# A SECURE AND EFFICIENT REVOCATION PROTOCOL FOR GROUP SIGNATURES IN VEHICULAR AD HOC NETWORKS

NUR FADHILAH BINTI MOHD SHARI

FACULTY OF SCIENCE
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

# A SECURE AND EFFICIENT REVOCATION PROTOCOL FOR GROUP SIGNATURES IN VEHICULAR AD HOC NETWORKS

NUR FADHILAH BINTI MOHD SHARI

DISSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

FACULTY OF SCIENCE
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

## UNIVERSITI MALAYA

## ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: (I.C./Passport No.: )

Registration/Matrix No.:

Name of Degree:

Title of Project Paper/Research Report/Dissertation/Thesis (“this Work”):

Field of Study:

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya (“UM”), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate’s Signature Date:

Subscribed and solemnly declared before,

Witness’s Signature Date:

Name:
Designation:

# A SECURE AND EFFICIENT REVOCATION PROTOCOL FOR GROUP SIGNATURES IN VEHICULAR AD HOC NETWORKS

## ABSTRACT

Vehicular ad hoc networks (VANETs) allow wireless communication between vehicles and roadside infrastructure to improve road safety and traffic efficiency. Due to the open wireless nature of a VANET, the network is exposed to several security attacks. The presence of attackers could pose a threat and further cause harm to the network. The attackers are categorised as internal and external. An internal attacker is a legitimate member of the network who possess valid credentials and may exploit its legitimacy to mislead and jeopardize the safety of other users, thus causing more damage than an external attacker. This thesis addresses a new revocation protocol for group signatures in VANETs. A revocation protocol protects VANETs against the internal attackers, where it enables such attackers to be removed from the network. A secure and efficient revocation protocol should be emphasized to ensure that VANETs are resilient to internal attackers and thus, vehicles can fully utilize the benefits of VANETs. We begin by analysing some existing revocation protocols based on various cryptographic primitives in the literature. From our analysis, we discover that one of the group signature schemes , called MLGS, lack of revocation protocol where no explicit revocation mechanism was presented. This gap in the literature highlights the need to design a secure and efficient revocation protocol for the scheme, as well as other schemes with similar setup and construction. Prior to the construction, we design a generic abstraction of a revocation protocol for group signatures. The generic abstraction serves as a guideline to design our revocation protocol. We then analyse the security of our proposed protocol and evaluate its performance. We ensure the performance of our revocation protocol is comparable (or better) to those of existing protocols in the literature.

**Keywords:** Revocation, group signature, vehicular communication.

# PROTOKOL REVOKASI YANG SELAMAT DAN EFISIEN BAGI TANDATANGAN BERKUMPULAN DALAM RANGKAIAN AD HOC KENDERAAN

## ABSTRAK

Rangkaian ad hoc kenderaan (VANET) ialah teknologi komunikasi tanpa wayar yang melibatkan komunikasi antara kenderaan dan infrastruktur jalan raya bertujuan untuk mempertingkatkan keselamatan jalan raya dan kelancaran lalu lintas. Oleh kerana VANET menggunakan rangkaian komunikasi terbuka, VANET terdedah kepada beberapa ancaman keselamatan. Kehadiran penyerang ini boleh dikategorikan sebagai dalaman dan luaran. Penyerang dalaman adalah merupakan ahli berdaftar yang mempunyai kelayakan yang sah dalam VANET dan boleh menyalah gunakan kredibiliti mereka untuk mengelirukan dan menjejaskan keselamatan ahli lain, yang mana boleh mendatangkan kerosakan yang lebih teruk berbanding penyerang luaran. Objektif utama tesis ini adalah untuk membina protokol revokasi yang baru khusus bagi skim tandatangan berkumpulan dalam VANET. Protokol ini melindungi VANET daripada penyerang dalaman, di mana penyerang tersebut akan ditarik keahliannya daripada VANET. Protokol revokasi yang selamat dan efisien perlu ditekankan supaya VANET bebas daripada penyerang dalaman. Dengan itu, kelebihan dan fungsi VANET dapat dimanfaatkan oleh pengguna. Kajian dimulakan dengan menganalisis beberapa protokol revokasi berdasarkan pelbagai kriptografi primitif yang terdapat dalam kesusasteraan. Daripada analisis yang dijalankan, salah satu skim tandatangan berkumpulan yang bernama MLGS hanya membincangkan mengenai protokol revokasi tanpa mempersembahkan mekanisme revokasi yang jelas. Kelompongan dalam kesusasteraan ini menekankan keperluan untuk membentuk satu protokol revokasi yang baru bagi skim tersebut, yang mana ia turut boleh diaplikasikan oleh skim lain yang berasaskan pembinaan yang sama. Abstrak generik protokol revokasi juga direka bentuk khusus untuk skim tandatangan berkumpulan dalam VANET. Abstrak ini dijadikan sebagai garis panduan kami untuk mereka bentuk protokol revokasi yang baru tersebut. Kemudian, tahap keselamatan dan prestasi protokol tersebut dianalisa. Prestasi protokol revokasi ini dipastikan setanding (atau lebih baik) daripada protokol revokasi sedia ada di dalam kesusasteraan.

**Kata kunci:** Revokasi, tandatangan berkumpulan, komunikasi kenderaan.

# ACKNOWLEDGEMENTS

I am deeply indebted to my supervisors, Dr. Amizah Malip and Assoc. Prof. Dr. Wan Ainun Mior Othman, for their priceless supervision, support and patience throughout my study. Despite being extremely occupied with other research and teaching, they always made themselves available for our research meetings and patiently responded to all my inquiries through emails. Their professional insights and gentle advice led me in the right direction to complete this research. My tremendous gratitude to my family for their wholehearted support and encouragement. They are my great source of inspiration and strength. I would also like to extend my gratitude to Public Service Departments of Malaysia for its generous sponsorship. Last but not least, my special thanks to those who have helped me either directly or indirectly throughout this thesis work.

