# Privacy Preserving Techniques for Smart Traffic

By

**Hadeeqa Nasir**

**Fall 2017-MS(IS) - 00000204396**

Supervisor

**Dr. Syed Taha Ali**

**Department of Computing**

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(November 2020)

# Approval

It is certified that the contents and form of the thesis entitled "Privacy-preserving techniques for smart traffic" submitted by HADEEQA NASIR have been found satisfactory for the requirement of the degree

Advisor : Dr. Syed Taha Ali

Signature: ________________________

Date: 23-Oct-2020

Committee Member 1:Dr. Arsalan Ahmad

Signature: ________________________

Date: 22-Oct-2020

Committee Member 2:Dr. Wajahat Hussain

Signature: ________________________

Date: 22-Oct-2020

Committee Member 3:Mr. Muhammad Imran Abeel

Signature: ________________________

Date: 22-Oct-2020

# THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Privacy-preserving techniques for smart traffic" written by HADEEQA NASIR, (Registration No 00000204396), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: ______________________________

Name of Advisor: Dr. Syed Taha Ali

Date: 23-Oct-2020

Signature (HOD): ___________________________

Date: ____________________________________

Signature (Dean/Principal): __________________

Date: ____________________________________

# Dedications

*This project is dedicated to my* ***Grandfather****, who always believed in me, prayed for my success and always appreciated and encouraged me.*

*It is also dedicated to my beloved* ***Parents****, who always supported and trusted me*

# Certificate of Originality

I hereby declare that this submission titled "Privacy-preserving techniques for smart traffic" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name:HADEEQA NASIR

Student Signature: ______________

# Acknowledgment

First of all I would like to thank Allah Almighty, who guided me through the knowledge.

Then, i would pay my gratitude to my supervisor. Dr. Syed Taha Ali for guiding me throughout my research work. His sage advice, insightful criticisms and patient encouragement aided the completion of this thesis work in innumerable ways.

Last but not least, i would like to present a special thanks to my parents and friends for their kindness, support, encouragement, help and confidence in me.

# Table of Contents

# List of Tables

# List of Figures

# Abstract

Due to the advancement in connected car technology, the toll calculation methods have been evolved to the electronic toll collection. As the toll collection methods evolved to be electronic, they are also exposed to various attack types. The plain text toll details are communicated to the toll server through the internet, which may be a great threat to security. Various schemes are proposed for this purpose but they are not much efficient. To maintain the privacy and to collect the correct toll according to time and location, a scheme has been proposed in this thesis that is more efficient than previous schemes and uses less computation and bandwidth comparatively.

# Chapter 1

# Introduction

The first chapter of the thesis walks through the basic concepts starting from the early approaches of toll collection to the modern methods, the discovery and importance of using Electronic Toll Collection methods, and hazards of using the conventional techniques of toll collection. It then highlights the need of collecting the tolls electronically, without needing to stop at the toll booths. This chapter also elaborates the motivation behind the research and research goals. This is followed by the objectives and the contributions that the said research has done in this field. This chapter is concluded by presenting a road map of rest of the thesis, its organization and the contribution of each chapter.

## 1.1 Motivation

Vehicular networks are scrutinized to be most optimistic technology for collection of traffic data that facilitate road efficiency and safety applications through Intelligent Transportation Systems (ITS). Increase in the number of vehicles in big cities has also increased the challenges of traffic congestion, road safety etc. for the concerned authorities. There is a critical need to cope up with these problems and for this purpose, advanced and innovative technologies are being used around the world to make the traffic management system better [1].

## 1.2 Background

The term "connected vehicle technology" refers to vehicles that are connected with one another and to its surroundings with the help of various applications and services. There are different communication devices installed in the connected vehicle so that the car may enable the connection with other external network services, devices, applications. These applications and services include traffic safety and efficiency, parking assistance, remote diagnostics and global positioning systems (GPS) or global navigation satellite system (GNSS). A connected car is usually equipped with a wireless local area network which allows it to share data with other devices outside the vehicle. This feature may also enable the real-time location to be shared with the service providers. According to a blog-post in [2], cars equipped with telematics, includes an always-on wireless transmitter that constantly sends vehicle performance and maintenance data to the manufacturer or service provider. In this way, cars know that how much they weigh and can also track the activities like where the driver lives, how fast he drives, where is his office and from where he buy grocery etc. In addition, by connecting a phone to the car, it may also know that who the driver calls and texts. The services discussed above, provides edge for automated law enforcement and make it easy to collect traffic statistics [3].

Due to the use of the technology discussed above and the other advanced technologies in intelligent transportation system, the location privacy has become a big threat to drivers in today's era. Electronic Toll Collection system is one of those technologies which automates the conventional "stop and pay the toll tax" at the toll booth system. This system uses an on-board unit (OBU) which continuously sends the real-time location data to the toll service provider (TSP) so that he may charge the tax accordingly. Although this is a big privacy concern, as the location data is stored over the TSPs databases and in case of dishonest TSP, this data may be leaked. Furthermore, the dishonest TSPs may trade this data to the third parties or advertisement companies and driver's privacy may invade.

As far as the privacy of driver's location is concerned with ETP systems, some of the protocols and methods have already been proposed by the researchers (which have been discussed in detail in related work section). Those protocols protect the driver's privacy in some way but some of them have a lot of communication and storage overhead. Some of the spot-check protocols reveal the location of security cameras to the drivers which could be helpful for dishonest drivers.

In this research, a scheme named 'Cryptograms' is implemented based on the elliptic curve cryptography, which not only ensures driver's location privacy but also provides the solution for correct toll collection using zero-knowledge proofs and traffic enforcement.

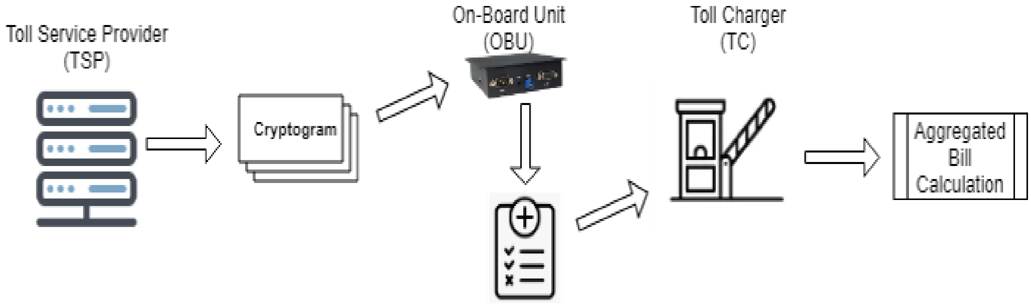


Figure 1.1: Basic workflow for proposed toll collection

This scheme has been implemented in C++ by using the crypto++ library.

In the proposed scheme, OBU's will not send the plain text location data to TSP. Instead, it'll send the correct cryptogram of the fee to the toll-charger. At the end of each tax period, the cryptograms will be aggregated to get the total toll tax. The single cryptogram will have no meaning so that the toll charger will have no idea about the cryptogram generation and he'll not be able to link back the data to the driver.

