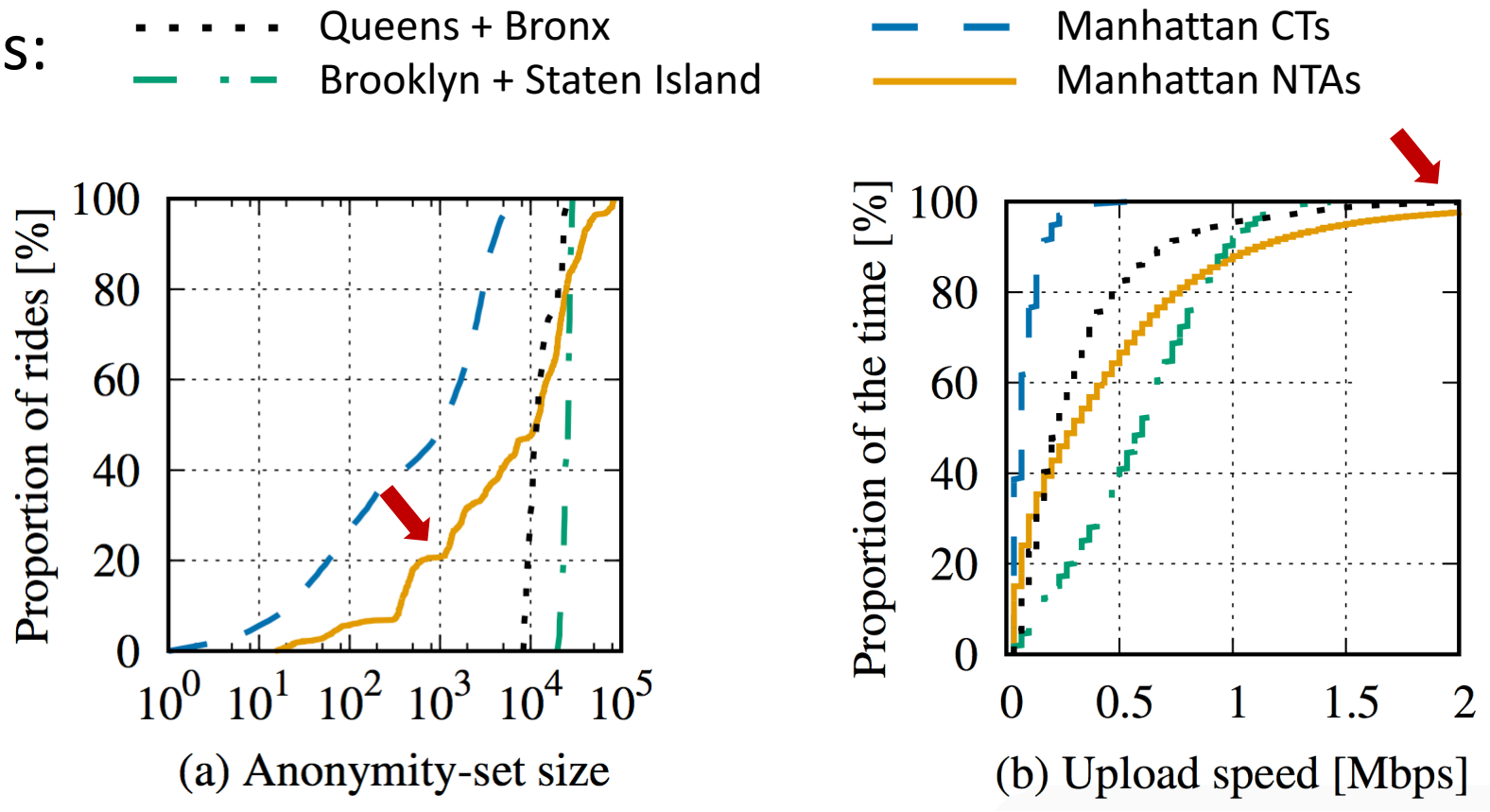
- Computation time

Setting	Rider			Driver		SP	
Algorithm	Gen. keys (ms)	Encrypt (ms)	Decrypt (ms)	Load key (ms)	Encrypt (ms)	Load key (ms)	Compute Dist. (ms)
S1	1.51	2.6	7823.4	0.53	2.6	0.53	113868.8
S2	1.51	2.6	2.2	0.53	2.6	0.53	208.9

The optimized approach significantly reduces bandwidth and computation overhead

Riders' Anonymity Set vs. Drivers' Bandwidth

- Zones:



Large anonymity set and reasonable bandwidth requirements

Conclusion

- ORide: practical and privacy-preserving
  - Strong privacy guarantees
  - Negligible overhead

- Still offers key RHS features:
  - Accountability
  - Easy payment
  - Reputation scores



Source: http://blog.cyberghostvpn.com/avoid-being-tracked-online/

http://oride.epfl.ch