# TABLE OF CONTENTS

## LIST OF FIGURES

# LIST OF TABLES

# LIST OF SYMBOLS AND ABBREVIATIONS

| | |
|---|---|
| CA | : Certificate Authority |
| CRL | : Certificate Revocation List |
| DLP | : Discrete Logarithm problem |
| DSRC | : Dedicated Short-Range Communication |
| ETSI | : European Telecommunications Standards Institute |
| FCC | : Federal Communications Commission |
| IEEE | : Institute of Electrical and Electronics Engineers |
| MA | : Master Authority |
| MM | : Membership Manager |
| OBU | : On-Board Unit |
| PKC | : Public Key Cryptography |
| RL | : Revocation List |
| RS | : Reputation Server |
| RSU | : Road-Side Unit |
| RTA | : Regional Transportation Authority |
| TA | : Trusted Authority |
| TM | : Tracing Manager |
| TP | : Trusted Party |
| TRD | : Tamper Resistant Device |
| V2I | : Vehicle-to-Infrastructure communication |
| V2V | : Vehicle-to-Vehicle communication |
| VANET | : Vehicular Ad Hoc Network |
| VLR | : Verifier Local Revocation |
| WAVE | : Wireless Access Vehicular Environment |

# CHAPTER 1: INTRODUCTION

*In this chapter, we first define our research motivation. Then, we present an overview of vehicular ad hoc network (VANET). We further discuss the importance of revocation in VANETs. Lastly, we state the scope and objectives of our thesis.*

## 1.1 Motivation

Road safety and traffic efficiency remain serious issues globally (WHO, 2015; Wegman, 2017; Ning et al., 2016; UNRSC, 2011; Han & Yang, 2008; Moya-Gómez & García-Palomares, 2017). Road accidents is one of the top three causes of death for people aged between 5 and 44 years (UNRSC, 2011). Every day, more than 3000 people are killed in road accidents around the world which gives a total of 1.25 millions fatalities a year (WHO, 2015). Additionally, 20 to 50 million people are injured as a result of road accident where many ended up being disabled (UNRSC, 2011). Meanwhile, traffic congestion has become worse in recent years, especially during peak hours and in the areas of high population densities (Han & Yang, 2008; Moya-Gómez & García-Palomares, 2017). The delay of traffic causes an increase in operating costs of vehicles, and travel time. According to the Texas Transportation Institute, drivers in the United States wasted 2.9 billion gallons of fuel, and 5.5 billion hours of time in 2011 due to road congestion (Schrank et al., 2012).

The factors contributing to these issues varies. Road accidents may be caused by three factors; human error, road-environment, and poor vehicle maintenance (Mohanty & Gupta, 2015; Abu-Zidan & Eid, 2015). Among the three factors, human factor is the leading cause of road accidents (Abu-Zidan & Eid, 2015). Instances of human factor include bad driving behavior and lack of road safety awareness. On the other hand, traffic delays continue to worsen due to an increase in the number of vehicles over the years (Alam & Ahmed, 2013; TAC, 2015). An obstacle on the road such as road construction may also lead to traffic congestion (TAC, 2015).

Vehicular ad hoc networks (VANETs) has become an emerging research area to alleviate the issues of road safety and traffic efficiency (Toh, 2001; Kroh et al., 2006; He et al., 2015; Artail & Abbani, 2016; Malip et al., 2014; Shao et al., 2016). It enables wireless communication between vehicles and roadside infrastructures to inform about traffic and road conditions so that drivers can be aware of the situation ahead of them. Early detection of potential dangers may improve road safety as drivers can take appropriate actions to minimise adverse consequences. VANETs may also improve traffic efficiency by providing information on traffic situation to assist drivers to decide which route is optimal for a better driving experience (Toulni et al., 2014).

## 1.2 Problem Overview

Despite the advantages of VANETs, the network is prone to security attacks due to its open wireless nature. An adversary who launch the attacks could pose serious threats and cause harm to the drivers (Qu et al., 2015). The type of attacks is heterogeneous, ranging from controlling the vehicle system to tracking drivers' activities. The adversary may also be a legitimate vehicle who is in possession of a valid credential (Raya & Hubaux, 2007). Such misbehaved vehicle may send false information in the network to affect the behaviour of other vehicles. Drivers may react to false information which may result in life-endangering situation.

People would be less likely to participate in VANETs if the system is vulnerable to attacks. The system vulnerability may render the technology to be unutilized. Thus, in order to make VANETs beneficial to vehicles, it is mandatory to protect the network against adversaries. One of the main solutions is to address a secure and efficient revocation protocol in VANETs system (Liu et al., 2010). Revocation is vital to ensure these misbehaved vehicles are held accountable for their own actions and to prevent them from further participation in the network.

## 1.3 Vehicular Ad Hoc Network

A vehicular ad hoc network (VANET) is a self-organised network that uses vehicles as mobile nodes to communicate without requiring a fixed wireless infrastructure. This section introduces the basic architectural system of vehicular ad hoc network (VANET) and the possible challenges associated with such architecture.

### 1.3.1 Entities

A VANET comprises of three main entities: vehicles, roadside units (RSUs), and trusted parties (TPs). Each entity is described below.

#### 1.3.1.1 Vehicles

Vehicles are equipped with a communication device, known as onboard units (OBUs), which enable short-range wireless connection to facilitate communication between vehicles (V2V), and between vehicles and roadside infrastructures (V2I). This allows vehicles to broadcast safety- and traffic-related messages in VANETs. Moreover, it is commonly assumed in the literature (Chen et al., 2011; Wu et al., 2010; Raya & Hubaux, 2007; Kounga et al., 2009; Papadimitratos et al., 2009; He et al., 2015; C. Zhang, Lu, et al., 2008) that a tamper proof device (TPD), such as a black box is embedded within vehicles to provide secure storage for private keys of the vehicles. Even if an attacker is in possession of the TPD, the private keys will never be disclosed to the possessors. The TPD also performs cryptographic operation such as generating and verifying signatures.

#### 1.3.1.2 Roadside Units (RSUs)

Roadside units (RSUs) are stationary infrastructures located at some critical sections of the road, such as traffic lights, and intersections. One of its main roles is to facilitate the message announcement phase in VANETs. RSUs facilitate the announcement phase by performing revocation check on each vehicle that enters the RSUs communication range before generating new credentials for the vehicle (Wasef et al., 2008; Hao et al., 2011; L. Zhang et al., 2010; Zhu et al., 2014; Shao et al., 2016; Park et al., 2011). In addition, RSUs provide a gateway between vehicles and trusted parties to relay information in VANETs. Nevertheless, the presence of RSUs is not assumed in some schemes in the literature (Chen et al., 2011; Q. Li et al., 2012; Malip et al., 2014) since they may not widely be distributed in the first years of VANET deployment due to the costs for installation and administration (Raya & Hubaux, 2007; Xue et al., 2017).