The European Commission (EC) announced in October 2009, that the conventional toll tax systems in the member states will be replaced by an European Electronic Toll Service (EETS) [4]. In this services, the problems of traffic congestion on the roads and other time and fuel related problems will be overcome. According to the EC, there will be a single on-board unit (OBU), communicating with a single service provider on subscription basis, to pay the taxes so the cars doesn't have to be in a queue to pay the tax hence, saving the time without any congestion on the roads.

Electronic Toll Pricing allows road taxes to be calculated depending on various parameters i.e. the time of use, the location of the car, kind of the road used etc.

### 1.2.1 The Electronic Toll Pricing Ecosystem

The architecture of ETP systems usually consists of an on-board unit (OBU) which, with the help of GPS or GNSS system, constantly sends real-time location data of driver, while driving, to the toll service provider (TSP). The drivers get the subscription of OBU from toll service provider at the start of the period. Upon receiving the data, it is stored in the database. At the end of the subscription period, the TSP calculates the sub-fee based on the parameters in the policy and then aggregates the sub-fees to get a total tax amount corresponding to a single driver.

### 1.2.2 GDPR Compliance with Transport Sector

The European Union's General Data Protection Regulation (GDPR) took effect from 25 May 2018, across its' 28 states [5]. This regulation has a remarkable influence on all organizations which collect, save or use the people's 'personal data'.

Personal data refers to passengers unique identity, while in this particular problem of transportation it will be passenger's or driver's name, contact details, location history, date and times etc. To hide this data, GDPR has made some laws which helps in preserving privacy of the driver.

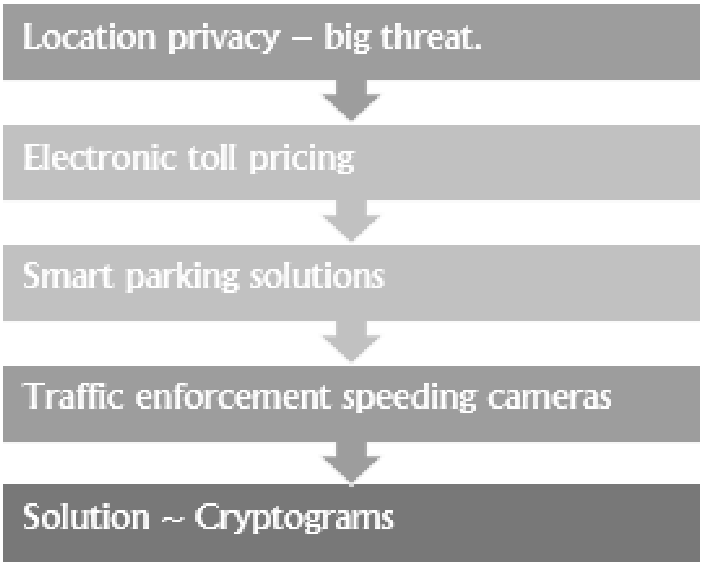


Figure 1.2: Problem Definition

## 1.3 Problem Statement

Implementation of a scheme which not only provides driver's location privacy but also ensures correct toll collection. Speed cameras cause the invasion of privacy. Due to the use of advanced technologies in intelligent transportation system, the location privacy has become a big threat to drivers in today's era. Electronic toll pricing uses an on-board unit which is a big privacy concern that it sends data to the service provider to charge the toll taxes. Smart Parking solutions use sensing devices to determine occupancy of the parking lots, owing to which, the location of the car can be easily detected. The security enforcement speed cameras that may took a picture of the license plate of vehicles are also invading the individual's privacy. In this research, cryptograms will be implemented which not only provides driver's location privacy but also ensures collect toll collection and traffic enforcement.

## 1.4 Objectives and Research Goals

The goal of the thesis is to introduce an Electronic Toll Pricing system in which there is no privacy invasion of users/ cars and which also calculates the correct tolls in less time as compared to the previous schemes by using less operations and providing anonymity. By the end of the implementation, the system would be able to achieve:

1. Identifying the issues of previous ETP systems.
2. To maintain the anonymity and privacy between the parties while calculating bill.
3. To get the desired accurate results with less computation.
4. To calculate the correct toll bills.

## 1.5 Thesis Organization

The thesis has been organized within seven chapters, where each chapter is compiled to shed light on all research aspects of the thesis.

- Chapter 1 “Introduction” describes the motivation behind choosing the topic for research, the problem statement, objectives and organization of the thesis.
- Chapter 2 “Literature Review” goes through the previous work done by authors and their schemes.
- Chapter 3 “Research Methodology” explains the research pathway that has been adopted to achieve the goals.It includes the Research Question, Research Objectives and some explanation about the Data Collection for

research purposes.

- Chapter 4 “Proposed Solution” describes the solution suggested for the research topic. It includes the workflow, an introduction to the cryptograms and overview of the datasets used.

- Chapter 5 “Implementation and Results” shows the architecture of system. It also shows the results of the testing done on the system.

- Chapter 6 “System Analysis” contains the properties of the proposed system ad discusses various attack scenarios.

- Chapter 7 “Conclusion and Future Work” concludes the thesis highlighting the areas which are open for future work.

# Chapter 2

# Literature Review

This chapter explains the hazards of using previous ETP schemes for toll collection and why there was a need of an alternate scheme. It discusses the ETP schemes and describes the pros and cons of those schemes.

Some of the work on the driver's location privacy has already been done which also assures spot-checks for detecting any malicious behaviour in addition with privacy.

There are usually two types of scenarios which are discussed in the previous related searches: In first scenario, the OBU sends the location data to TSP and TSP binds the data to the pricing policy to get the pricing fee calculated. In the other scenario, the pricing policy is shared with OBUs in the cars and they obtain the location data through GPS and calculates the fee and sends the fee to the TSP.

In [6], the OBU sends the path information to the service provider. As the pricing policy is not shared with OBU, the service provider assign prices to the paths accordingly and calculates the bill. In this scheme the users are divided into groups to allow group signatures for achieving anonymity within a group. Another protocol proposed by the authors of [7], the location data is sent to to the TSP sliced into segments such that it is hidden among other OBU segments. Then the TSP calculates the sub-fee from those segments and send it back to each OBU which then calculates the final fee and without disclosing any location data to TSP can prove that final fee is correct. The secure two-party computation protocol is used to detect the dishonest drivers in case they cheat on total tolling price.The authors have used zero-knowledge proofs to ensure the location privacy. For spot-checking, authorities randomly records some time and location tuples corresponding to a license plate and challenge the driver to prove that the location is correct. The authors [8] have proposed two schemes named 'spot record' in which the authority only receives the time and place as location data about a vehicle and 'No Record' in which no data about honest drivers is being shared to maintain driver privacy while ensuring that tolls are accurately collected. They have used e-cash system to prepay for the subscription and when pass by any road that charges the toll, the tokens will automatically be deducted. Another toll collection system is proposed and built, based on Black-box Accumulation (BBA+) in [9]. BBA+ schemes offers unlinkability, and allows users to post- payments.