#### 1.3.1.3 Trusted Parties (TPs)

The TPs are responsible for managing the admission and eviction of vehicles to the network. This includes managing cryptographic keys of vehicles, and revoking them in case of misbehaviour. The TPs are commonly referred to as certification authorities (CAs) (Papadimitratos et al., 2009; Kounga et al., 2009; Wasef et al., 2008; Park et al., 2011; Calandriello et al., 2007; Hao et al., 2011), trusted authorities (TAs) (Artail & Abbani, 2016; He et al., 2015; C. Zhang, Lu, et al., 2008; Zhu et al., 2014; Studer et al., 2009), and tracing managers (TMs) (Shao et al., 2016; Wu et al., 2010; L. Zhang et al., 2010) in the literature. In some schemes, the TP is known as a regional transportation authority (RTA) (Sun et al., 2010), an issuer (I) (Chen et al., 2011), a reputation server (RS) (Q. Li et al., 2012; Malip et al., 2014), and a membership manager (MM) (Lin et al., 2007). The TPs may interact periodically with vehicles in VANETs. When the TP is unreachable, roadside infrastructures (RSUs) may provide an alternative interaction between the TP and vehicles or an offline communication is assumed in the system (Chen et al., 2011).

### 1.3.2 Network Model

A Dedicated Short-Range Communication (DSRC), also known as Wireless Access in Vehicular Environments (WAVE), is adopted to support vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications in VANETs. DSRC which uses the standard IEEE 802.11p, operates in 5.9 GHz band with 75 MHz spectrum allocation from The US Federal Communications Commission (FCC) and 30MHz spectrum allocation from European Telecommunications Standards Institute (ETSI). Radio range of up to 1000m is supported by DSRC for vehicles to communicate in VANETs.

### 1.3.3 Characteristics

Similar to other kind of ad hoc networks, VANETs require short radio transmission range, self-organization, self-management and low bandwith of the nodes. There are several features that VANET can be distinguished from other ad hoc networks (F. Li & Wang, 2007; K. C. Lee et al., 2010). The network topology is highly dynamic and has short connection period due to the high speed movement of vehicles in VANETs. This leads to a frequent change of network topology which poses a considerable transmission overhead. Even though VANETs have highly dynamic topology, vehicular movements are predictable due to the constrains of roads, streets, highways, buildings, and traffic conditions. Furthermore, vehicles have higher energy and computational power which is provided by an embedded on-board unit.

### 1.3.4 Applications

VANETs applications are divided into two categories; safety applications and non-safety applications. Safety applications (J. F. Lee et al., 2010; Zhuang et al., 2011) aim to enhance road safety and traffic efficiency. Safety applications composed of safety-critical and safety-related. Some examples of safety-critical messages include collision avoidance, lane change warning, blind spot warning and sudden brake alert. Drivers should receive these information immediately in order to assess dangerous situations and react accordingly. On the other hand, safety-related messages such as traffic information and road condition has less time restriction.

Non-safety applications (Wischhof et al., 2005; Raya & Hubaux, 2007) aim to provide users infotainment, a combination of "information" and "entertainment", for a more pleasant traveling experience. Vehicles may utilize internet connectivity, electronic toll collection, and location based-services. For instance, drivers are able to locate nearest restaurants and free parking space with the help of location based services. This adds another benefits where drivers may save time from looking around places and thus reduce fuel consumption. In this thesis, we shall focus on safety application.

### 1.3.5 Vulnerabilities

Due to inherent wireless environment, VANETs are vulnerable to attacks when vehicles join the network. Before discussing types of attacks, it is necessary to identify the adversaries who perform the attacks as different security solutions are employed to combat different types of adversaries. The discussion is presented in the following subsection.

#### 1.3.5.1 Types of Adversaries

The presence of a small fraction of adversaries is a common assumption in VANETs (Wu et al., 2010; Lin et al., 2007; Malip et al., 2014; Q. Li et al., 2012; Chen et al., 2011; Golle et al., 2004; Papadimitratos et al., 2009). The adversaries can be categorised as internal and external adversaries which are defined as follows.

- **External Adversaries**. An external adversary is a malicious entity who does not possess valid credentials in VANETs. Most of external adversaries can be prevented by means of authentication and privacy protection. Authentication phase prohibits illegitimate vehicles from entering the network to pose threats on other vehicles. Meanwhile, privacy protection keeps the identity of each vehicle safe. An announcement scheme with an efficient authentication and a strong privacy protection in VANETs is able to keep the network safe from external attacks.

- **Internal Adversaries**. An internal adversary is a legitimate vehicle who possesses valid credentials. They may exploit their legitimacy to mislead other vehicles and cause damages in the network. This thesis focuses on the presence of internal adversaries as it poses higher risk than the external adversaries (Papadimitratos et al., 2009). Its presence is also a common assumption in the literature (Chen et al., 2011; Q. Li et al., 2012; Malip et al., 2014; Papadimitratos et al., 2009; Golle et al., 2004).

### 1.3.6 Types of Attacks

There are several types of possible attacks performed by adversaries in VANETs (Qu et al., 2015; Raya & Hubaux, 2007; Tyagi & Dembla, 2014). In this section, we provide some of the common attacks in the network, which the detailed descriptions of the attacks are given below.

- **Bogus Information**. Adversaries inject misleading messages into the network for personal benefits. For instance, an adversary creates false report about non-existence traffic congestion so that drivers divert from the routes and thus making the routes free for the adversary.
- **Denial of Service**. Adversaries make the network unavailable to vehicles in order to prevent them from accessing information. For instance, it floods the communication channel with irrelevant messages which congest the channel, eventually crashing the network and leads to disconnectivity.
- **Impersonation Attack**. Adversaries pretend to be a legitimate vehicle or a RSU

by stealing its identity and use the identity for illegal purposes. For example, an adversary who is involved in an accident, pretends to be another vehicle, say vehicle A to confuse the police and thus denying its guilt.

- **Sybil attack**. This attack is an advanced version of impersonation attack. Instead of impersonating one identity, an adversary forges multiple legitimate vehicles identities in the network to pose harmful threats. The adversary is able to use these multiple fake identities to perform any type of attacks in VANETs.