A privacy oriented architecture for ETP in which the service provider does not see any location data from OBU is presented in [10]. However, the architecture does not allow the TSP and TC to verify the correctness of the operations carried out in the OBU. The authors in [3] have achieved the similar goals by using a cryptographic protocol 'Optimistic Payment' and prove it secure with the help of RSA assumption and zero-knowledge proofs. The homomorphic commitments to the location data are used to disclose minimum amount of location data to the Toll Charger. The TSP asks to open a certain commitment in order to prove the spot-checks. The authors have presented performance analysis which shows that communication and storage overhead is less than previous systems. Although, the protocol described in this paper discloses the location of spot-check cameras to the drivers and in this way the colluding drivers can avoid those routes to pay for the road fee. Another protocol Milo [11], proposed by meiklejohn et al.'s, overcomes the problem of disclosing the location of cameras to drivers (as in [3]). It uses the blind identity encryption scheme and doesn't reveal the security camera's location to the drivers. Another research is carried out [12] using the secure multi-party protocol for communication between TSP and OBU while preserving the location privacy, in which TSPs are allowed to detect malicious OBUs and calculate the total fee.

The research about privacy-preserving traffic enforcement and toll collection was first started in papers of the authors named, Blumberg, Keeler, and shelat [13] and Blumberg and Chase [14]. The first paper introduced a traffic enforcement system i.e. red-light violations as well as introduced a private set-intersection protocol, the second paper discusses a system for toll and road pricing and uses secure function evaluation method.

The papers, [1,15–19], also talks about the pricing scheme for tolls, which includes the sharing of location data with the toll server.

There are also many privacy preserving parking solutions proposed by various authors. Some substantial work is carried out to study the currently designed parking scenarios and to improve the parking efficiency. The authors in [20] have proposed a model P-SPAN that uses bloom filters to help choosing the vacant space for parking without disclosing personal information about driver hence preserving anonymity.

# Chapter 3

# Research Methodology

This chapter describes the steps that have been followed to accomplish the research end goals. All the steps involved in the research methodology are clearly explained and the end results achieved after each step are also presented.

## 3.1 Defining Research

A systematic investigation that includes collection, organization and analysis of data and information is said to be the research. It may also involves the past researches and can also expand the researches already been done.

In section 3.2, the research methodology steps followed for the thesis are explained in detail.

## 3.2 Research Methodology

Research methodology tells about the techniques, that are used to identify, select, process, and analyze information about a specific matter.

The following sections include the steps performed for the undergoing thesis.

### 3.2.1 Define Research Question

The very first step in research is to define the research question which tells that what do you want to do in the research and what things are needed to be discussed in the research and what is the research about?

The research question for this thesis is defined as follows:

"What are the Location Privacy Considerations in Electronic Toll Collection for Billing Purposes?"

The question defines that the area of concern for this research project is about location privacy and specifically it sticks to the Electronic Toll pricing concept for the location privacy. Interest is more towards the billing/ toll collection while preserving the privacy of the car owner, so that no attacker or hacker is able to define the routes that the car travelled through.

### 3.2.2 Determine Research Objective

After defining the research question properly, it is needed to now clearly define the objectives that are to be fulfilled by the end of the research in order to answer the research question. This will help to conduct the research systematically and will allow the researcher to clearly vision out that what needed to be done.

The research objectives for this thesis are defined as follows:

First of all, it is needed to identifying the issues of previously proposed ETP schemes. This will help in making it clear that what are the flaws that your scheme is not supposed to repeat. Also, it will help in addressing the flaws that previous schemes have so that those may be solved in our scheme.

After successfully identifying the issues of previous schemes, the second goal is to figure out that what properties your system needs must to be achieved. For this thesis, the properties include are maintaining the anonymity and privacy between the parties while calculating bill and transparency between the TSP and TC.

The final objective is to figure out that what sort of results we want from our scheme and how much time and computations they take? So the third goal is to get the desired accurate results with less computation in less time as compared to other schemes.

### 3.2.3 Literature Review

Now after narrowing down the objectives of the ETP scheme that this research is going to be achieved, the relevant previous work done was collected and summarized. For gathering the research papers for literature, the official resources used were journal papers, conference papers, white papers, projects websites involved in similar researches, news articles and reports. After we concluded the objectives, the next step was to conduct a detailed study of ETP system, entities involved, their properties and the schemes already proposed.

Some of the schemes proposed, follow the method in which the location data is sent to the TC without any encryption and the cameras are involved to check for the verification.

Other schemes involved the encryption based solutions to send the location data to the server (TC), which then aggregates and calculates the bill.

### 3.2.4 Data Collection and Analysis

After going through a lot of the literature review papers, the detailed data was collected through the help of previous schemes. How much entities involved in others projects? Did they used any third parties? What were the objectives of their schemes? How did they compiled their results? What sort of datasets they used? And what were the results they got? After collecting all the required data, the architecture and work flow was analyzed for carrying out our scheme. The routes where the toll tax is charged were identified through google maps. The tax rate charged for different type of vehicles was identified through the google websites. The tax for the specific route was then calculated accordingly.

### 3.2.5 Research Design

For finalizing the solution domain, numerous research articles, blog posts and github commits were studied. We started by working on the libraries that we have to use for encrypting the cryptograms. Then, the IDE was finalized for coding purposes. For simulating the OBU, Raspberry Pi 3 was chosen.

After carefully testing the platforms, it was decided that the following tools and techniques will be required for the system:

- Elliptic-Curve Cryptography (ECC)
- Cryptograms
- Visual Studio C++
- Raspberry Pi
- Library-CryptoPP
- Decisional Diffie-Hellman

# Chapter 4

# Proposed Solution

The proposed solution has retained the architecture discussed in earlier searches. It has only some key differences.

## 4.1 The Workflow

The communication flow between the entities of the proposed system will be described in this section in detail. The OBU will be installed in each vehicle to get this scheme running. For this purpose, the vehicle owners may take monthly subscriptions from Toll Charging Company.

1. The Toll Service Provider (TSP) will act as a road-side entity or any road-side unit which will provide the parameters i.e. a random number and a generator point from the elliptic curve, for generating the cryptogram, to the passing vehicles.

2. The vehicles will store the random number in the OBU's memory.

3.Then the OBU will generate the cryptograms using the parameters received by TSP and will send those generated cryptogram to the Toll Charger (TC).

4. The OBU will also keep the counter track for the random numbers so it will check if the count for random numbers is '100'? If No, it'll continue as normal. If yes, then it'll sum all the previous random numbers and multiply the answer by the minus sign. Then send the resulted summation random numbers to the TC.

5. The TC will store the received cryptograms in the database for further calculation and it'll also count the number of entries i.e. if '100' or not? If 100, then it'll calculate the aggregate on the cryptogram entries.

Figure 4.1 shows the work flow.

## 4.2 Introducing the Cryptogram

The underlying cryptographic primitive used in [21] has been modified to meet the requirements of our model. There are $i \in [1, 2, 3, ....n]$ search results corresponding to $j \in [1, t]$ search terms. The search results are ranked $v_i$ ranging from 0 to 10 on each search engine result page. Consider a cyclic group consisting of large primes $p$ and $q$ satisfying $q \mid p - 1$. We have a generator $g$ of subgroup $Z_q$ of order $q$ of the group $Z_p$. The system on setup generates random values $r_i \in [0, 100]$, then the following one dimensional matrix is calculated,

$$R_i = g^{r_i}$$

and the corresponding cryptogram matrix is calculated as,

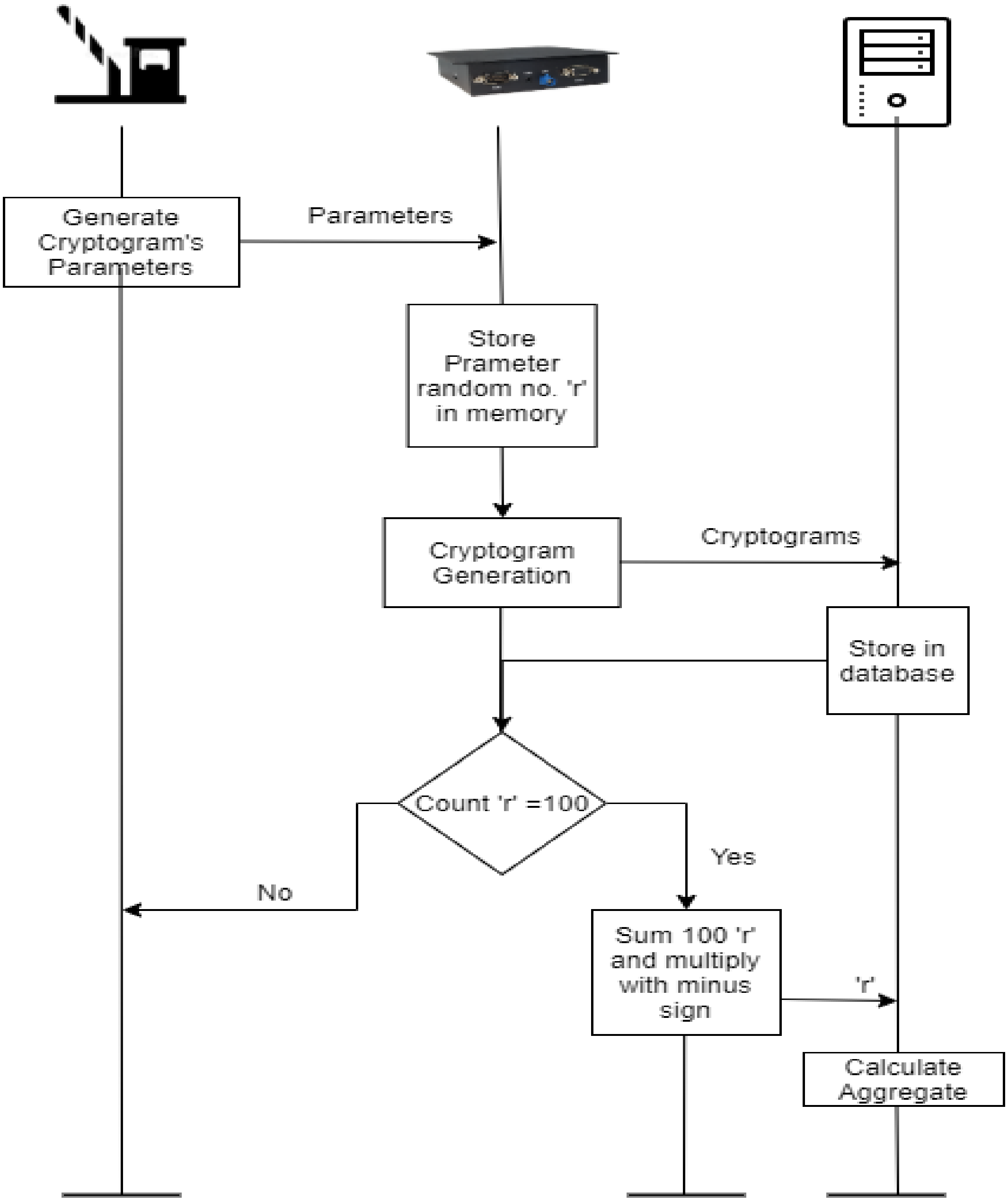

Generate Cryptogram's Parameters
Parameters
Store Prameter random no. 'r' in memory
Cryptogram Generation
Cryptograms
Store in database
Count 'r' =100
No
Yes
Sum 100 'r' and multiply with minus sign
'r'
Calculate Aggregate

Figure 4.1: Work Flow of Proposed Scheme

$$Z_i = g^{r_i} g^{v_i}$$

or it can be calculated as,

$$Z_i = g^{r_i + v_i}$$

where $v_i \in [0, 9]$ is the index of search result. The last $(i = n)$ cryptogram i.e. dummy input is calculated as,

$$r_i = -\sum_{i<n} r_i \tag{4.1}$$

This dummy input is used to cancel the randomness introduced for privacy, such that only aggregate can be deduced from the calculations. It can also be verified by using the following equation,

$$\sum_{i \in n} r_i = 0. \tag{4.2}$$

When the randomness is cancelled, the remaining is the aggregate of votes i.e.

$$\prod_{i \in n} Z_i = g_i^{\sum_{i \in n} v_i} \tag{4.3}$$

Here $g$ is a publicly available so $\sum_{i \in n} v_i$ can easily be calculated.

Correspondingly in Elliptic curve cryptography, $G$ is a generator of elliptic curve $secp256k$. The equations are then converted as follows,

$$R_i = r_i * G$$

and the corresponding cryptogram is calculated as follows,

$$Z_i = r_i * G + v_i * G$$

or,

$$Z_i = [r_i + v_i] * G$$

and the condition in equation 4.1 and 4.2 remains the same.

The aggregate is then calculated as,

$$\sum_{i \in n} Z_i = G \sum_{i \in n} v_i \tag{4.4}$$

Here, the total sum of votes is calculated without giving any information about the individual votes.

## 4.3 Overview of Datasets

The datasets are used for the verification of results of the proposed scheme. There was a T-drive trajectory data sample containing the dataset of 10,357 taxis in China's city Beijing. It contains the Taxi id, longitude and latitude information with time stamp [22,23]. The longitude and latitude information was used from the dataset to check that on which path the taxi was so that the taxi's toll price can be calculated accordingly. Another dataset was used to test the results. This dataset belonged to the routes of Lothian buses in

Edinburgh. We calculted the coordinates from the maps and used them in out program as longitude and latitude to calculate the price of the toll at different cordinates accordingly [24]

### 4.3.1 Dataset Used

The coordinates for calculating the toll for this project's sample results were taken by the google maps of Sydney motorway, Australia [25]. The scenario taken was as follows:

A person goes from his home to the office, 5 days a week. His house is in "Auburn New South Wales 2144, Australia" where as his office is on the " Silverwater RD, Sydney NSW, Australia".

The person takes the West Cornex M4 motorway route as it may be convenient for him and always takes this route for going to and coming from office.