### 1.3.7 Security Requirement

VANET must consider a number of security requirements in order to ensure that vehicles can fully utilize its safety applications (Raya & Hubaux, 2007; Q. Li et al., 2012; Wu et al., 2010; Malip et al., 2014; Chen et al., 2011). Firstly, communication in VANETs must be trustworthy. A message is trustworthy if it is sent by legitimate vehicles without unauthorised modification. Furthermore, the message must reflect the actual situation. Secondly, the privacy of vehicles must be protected. Vehicles stay anonymous provided they have not misbehaved. Moreover, different messages generated by the same vehicle must be unlinkable to each other. Lastly, vehicles must be held accountable if they misbehaved in VANETs. These misbehaved vehicles can be traceable, assured the message originator and revokable from the network.

## 1.4 Revocation in VANETs

Revocation is one of the crucial security requirements in VANETs where it removes legitimate vehicles who is misbehaving (internal adversaries) from the network. VANETs must be resilient to internal adversaries in order to acquire public acceptance towards the deployment of this technology. The presence of external adversaries has no impact in the network as they do not possess valid credentials issued by the TP. These external adversaries who conduct an attack from outside the network can be prevented by means of authentication and privacy protection.

In this thesis, we focus on revocation as an attack from internal adversaries has more severe consequences than the external ones (Papadimitratos et al., 2009; Porwal et al., 2014). Moreover, we found that the importance of revocation has been neglected in some schemes (Wu et al., 2010; Artail & Abbani, 2016; He et al., 2015; C. Zhang, Lu, et al., 2008; C. Zhang, Lin, et al., 2008; Xi et al., 2007; Choi et al., 2005) in the literature where no revocation protocol is proposed in the system.

Revocation protocol must fulfill two properties in order to be practical. First, the revocation procedure should be integrated with other security requirements in VANETs. Second, an efficient revocation procedure is required as delay in revoking the misbehaved vehicles may open up the possibility for them to continue jeopardizing the safety of other vehicles. To meet these two requirements, various types of revocation protocols have been proposed by various cryptographic primitives in the literature. However, some existing revocation protocols may not be efficiently addressed or even suitably implemented by certain schemes. This rises the need to design a more efficient and practical revocation protocol in VANETs.

## 1.5 Scope and objectives of the Thesis

The scope of the thesis focuses on revocation protocol particularly for group signature schemes in VANETs. Adopting a secure and efficient revocation protocol in VANETs is a key requirement to the success of removing adversaries who may incur damages to the network. We propose a new revocation protocol for group signature schemes in VANETs. We show that our revocation protocol can be securely adopted in group signature schemes while achieving performance efficiency.

To achieve this goal, we have set the following objectives:

- to explore various revocation protocols adopted in some current schemes and discover a secure, efficient and comparable construction;
- to create an abstract formulation of revocation protocol particularly for group signature schemes in VANETs;
- to design a secure and efficient revocation protocol based on the formulated abstraction.

## 1.6 Organisation of the Thesis

This thesis consists of five chapters. Chapter 1 presents an introduction to this thesis, while the other chapters are organised as follows:

**Chapter 2 (Literature Review)**. This chapter analyses revocation protocols in some recent announcement schemes based on different cryptographic primitives in VANETs. We discuss the advantages and disadvantages of the protocols and summarize each protocol at the end of the section.

**Chapter 3 (Cryptographic Tools)**. In this chapter, we introduce the cryptographic primitive used in our work, that is, group signature. Then, we provide some mathematical background underlying the construction of our work in the thesis.

**Chapter 4 (Revocation Protocol for Group Signature Schemes in VANETs)**. In this chapter, we design a generic abstraction of revocation protocols for group signature. This abstraction then serves as a guideline for our new revocation protocol for group signature schemes in VANETs. Analysis shows that our revocation protocol achieves comparable performance to the existing schemes in the literature. The work presented in this chapter has been submitted to an ISI Journal as stated below:

- N.F. Mohd Shari, A. Malip and W.A. Mior Othman. Revocation Protocol for Group Signatures in VANETs: A Secure Construction, “ International Journal of

Communication Systems," 2017 (submitted).

**Chapter 5 (Conclusion and Future Work)**. This chapter summarizes our contributions and we discuss some future directions of the research.

# CHAPTER 2: LITERATURE REVIEW

*This chapter reviews revocation protocols based on various cryptographic primitives in VANET. We discuss the advantages and shortcomings of each revocation protocol under each cryptographic primitive. We then summarize and examine the extent of security of these revocation protocols.*

## 2.1 Reviews of Revocation Protocols

In this section, we review revocation protocols designed using different cryptographic primitives, including "traditional" public key cryptography, identity-based cryptography, symmetric key cryptography, reputation-based, and group signature. We examine multiple schemes under each primitive to analyse the variation of the revocation protocols. We then discuss the advantages and shortcomings of each revocation protocols.

### 2.1.1 Revocation in "Traditional" Public Key Cryptography

"Traditional" public key cryptography (PKC) is the most commonly used primitive to provide security in VANETs (Hasrouny et al., 2017). It uses two unidentical but mathematically related keys; one is the public key and the other is the private key. The public key is made known to everyone in the network while the private key is kept secret. A public key is associated to a user by a certificate, which is the signature of the trusted party (TP) on the public key. This certificate indicates that the public key is authentic where it belongs to a specific user in the network. There are two types of certificates used in the "traditional" PKC; long-term certificates and short-term certificates (Schoch, 2012). The long-term certificate may contain vehicle's identity while the short-term certificate (also known as pseudonym) does not contain any identifiers associated with a particular user. The TP stores all the issued certificates to allow traceability in case of misbehaviours. We review some revocation protocols based on the "traditional" public key cryptography in (Artail & Abbani, 2016; Kounga et al., 2009; Papadimitratos et al., 2009; Wasef et al., 2008) and discuss their advantages and limitations.

#### 2.1.1.1 A pseudonym management system to achieve anonymity in vehicular ad hoc networks

Artail and Abbani (2016) proposed a pseudonym management system to achieve anonymity in VANETs. Each vehicle initially receives its public and private key pairs, and long-term certificates from the TP during the registration phase. RSUs are involved in message broadcast phase by receiving a set of pseudonyms from the TP, and distributing the received pseudonyms to vehicles who enter its communication range. The vehicle then uses the pseudonyms to communicate with each other in the network. The RSU shuffles the set of pseudonyms with each other under a predefined shuffling period so that the sets can be reused by different vehicles in order to limit the burden of the TP who needs to generate new sets of pseudonyms, as well as to maximize anonymity. However, this scheme does not mention any revocation protocol in the construction. It only focuses on improving the system of generating, distributing and replenishing the pseudonyms to achieve a sufficient level of anonymity.