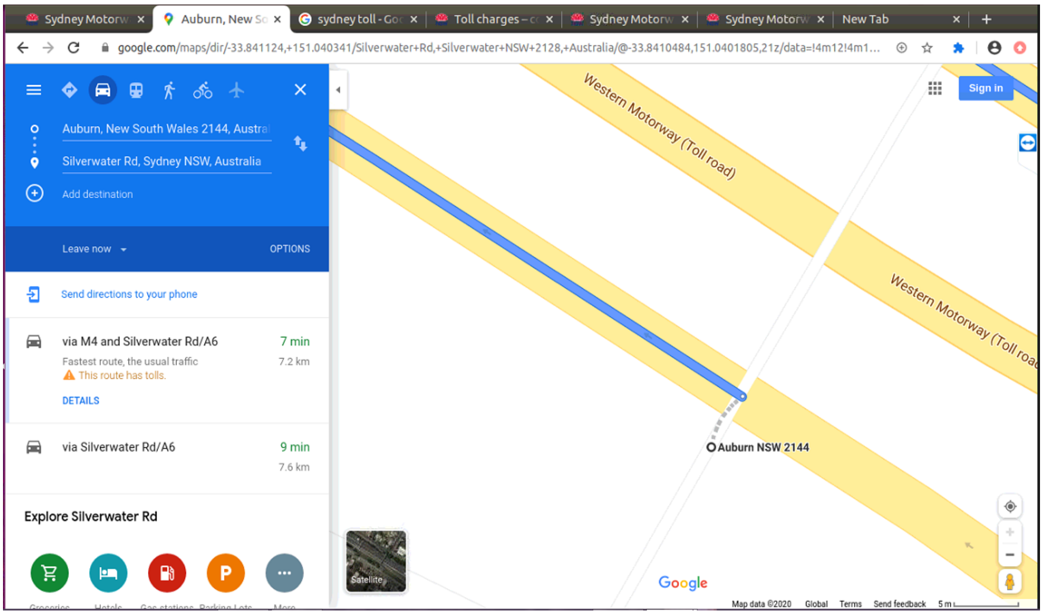
Figures describe the implemented scenario in detail:

The starting and ending point searched on the google maps so that their coordinates may be extracted for feeding in the code is described in figure 4.2.

The figure 4.3 shows the coordinates extracted for start and end of the toll trip.

Whole route on the motorway from where the start of the trip i.e. Hay-Market to the end point of the trip i.e. Lidcombe is shown in figure 4.4.

All the motorways of Sydney city and their map and routes are shown in figure 4.5.



google.com/maps/dir/-33.841124,+151.040341/Silverwater+Rd,+Silverwater+NSW+2128,+Australia/@-33.8410484,151.0401805,21z/data=!4m12!4m1…

Auburn, New South Wales 2144, Austra

Silverwater Rd, Sydney NSW, Australia

Add destination

Leave now ▾ OPTIONS

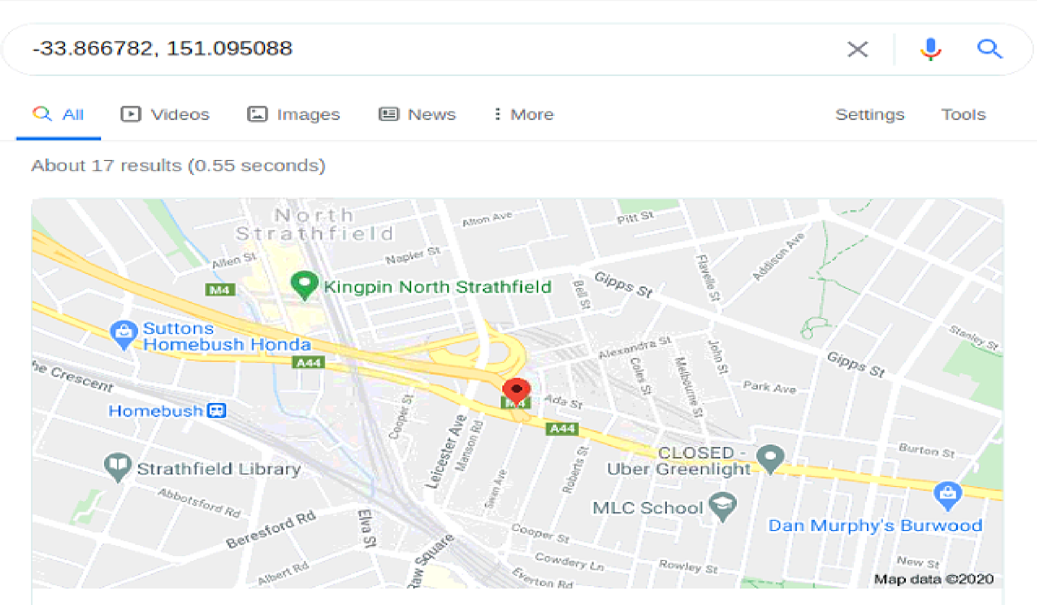
Send directions to your phone

via M4 and Silverwater Rd/A6 7 min
Fastest route, the usual traffic 7.2 km
⚠ This route has tolls.
DETAILS

via Silverwater Rd/A6 9 min
7.6 km

Explore Silverwater Rd

Figure 4.2: Start and End of route

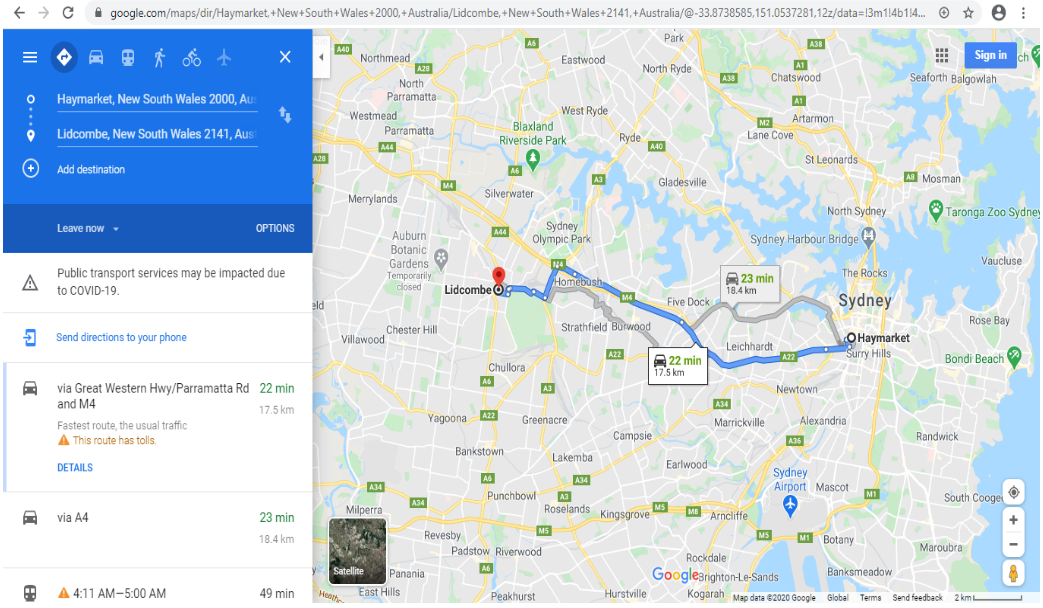


-33.866782, 151.095088

All Videos Images News More Settings Tools

About 17 results (0.55 seconds)

Figure 4.3: Coordinates Extraction



google.com/maps/dir/Haymarket,+New+South+Wales+2000,+Australia/Lidcombe,+New+South+Wales+2141,+Australia/@-33.8738585,151.0537281,12z/data=!3m1!4b1!4...