#### 2.1.1.2 Proving Reliability of Anonymous Information in VANETs

Kounga et al. (2009) proposed an announcement scheme for VANET based on the "traditional" public key cryptography. This scheme focuses on V2V communication as it does not assume the availability of RSUs in its construction. Each vehicle generates its own public and private key pairs, together with the certificates to broadcast safety messages using a unique secret key preloaded in the vehicle’s tamper-proof device. This method reduces the management overhead to the TP since it does not need to manage huge number of certificates per vehicle. Its revocation protocol is based on the traditional method of revoking certificates, that is, the distribution of certificate revocation lists (CRLs) which contain a list of revoked certificates. The revocation is described as below.

- **Database Lookup**. The TP issues, updates, and distributes the CRL across the network. A message receiving vehicle checks the CRL by performing a database lookup in order to determine revocation status of a sender's certificate. The receiving vehicles will reject the message from the sender if they found a match against the CRL, resulting in the eviction of such misbehaved vehicle from the network. If the receiving vehicle experiences any misbehaviours, it may lodge a report and send it to the TP who later verifies the report and updates the CRL.

**Discussion**. The advantage of using the CRL database lookup for revocation is that the method is efficient if there are a few revoked vehicles exist in the network. However, the CRL size is expected to be very large in a large scale VANET. This protocol will cause computational burden on receiving vehicles when a large number of revoked vehicles exist in the CRL. This leads to long delay of message verification in VANETs.

#### 2.1.1.3 Secure Vehicular Communication Systems: Design and Architecture

Papadimitratos et al. (2009) proposed a secure and privacy-enhancing VANET announcement scheme based on the "traditional" public key cryptography. Each vehicle obtains a pair of public and private keys, together with certificates when it registers with the TP. In order to announce safety messages, the vehicle regularly requests for a set of pseudonyms from the TP using the key pairs via a secured communication channel. Even though the involvement of RSUs is not needed during message broadcast between vehicles, its involvement is required in the revocation phase. This scheme adopts the CRL database lookup in conjunction with some additional methods for revocation. Each protocol is given as follows.

- **Database Lookup**. The TP distributes the updated CRLs across the network. Instead of the TP as in (Kounga et al., 2009), this scheme relies on the RSUs to distribute the CRLs. A receiving vehicle uses the received CRLs to perform a revocation check in order to verify if the sending vehicle is revoked or not. If there is a match of identity against the CRL, the receiving vehicle will reject the message from the sender, who then no longer be able to participate in the network.

- **Revocation protocol of tamper-proof device (RTPD)**. In this scheme, the TP initiates the revocation by sending a revocation message to a particular misbehaved vehicle. Upon receiving the message that has been encrypted with the vehicle's public key, the tamper-proof device (TPD) of the vehicle decryptes the message and erases all stored keys so that the vehicle would no longer be able to sign safety messages. The distribution of the message from the TP to the vehicle's TPD takes place in several options. First, if the location of the vehicle is known to the TP, the message will be sent to the RSU that is closest to the targeted vehicle. Second, if the TP does not know the exact location, it retrieves the most recent location of the vehicle, defines a paging area consisting of several RSUs covering these locations, and sends the revocation message to these RSUs. Lastly, if recent location entries could not be found, the revocation message is broadcasted via the low-speed FM radio.

- **Revocation protocol using compressed certificate revocation lists (RCCRL)**. RCCRL is performed when the TPD of a vehicle is unreachable, where an attacker blocks a revocation message, for instance. In this protocol, the size of CRL is compressed using a probabilistic data structure, notably a bloom filter (Bloom, 1970), to reduce communication and storage overhead in managing the CRL. Instead of storing a full copy of each certificate, the bloom filter provides a space-efficient data structure to represent an element, thus making the size of CRL to be small. The TP broadcasts the compressed CRLs across the network via the RSUs. The rest of the process runs similarly to the CRL database lookup.

- **Distributed revocation protocol (DRP)**. The DRP is composed of a misbehavior detection system (MDS) and a local evicition of attackers by voting evaluators (LEAVE). The objective of both MDS and LEAVE is to allow neighbouring vehicles defending themselves by temporarily revoking the misbehaved vehicles in the network. In MDS, each vehicle is equipped with a misbehaviour detection system (Golle et al., 2004) to identify any misbehaved vehicles in the network. Once a misbehaved vehicle has been identified, it executes the LEAVE where the neighbouring vehicles will accumulate accusations against the identified misbehaviours, broadcast warning messages to all vehicles in range, and report the accusations to the TP once they reach an RSU point.

**Discussion.** This scheme adopts multiple revocation protocols in order to diminish any possible vulnerability windows in VANETs. However, RSU involvement is required in all protocols. The reliance of RSUs may lead to scalability problem as the existence of pervasive RSUs is not realistic particularly in the intial stage of VANET deployment (Xue et al., 2017). This is because installing and maintaining a relatively large number of RSUs imposes sufficiently high costs on developers (Raya & Hubaux, 2007).

#### 2.1.1.4 ECMV: Efficient certificate management scheme for vehicular networks

Wasef et al. (2008) proposed an efficient certificate management scheme (ECMV) based on the "traditional" public key cryptography. This scheme supports hierarchical architecture which has a master authority (MA) as a centralised authority and several regional TPs working with the RSUs for effective management. Each vehicle receives a short-lifetime certificate that requires frequent update from the RSUs. Revocation protocol in this scheme is based on the database lookup but it is adopted in a different setting, which is described below.

- **Database Lookup (RSU Reliance)**. Given the validity period of certificate is short enough, this scheme suggested that the CRL database lookup during message verification phase is unnecessary. Instead, the TP distributes certificate revocation list (CRLs) to the RSUs who will check the revocation status of each vehicle that requests for a new certificate. A misbehaved vehicle is unable to continue its participation in the network when its request of obtaining new certificates is rejected by the RSUs.

**Discussion**. The efficiency of CRL database lookup only occurs when the revocation list is sufficiently small. However, this is unlikely to happen because the list is expected to be large in the high density vehicular environment. On the other hand, the short lifetime certificate may create some vulnerability issues as a misbehaved vehicle is able to jeopardize the safety of other vehicle before the certificate expires. In order to keep the vulnerability window very small, a more frequent communication with the RSUs is required for prevention purposes.

### 2.1.2 Revocation in Identity-based Cryptography

An identity-based cryptography is a variant of public key cryptography (PKC) introduced by Shamir (1984) to reduce the computation and communication overheads associated with certificates management in the "traditional" PKC. In this primitive, the identity of each vehicle, such as an email address or a phone number is used as a public key to replace the use of certificates in announcing safety messages. A trusted party (TP) is required to compute a private key that corresponds to a particular public key. This TP has to be completely trusted as it is in possession of the vehicles private keys. We review revocation protocols based on identity-based schemes in (He et al., 2015; Sun et al., 2010; C. Zhang, Lu, et al., 2008).

#### 2.1.2.1 An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks

He et al. (2015) proposed an identity-based conditional privacy-preserving authentication scheme for VANETs. The conditional privacy allows the TP to retrieve the real identity of a vehicle in case of misbehaviours. Each vehicle is equipped with a tamper-proof device (TPD), which is used to generate pseudo-identities from the real identity of the vehicle preloaded into the device by the TP. The vehicle then uses the pseudo-identities to broadcasts safety messages in VANETs. Even though this scheme is able to detect misbehaviours, it does not further address revocation protocol to remove such misbehaved vehicles from the network.

#### 2.1.2.2 An identity-based security system for user privacy in vehicular ad hoc networks

Sun et al. (2010) proposed the use of identity-based cryptography for privacy-preserving scheme in VANETs. To broadcast a message, each vehicle has to submit its real identity to the TP during registration, and in return it receives a pool of pseudo-identities. This pseudo-identities will be replenished frequently through the regional RSUs to preserve privacy. Revocation protocol in this scheme is similar to the traditional distribution of CRLs, described below.

- **Database Lookup**. The only difference between this revocation and the CRL database lookup is it replaces certificates with pseudo-identities in the revocation list (RL). The TP distributes the pseudo-identity revocation list (RL) across the network via the RSUs. A message receiving vehicle uses the pseudo-identity RL during message verification phase to check revocation status of a sender. The receiving vehicle will reject the message if the database shows a match of identity, thus removing the misbehaved vehicle from the network.

**Discussion**. The merit of this protocol is that vehicles only need to store the pseudo-identities, which save the storage space required for certificates. Therefore, it is more efficient to manage the pseudo-identity RL as it can reduce communication and storage overhead on vehicles. However, relying solely on this revocation method is still inefficient particularly when a large number of revoked vehicles exists in VANETs.

#### 2.1.2.3 An efficient identity-based batch verification scheme for vehicular sensor networks

C. Zhang, Lu, et al. (2008) proposed an identity-based batch verification scheme to address the communication overhead incurred during message verification process. A tamper-proof device (TPD) is used to generate pseudo-identities for a vehicle based on the vehicle's real identity. The generation of pseudo-identities can be done offline by the tamper-proof device to avoid communication delay if vehicles run out of their pseudo-identities. Misbehaved vehicles are traceable by a trust party (TP) in this scheme but no technique has been discussed on how to revoke such vehicles from the network.

### 2.1.3 Revocation in Symmetric Key Cryptography

The symmetric key cryptography is an approach that requires an establishment of pairwise symmetric keys during authentication phase since the same key is used for both encryption and decryption procedures. This primitive is more efficient than the "traditional" PKC in terms of computation overhead as it requires low computational complexity. However, vehicles have to authenticate each other frequently via trusted parties (TPs) in the key establishment phase. Furthermore, the trusted parties must be online all the time to establish symmetric keys. We review revocation protocols in some schemes (C. Zhang, Lin, et al., 2008; Xi et al., 2007; Choi et al., 2005) based on the symmetric key.

#### 2.1.3.1 RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks

C. Zhang, Lin, et al. (2008) proposed an RSU-aided message authentication scheme for VANETs based on the symmetric key cryptography. In this scheme, each vehicle initiates a mutual authentication process with the RSUs and receives a unique shared symmetric key during the process. Using the symmetric key, the vehicle generates a symmetric hash message authentication code (HMAC) to sign safety messages. The RSU who has the HMAC encryption keys is responsible to verify the authenticity of the message by computing a matching HMAC and distribute the authentication results back to message receiving vehicles. This scheme does not mention any revocation protocol in its construction. It only focuses on addressing the issue of communication overhead during message verification in VANETs.

#### 2.1.3.2 Enforcing privacy using symmetric random key-set in vehicular networks

Xi et al. (2007) proposed a privacy-preserving authentication scheme for VANETs based on the symmetric key cryptography. In this scheme, each vehicle draws a set of symmetric random key from a central shared key pool. A set of keys is used for authentication in order to preserve the privacy of a vehicle. This is because there is a high probability that each random key in the set is shared by multiple vehicles so that tracking of vehicles would become difficult. The limitation of this scheme is that a frequent interaction between vehicles and RSUs is required for symmetric key authentication every time vehicles enter a new RSU's range. Revocation is discussed in this scheme, but no explicit mechanism is presented. It is mentioned that the details of revocation will become the starting point for future work.

#### 2.1.3.3 Balancing auditability and privacy in vehicular networks

Choi et al. (2005) proposed the use of symmetric key cryptography to balance the requirement of privacy and auditability in VANETs. This scheme combines the symmetric key authentication with the use of short-term pseudonyms. Each vehicle obtains short-term pseudonyms whenever it enters a RSU domain. The vehicle uses these pseudonyms to generate messages for V2V communication. The limitation of this scheme is similar to the limitation in (Xi et al., 2007), where vehicles are required to frequently authenticate each other using the symmetric key via the RSUs in order to obtain the pseudonyms. Revocation protocol is not addressed in this scheme. A misbehaved vehicle is traceable but no further action has been discussed to revoke the vehicle from the network.

### 2.1.4 Revocation in Reputation-based Models

A reputation-based model is adopted to evaluate message reliability in VANETs. A message is considered reliable if a vehicle who generates the message has a sufficiently high reputation score. The reputation score is computed based on the recommendation given by surrounding vehicles and RSUs. For instance, the recommenders give higher reputation for vehicles who provide correct messages about congestion and accidents. We review revocation protocol in (Malip et al., 2014; Q. Li et al., 2012; Park et al., 2011) based on the reputation-based system.