Haymarket, New South Wales 2000, Au

Lidcombe, New South Wales 2141, Aus

Public transport services may be impacted due to COVID-19.

via Great Western Hwy/Parramatta Rd and M4 — 22 min, 17.5 km

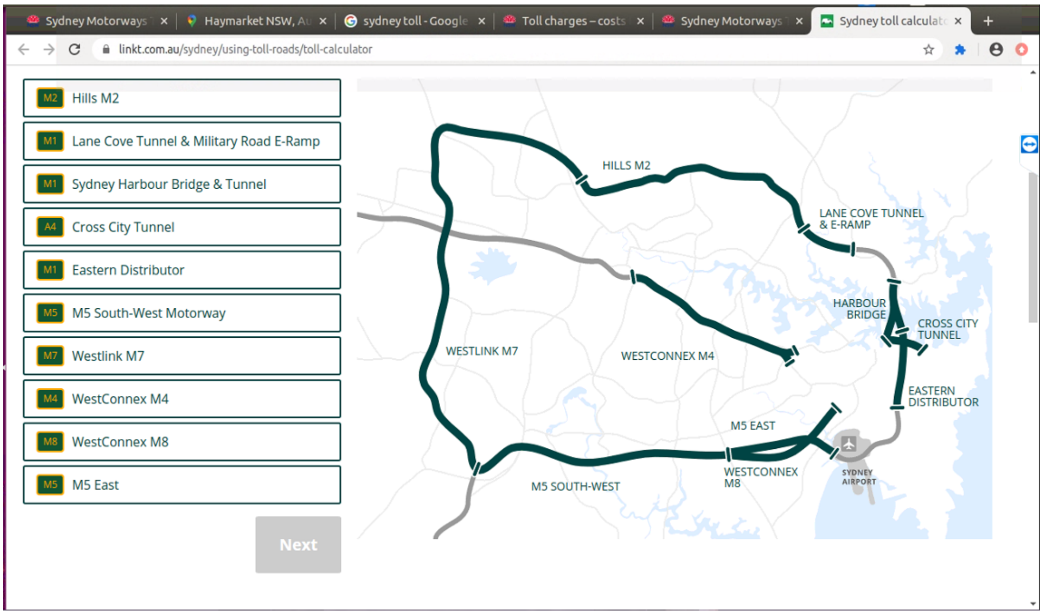
Fastest route, the usual traffic

This route has tolls.

via A4 — 23 min, 18.4 km

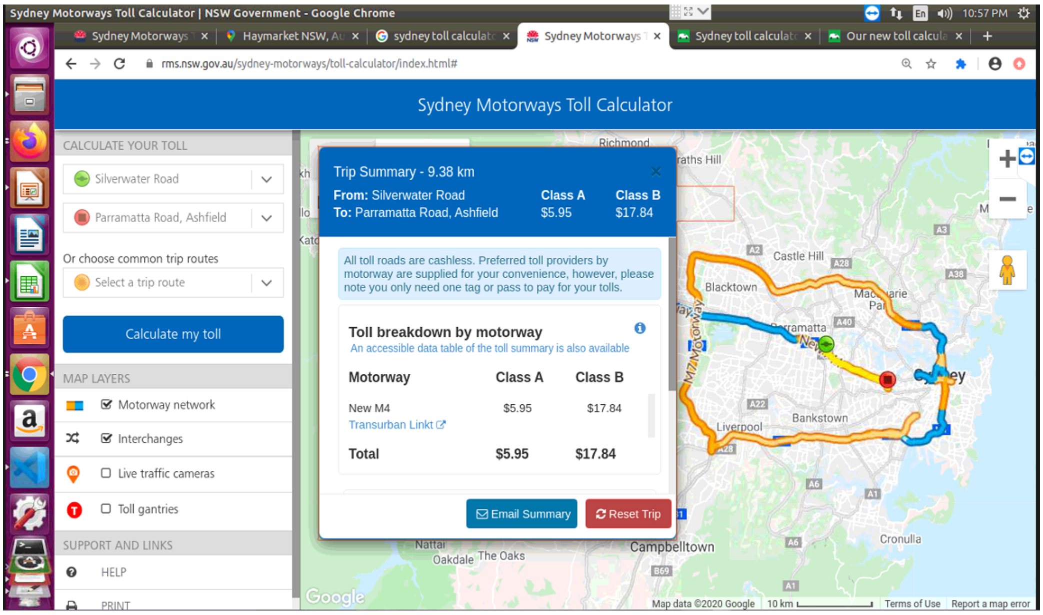
4:11 AM—5:00 AM — 49 min

Figure 4.4: Defined Route



linkt.com.au/sydney/using-toll-roads/toll-calculator

Figure 4.5: Motorway Names



Sydney Motorways Toll Calculator

CALCULATE YOUR TOLL

Silverwater Road

Parramatta Road, Ashfield

Or choose common trip routes

Select a trip route

Calculate my toll

MAP LAYERS

☑ Motorway network

☑ Interchanges

□ Live traffic cameras

□ Toll gantries

SUPPORT AND LINKS

HELP

PRINT

Trip Summary - 9.38 km

**From:** Silverwater Road
**To:** Parramatta Road, Ashfield

| | Class A | Class B |
|---|---|---|
| | $5.95 | $17.84 |

All toll roads are cashless. Preferred toll providers by motorway are supplied for your convenience, however, please note you only need one tag or pass to pay for your tolls.

**Toll breakdown by motorway**

An accessible data table of the toll summary is also available

| Motorway | Class A | Class B |
|---|---|---|
| New M4<br>Transurban Linkt | $5.95 | $17.84 |
| **Total** | **$5.95** | **$17.84** |

Email Summary  Reset Trip

Figure 4.6: Toll Details

The toll details and the prices apply on the toll roads for different kind of vehicles is shown in figure 4.6.

The values were used as an input to the program (code), and the desired result was the total price of total in cryptogram form so that no one can back track the exact locations.

# Chapter 5

# Implementation and Results

In this chapter, the developed prototype for the proposed scheme is discussed to compute the efficiency of the protocol under the use of real-world datasets.

Starting from section 5.1, we move forward by giving an overview of the problem and solution detail.

The idea involves the three entities: On-board unit (OBU) in the car, Toll Service Provider (TSP), Trusted Third party (Road side-unit) who will generate cryptogram or just give the random number for creating the cryptogram (based on the scenario) and will provide it to the driver with the OBU.

## 5.1 Research and Implementation Overview

The pricing policy based on the location and time will be shared to both, the toll service provider and the OBU. There could be the following scenarios:

1. One way could be that at the start, the car owner will take the sub-

scription or tokens from service provider and will use them.

*Problem:* The problem arises in this scenario at the time of spot-checking. How will the service provide assures that the tokens were redeemed correctly according to the location and time.

2. Another way could be that there'll be a road side unit providing the cars with random numbers and by using those random numbers, the OBU will calculate the cryptogram of the price, based on the time and location. After calculating the cryptogram the OBU will send that to the service provider. There is a policy that lets say after getting the100 cryptograms from a single OBU, the service provider will aggregate those cryptograms to get the bill of that car. In this scenario, after calculating the 99 cryptograms, the last cryptogram would be a dummy in which the price will be zero and the random number will be calculated in a way that cancels out all other random numbers so that the actual bill can be calculated. This last cryptogram will be automatically calculated by OBU after consuming the 99 cryptograms. After receiving 100 cryptograms from a single OBU, the service provider will calculate their bill. For spot-checks, there could be cameras and the location of cameras won't be revealed.

*Spot-checks:* The service provider will ask to open a random cryptogram to check that either it was calculated correct according to the location or not. From that camera, service provider will know the location of the car and the random number for that specific cryptogram will be given by road side unit. The OBU will provide the price value which was used in that cryptogram calculation. In this way, if that price will not be true according to the location, the driver will said to be as dishonest and his license might get cancelled. The electronic toll bill will be calculated at the end of the month.