#### 2.1.4.1 A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks

Malip et al. (2014) proposed a centralised reputation-based announcement scheme to achieve message reliability for VANETs. The reliability of a message is reflected by a reputation score that is computed based on feedbacks reported by receiving vehicles in the network. The higher the reputation score, the more reliable the message generated by a vehicle. Positive feedbacks due to reliable messages increase the reputation score and vice versa. Each vehicle periodically renew its reputation credential from the TP and generates its own pseudonymous key pair which is used to sign a message. This scheme is an extension to the previous work in (Q. Li et al., 2012). The novelty of this scheme lies in its adoption of a certificateless signature to address the requirement of privacy that is not fulfiled in (Q. Li et al., 2012). Revocation protocol in this scheme is described as follows.

- **Implicit revocation**. Revocation is achieved implicitly in this scheme as the revocation technique is embedded within the construction. A vehicle whose reputation score decreases to 0 or a certain threshold will be revoked from the network. The TP will stop providing this misbehaved vehicle with a new reputation credential in the future. Therefore, this vehicle will not be able to continue its participation in the network. Note that the old reputation credential will expire gradually after a certain period of time.

**Discussion**. The advantage of this protocol is that, no additional mechanism is required to achieve revocation, thus reducing computational burden on the system. However, vulnerability may arise before an old credential expires as a misbehaved vehicle can cause harm to other vehicles until the end of its certificate lifetime.

#### 2.1.4.2 A reputation-based announcement scheme for VANETs

Q. Li et al. (2012) proposed a centralised reputation-based announcement scheme for VANETs which uses the same reputation system as that of (Malip et al., 2014). However, in this scheme, a vehicle is not required to authenticate itself periodically to the TP since it uses reputation certificates that are not confidential. The revocation protocol is similar to the protocol in (Malip et al., 2014) since it addresses the same reputation system. The protocol is given as follows.

- **Implicit revocation**. A vehicle is revoked from the network if its reputation score decreases to 0 or a certain threshold. The revoked vehicle is then unable to retrieve a new reputation certificate from the TP. Meanwhile, the previously issued certificates will be expired as time elapses. This is an act of implicit revocation because no explicit mechanism is required to remove the misbehaved vehicles from the network.

**Discussion**. This scheme has less computational burden since revocation mechanism is "embedded" within the construction. However, the revocation may open up some vulnerabilities issues since a misbehaved vehicle can cause harm to other neighbouring vehicles before its previously issued certificate expires.

#### 2.1.4.3 Long-term reputation system for vehicular networking based on vehicle's daily commute routine

Park et al. (2011) proposed a long-term reputation system that relies on the RSUs to determine vehicles reputation scores based on its daily behaviour since each vehicle is assumed has its predefined commute route. The RSU issues reputation certificates to each vehicle in its region, which is used to sign safety messages in the network. The reputation certificate is updated and distributed daily to prevent unlawful tracing. Revocation protocol is similar to the traditional method of revoking certificates since this scheme adopts the use of certificates in the construction. The protocol is described as follows.

- **Database Lookup (RSU Reliance)**. A revocation list that contains revoked reputation certificates for each revoked vehicle is distributed in the network. The RSUs who receive the revocation list will run the database lookup to match the certificates for revocation. Once a match of certificate is found, the RSUs will stop generating a new certificate for the revoked vehicle who is then, unable to continue its participation in the network.

**Discussion**. This revocation is efficient if small number of misbehaved vehicles are present in the network. However, in a large VANET environment, the possibility of misbehaviours increases as the vehicle density increases, which may render the revocation protocol inefficient.

### 2.1.5 Revocation in Group Signatures

A group signature scheme allows a member of the group to sign messages on behalf of the group without the member's identity being revealed to the receiver. Each vehicle is equipped with a group user key, which is used to sign and broadcast messages. The signatures are anonymous and unlinkable, but a trusted party (TP) has the ability to identify them in case of dispute. We review revocation protocols in some schemes (Shao et al., 2016; Calandriello et al., 2007; Studer et al., 2009; Chen et al., 2011; Lin et al., 2007; Wu et al., 2010; Hao et al., 2011; L. Zhang et al., 2010; Zhu et al., 2014) based on group signatures and evaluate their advantages and shortcomings.

#### 2.1.5.1 A threshold anonymous authentication protocol for VANETs

Shao et al. (2016) proposed a threshold anonymous authentication protocol for VANETs in a decentralized group model by using a new group signature scheme. The proposed new group signature achieves traceability where the TP reveals a misbehaved signer's identity at an efficient computational cost. In the decentralized group model, the whole network is divided into several domains which is managed by an RSU in each domain. The RSU issues a group certificate to each legitimate vehicle within its communication range that is used to sign messages in VANETs. Revocation in this scheme uses the database lookup method to remove misbehaved vehicles from the network. The protocol is given as follows.

- **Database Lookup (RSU Reliance)**. The TP issues and distributes the most current certificate revocation list (CRL) to the RSUs. When a vehicle enters a new RSU domain, the RSU performs database lookup on the CRL (before issuing a group certificate to the vehicle) to check whether the vehicle exists in the RL or not. If yes, the vehicle will be rejected from getting a group certificate, thus unable to join the network. If dispute arise while a vehicle is in possession of a group key, a receiving vehicle is able to determine if different signatures on the same message are generated by the same signer, and report the event to the TP for tracing purposes.

**Discussion**. This protocol does not require vehicles to perform revocation check during message verification phase. However, the availability of RSUs who take over the workload may not be adequate to manage all vehicles within their domains, particularly during the first few years of network deployment.

#### 2.1.5.2 Efficient privacy-preserving authentication for vehicular ad hoc networks

Zhu et al. (2014) proposed a privacy-preserved authentication scheme in VANETs based on the group signature to improve the previous work in (Zhu et al., 2013). This scheme addresses a semi-trust model of RSUs, where the issue of compromised RSUs is considered. A compromised RSU will be identified and revoked during mutual authentication between the RSU and vehicles who enter the domain based on revocation information sent by the TP to the vehicles. Each vehicle who has been authenticated upon entering the same RSU's domain receives the same group key seed to compute a group key. Vehicles that receive the same group key from the same RSU form a group. A hash message authentication code (HMAC) value will be computed using the group key and attached in each message sent by the vehicle. When a receiving vehicle receives a message, it performs a HMAC checking. Only messages from valid vehicles will be accepted since revoked vehicles could not generate correct HMACs. Revocation in this scheme is described as follows.