## 5.2 Evaluation

Evaluation is an important step for any scheme. It involves testing the scheme with various parameters and check whether it takes more or less time than the previously proposed schemes. Also, it will check the bandwidth consumed and the storage capacity.

After thoroughly studying the previous schemes, they are compared to our scheme and the result is discussed in Table 6.1 and Table 6.2.

The details of the testing performed, is given in the following sections.

## 5.3 Security Testing

After discussing the proposed solution and its implementation in detail, this section will discusses about the security of the proposed scheme.

The scheme is simulated on the Raspberry Pi, which works as the OBU in this scenario. Dedicated cores for running the code, were assigned. The system used for aggregation was Ubuntu i7 and it is assumed that the TC will also have the same setup for aggregating the cryptograms. The core i7 used for testing purposes has GHz and RAM, running a 64 bit ubuntu system.

It was first tested on a single core. Then the all four cores were dedicated for running the scheme code, to check that how much less time it takes.

Then, some of the cores were dedicated for this purpose. Also, the threads were used for dedicating the cores and to run all the threads concurrently on the cores.

To run on a Raspberry Pi, it took 481 milli seconds for creating a single cryptogram.

## 5.4 Performance Testing

This section discusses about the performance of the proposed scheme. It includes further two sub sections i.e. computation overhead and bandwidth overhead.

### 5.4.1 Computational Overhead

The generation time for one cryptogram is 418 microseconds which in comparison with other scheme is less time. It tells that the proposed scheme is efficient as it doesn't take much time to execute.

## 5.5 An Alternative Implementation

The proposed protocol in this research has less computations, hence lightweight. In this scheme, the cryptograms are pre-computed by the broker i.e. TSP and the OBU has to only select from those cryptograms, the value of current toll, according to the time and location. The toll pricing policy will be shared with the OBU by the toll company or government (whoever is controlling the procedure). The less computation time also means that the less bandwidth will be used.

An alternative method can also be implemented which may go as, the OBU will ask for the parameters from the TSP and the TSP will send only the public parameter i.e. 'g' to the OBU, along with a random value 'r' used to calculate the cryptogram as (g$^{v}$) $*$ $(g^{r})$.

The toll pricing policy will already be shared with the OBU, so OBU will be able to pick the right cost of toll according to time and location and will use it as the parameter 'v' in the formula to calculate the final cryptogram. Then the OBU will send the cryptogram to the TC. In this scenario, there will be need to be check that the OBU will use the correct toll value to calculate the cryptogram and it is not dishonest.

# Chapter 6

# System Analysis

## 6.1 General Properties

This scheme aims to provide the general functionality along with the advantages coinciding with previous schemes. This schemes keeps the existing ecosystem of OBU in the car, the toll service provider and the toll charger without adding any new entities. The general properties, other than privacy are as follows: this system is efficient and the data which OBU sends to the server will have no meaning until and unless it is aggregated. Once aggregated, it'll only reveal the total pricing fee for a month or for a subscription period and will reveal no any other data about driver or its location. The proposed scheme does not empower malicious attackers to manipulate the results.

The key privacy properties of the solution will be described next.

## 6.2 Privacy Properties

The foremost privacy property is that location is not known to anyone in this scheme except the driver's OBU itself. The location data is not communicated to anyone so that the driver's location history can't be tracked. The individual cryptograms that are sent to the TSP by the OBU will have no meaning to the TSP, so the individual track of the driver is also not possible.

### 6.2.1 Trust Model

The trust assumption about the three of the participated entities, are as below: User: The user interfaces with the analytics team via a local device OBU, that cathes the signal upon going from the place where toll has to be paid.It also maintains a the record of the toll enteries. Here it is assumed that the user trusts the device. It is also assumed that the OBU's privacy is also protected and it is temper proof. The OBU can control and only send the data to the publisher that is needed by them. It doesn't releases any information that that is beyond what is requested.

In the threat model, the case is defined as, the user or the OBU may be malicious or dishonest. Such users may withhold the data that is supposed to be send to the service provider. The dishonest users may also tweak the OBU in their cars, so that OBU may send the wrong data instead of the actual data. The proposed scheme defends against the above defined possibilities by the use of the camera which may take snapshot time to time.

In the scheme, it is not proposed that user directly sends the personally identifiable information to the toll service provider or toll charger. Instead, the public values and random values will be provided by the TSP and the cryptogram will be sent to TC with a random vehicle id, after generation.

The scenario in which malware is injected into the user's device to steal or tweak its information in order to send false information or no information at all to TSP, is not discussed.

### 6.2.2 Broker

Broker is a middle agent that deals with the transactions between two parties. TSP acts as a middle agent between the OBU and the TC in this architecture.The broker pre-generates the cryptograms for all the vehicles and distributes them to all the OBUs. OBU will select the correct cryptogram according to the route, from the list and will send it to the publisher instead of broker, to achieve the transparency between all the parties. In this way, broker, who has generated the cryptograms will not be able to acquire the answers and the publisher, who got the cryptograms from OBUs, will not be able to identify that what is the meaning of the cryptogram, hence anonymity is achieved. The separation of tasks between broker and TC is important because individual cryptograms from OBU may be decoded if the broker and publisher collude. It is expected that the separation of duties can be legally enforced and regulated by industry watchdog bodies. In such a case, where both the publisher and the broker are same parties, there will have a technical separation to be maintained strictly. The publisher and broker parties should be authentic, honest and trusted and must be approved by the government.

Two different threat scenarios are addressed in this research, first is related to honest but curious broker. In this scenario, we consider that broker follows the protocol but also tries to learn the information. The other scenario is related to a malicious broker, who intentionally colludes with publisher to decrypt the information of the cryptogram.

## 6.3 Security Properties

The proposed scheme has the folloeing security properties:

1. It ensure that drivers behave honestly.

2. Inactive OBUs in the driver's car must be detected.

3. False GPS data from OBU must be detected so that the drivers may not be able to spoof the GPS data to get charged for cheaper price on a cheaper route than the actual route on which they are driving.

4. OBUs in the car must not be tweaked in a way that they charge arbitrarily for road prices instead of following the pricing policy.

5. There must be some method to verify the final calculated fee from the OBU that if its true or not.

6. A dishonest central authority cannot learn any more information than they do by spot-checking. In first scheme, the central authority only learns the location data corresponding to times and places where the vehicle is physically observed.

| **Comparison of other proposed schemes** | | | | |
|---|---|---|---|---|
| **Scheme Names** | **Security Assumptions** | **Privacy** | ***(RCD)** | **(RVC) |
| VPriv [7] | RSA, ZKP, SMC | Partial | No | No |
| PrETP [3] | RSA, ZKP | Partial | No | No |
| Milo [11] | RSA, ZKP, SMC | Partial | No | No |
| Spot Record [8] | RSA, Hash | Partial | No | No |
| Basic NR | RSA, Hash | Full | Yes | Yes |
| t-bound NR | RSA, Hash | Full | Yes | Yes |

* real-time cheating detection; **real-time verifier communications

Table 6.1: Comparison of various security protocols

## 6.4 Attack Scenarios

Numerous attack scenarios are discussed in this section which tells that how the proposed solution is secure against them.

Dis-honest Broker: Broker's role is to send the pre-computed cryptograms to the OBU. In [21], there are Zero knowledge proofs, along with each cryptogram, which ensures that the cryptogram values sent by the broker are correct and the broker is performing honest, while in our scheme, there is no need of ZKP's, as our scheme is based on the assumption that the broker is honest, whether it is a third party or the TSP. Most probably, the broker will be TSP which means that it will not be any third party but a party from toll's own company. The broker will be honest and will not manipulate the cryptograms. Even if the broker try to manipulate the cryptogram by embedding some code i.e. tracking protocol, it will not be succeeded, as the

| **Comparison of other proposed schemes** | | | | |
|---|---|---|---|---|
| **Scheme Names** | **GPS Location Collection By** | **Tax Calculation by** | **Spot Checking Cameras?** | **Disputes solved by** |
| Vpriv [7] | Server | Server | Yes | TSP |
| Group-Signature Scheme [6] | Server | OBU | No | Authority |
| PrETP [3] | OBU | OBU | Yes | TSP |
| Phantom Toll Booth [11] | OBU | OBU | Yes | Authority |
| PriPAYD [10] | OBU | OBU | No | TSP |
| Electronic Road pricing [19] | Not Required | OBU | Yes | Not Required |

Table 6.2: Comparison of various pre-proposed solutions

results of the cryptogram will not be sent to the broker. The broker has to collude with the TC, in order to get the tracking information in this case. But as far as the TC is honest, the broker will not be able to collude.

Dishonest Utility Provider (TC): In the proposed protocol, the utility provider i.e. TC's role is to aggregate the cryptograms sent by the OBU at the end of the month, to get the total toll bill value. It can also check for the verification, that whether the cryptogram sent by the OBU is correct according to the location and time, or not. If the TC is dishonest, it will conduct the aggregation on the smaller sets, sent by OBU to find out its location patterns by back-tracking.

## 6.5 Securing the Broker

The proposed protocol's security and privacy lies in the assumption that the broker (TSP) is trusted and it doesn't collude with the utility provider (TC). This assumption can be made more reliable, by distributing the trust among multiple brokers which means that the TC has to collude with all the brokers, in order to get a single location data of a user.The services from trusted third parties may also help. This will result in that the TC has to collude with all the parties, to get the information about the cryptograms or the location data.

# Chapter 7

# Conclusion & Future Work

Installing the OBU device in the cars will give an advantage to the car drivers that they doesn't have to reduce the speed or to stop at the road to pay the toll, hence, reducing the road congestion and saving time. The proposed scheme has detected the flaws in previous schemes and addressed the problems related to various schemes. The approach that is introduced called cryptograms, let the toll service providers collect the toll bill correctly while ensuring that the toll price sent by the OBU in driver's car is correct as per the location and time. The proposed scheme maintains the anonymity and location privacy between the car driver and the toll bill calculator. It has also shown that the proposed scheme is more efficient than previous schemes in terms of computations. An implementation is also done on Visual Studio Code in C++ using elliptic curve cryptography.

## 7.1 Future Work

There is some work that can be done in future on this scheme and other related schemes may be proposed. One can work on attack scenarios where malware is injected in OBU so that it may never send the false information to TSP. Driving violations may be addressed. Another way to extend this work can be that the solution is applied to parking schemes and traffic enforcement's as well.

# Bibliography

[1] S. Djahel, R. Doolan, G.-M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 125–151, 2014.

[2] B. Hanvey, "Your car knows when you gain weight," https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html, THE NEWYORK TIMES, May 2019.

[3] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "Pretp: Privacy-preserving electronic toll pricing." in *USENIX Security Symposium*, vol. 10, 2010, pp. 63–78.

[4] E. Commission, "Commission decision of 6 october 2009 on the definition of the european electronic toll service and its technical elements, 2009." THE European Commission, October 2009.

[5] Robert, "The gdpr: what organisations in the transport sector need to do now."

[6] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, 2012, pp. 85–93.

[7] R. A. Popa, H. Balakrishnan, and A. J. Blumberg, "Vpriv: Protecting privacy in location-based vehicular services," 2009.

[8] J. Day, Y. Huang, E. Knapp, and I. Goldberg, "Spectre: spot-checked private ecash tolling at roadside," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 61–68.

[9] M. Hoffmann, V. Fetzer, M. Nagel, A. Rupp, and R. Schwerdt, "P4tc-provably-secure yet practical privacy-preserving toll collection." *IACR Cryptology ePrint Archive*, vol. 2018, p. 1106, 2018.

[10] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "Pripayd: Privacy-friendly pay-as-you-drive insurance," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 742–755, 2010.

[11] S. Meiklejohn, K. Mowery, S. Checkoway, and H. Shacham, "The phantom tollbooth: Privacy-preserving electronic toll collection in the presence of driver collusion." in *USENIX security symposium*, vol. 201, no. 1, 2011.

[12] S. Rass, S. Fuchs, M. Schaffer, and K. Kyamakya, "How to protect privacy in floating car data systems," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. ACM, 2008, pp. 17–22.

[13] A. J. Blumberg, L. S. Keeler, and A. Shelat, "Automated traffic enforcement which respects" driver privacy"," in *Proceedings. 2005 IEEE Intelligent Transportation Systems, 2005.* IEEE, 2005, pp. 941–946.

[14] A. J. Blumberg and R. Chase, "Congestion pricing that preserves driver privacy," in *2006 IEEE Intelligent Transportation Systems Conference.* IEEE, 2006, pp. 725–732.

[15] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1592–1603, 2018.

[16] D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489–516, 2017.

[17] T. Frosch, S. Schäge, M. Goll, and T. Holz, "On locational privacy in the absence of anonymous payments," in *Data Protection on the Move.* Springer, 2016, pp. 75–100.

[18] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "Design and formal analysis of a group signature based electronic toll pricing system." *JoWUA*, vol. 4, no. 1, pp. 55–75, 2013.

[19] R. Jardí-Cedó, M. Mut-Puigserver, J. Castellà-Roca, M. Magdalena, and A. Viejo, "Privacy-preserving electronic road pricing system for multifare low emission zones," in *Proceedings of the 9th International Conference on Security of Information and Networks*, 2016, pp. 158–165.

[20] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, “Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6504–6517, 2018.

[21] S. F. Shahandashti and F. Hao, “Dre-ip: a verifiable e-voting scheme without tallying authorities,” in *European Symposium on Research in Computer Security.* Springer, 2016, pp. 223–240.

[22] J. Yuan, Y. Zheng, X. Xie, and G. Sun, “Driving with knowledge from the physical world,” in *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining.* ACM, 2011, pp. 316–324.

[23] J. Yuan, Y. Zheng, C. Zhang, W. Xie, X. Xie, G. Sun, and Y. Huang, “T-drive: driving directions based on taxi trajectories,” in *Proceedings of the 18th SIGSPATIAL International conference on advances in geographic information systems.* ACM, 2010, pp. 99–108.

[24] S. of Informatics, “Lothian buses full fleet gps traces, 2014 to 2015 [dataset],” University of Edinburgh.

[25] N. Government, “Sydney motorway toll charges from 1 october 2020,” NSW Government.