- **Database Lookup (RSU Reliance)**. The inability of revoked vehicles to generate valid HMACs is because RSUs have filtered them from joining the network. The RSU uses the revocation lists distributed by the TP to check the revocation status of each vehicle passes by its domain before issuing group key seed to the vehicle. Revoked vehicles whose identity is in the list would not be able to receive the group key seed, hence unable to participate in the network.

**Discussion**. Checking the HMAC, which is shared between non-revoked vehicles is able to minimize the computational burden of performing CRL revocation check during message verification phase. This is because the size of the HMAC is smaller than the size of the certificate. However, the revocation check is still performed by the RSUs whenever a vehicle request for a group key seed. The reliance on RSUs to check the vehicle revocation status may pose a scalability issue since adequate number of RSUs may not be available in the initial deployment phase of VANET.

#### 2.1.5.3 A distributed key management framework with cooperative message authentication in VANETs

Hao et al. (2011) proposed a distributed key management scheme based on the group signature. This scheme allows neighbouring vehicles to cooperatively authenticate messages in order to reduce computation overhead during message verification. Semi trusted RSUs are responsible in distributing short-term group keys to vehicles every time they enter the RSU communication range. Vehicles who receive the same group key from the same RSU will be assigned to be in a same group. In case of dispute, compromised RSUs and malicious vehicles can be traced and revoked in this scheme. The revocation protocol is described as follows.

- **Database Lookup (RSU Reliance)**. When a vehicle drives into an RSU domain, the RSU checks the vehicle's revocation status before issuing it a group key. Using a revocation list (RL) distributed by the TP, the RSU performs the database lookup to find a match of identity. The RSUs will reject the vehicle request to acquire a group key if they found a match against the RL. Failure to obtain a new group key from the RSU resulting in eviction of the misbehaved user from the network.

**Discussion**. The reliance on RSUs can reduce the computation overhead of vehicles to perform revocation check during message verification phase especially in a high density VANET. However, there will be insufficient numbers of RSUs being installed in the early stage of VANET due to high installation and administrative cost. An inadequate number of RSUs to perform revocation check within their domains may lead to scalability problem.

#### 2.1.5.4 Threshold anonymous announcement in VANETs

Chen et al. (2011) proposed a threshold anonymous announcement (TAA) scheme for anonymous authentication in VANETs. This scheme adopts and combines direct anonymous attestation (DAA) and $k$-time anonymous techniques to achieve goals of reliability, privacy and auditability. The DAA technique functions like a group signature scheme without the ability to trace the signer of a signature. Meanwhile, the $k$-time anonymous technique fulfill the traceability requirement as it allows a user's identity to be revealed by the TPs if a vehicle attempts to sign the same message more than $k$ times. Revocation in this scheme are based on two methods; which are:

- **Database lookup**. In group signature, revocation check is performed by message receiving vehicles is called verifier-local revocation (VLR), introduced by Boneh and Shacham in (Boneh & Shacham, 2004). The TP distributes the updated revocation list (RL) across the network which is then used by the receiving vehicle to run database lookup upon receiving a message from a sender. The receiving vehicles will reject the message from the sender if they found a match of identity against the RL. This prevents misbehaved vehicles from joining the network.

- **Credentials Update**. This method is executed when the number of revoked vehicles in the RLs exceeds a predefined threshold. Both TPs and vehicles' credentials are updated in this scheme since issuer's key is used by the verifying vehicles during the message verification phase. The TP initiates the revocation by updating its key and updating unrevoked vehicles' credentials. To update the keys, communication between vehicles and the TP may be required at intervals since this scheme does not entirely assume the availability of RSUs. Vehicles may also interact with the TP during regular maintenance visit or at VANET service points. The TP publishes its new public key and makes the new credentials available to the vehicles. The revoked vehicles would not have their credentials updated. This prevents them from further participation in the network as their signatures would not be valid under the new TP's key.

**Discussion**. This revocation protocol adopts an additional method in conjunction with VLR for an efficient revocation. This adoption is crucial because VLR should not be used alone as it is known to be inefficient when a large number of revoked vehicles exist in the revocation list.

#### 2.1.5.5 Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications

Wu et al. (2010) proposed a message-linkable group signature (MLGS) scheme that preserves vehicle's safety and privacy in VANETs. The MLGS is a variant of group signatures where linkability feature is adopted in order to distinguish the signature generated by the same signer on the same message. This adoption enables malicious vehicles who sign the same message more than once to be linked and traced. This scheme discusses the importance of revocation, that is, to prevent misbehaved vehicles from compromising public safety. Although the misbehaved vehicles are traceable in MLGS, no explicit mechanism is presented to revoke them from the network.

#### 2.1.5.6 A scalable robust authentication protocol for secure vehicular communications

L. Zhang et al. (2010) proposed a scalable robust authentication scheme based on the group signature in VANETs. In this scheme, each vehicle request for a group key from a RSU using a signcryption method (Zheng, 1997) upon entering the RSU communication range. The method allows a sender to sign and encrypt a message at the same time which takes less computational time than to sign and encrypt the message separately. Revocation in this scheme relies on RSU to perform the revocation check, described as follows.

- **Database Lookup (RSU Reliance)**. The TP issues, updates and distributes the revocation list to RSUs for revocation check operation. Upon receiving a request from a vehicle who enters RSU communication range, the RSU uses the list to check the vehicle revocation status. If there is no identity matched, RSU will issue the vehicle a group key to be used for signing messages. Otherwise, the request will be discarded, as it indicates that the request is generated from a revoked vehicle.

**Discussion**. Since RSUs are responsible for the revocation check operation, message verification phase becomes more efficient. However, RSUs may not be densely installed in the early stage of VANET deployment, thus, relying on RSUs to manage and perform revocation check will be infeasible.

#### 2.1.5.7 Tacking together efficient authentication, revocation, and privacy in VANETs

Studer et al. (2009) proposed a TACK scheme in VANETs based on the group signature. In this scheme, a RSU acts as an intermediary authority in its region by issuing a temporary anonymous certified key (TACK) for vehicles upon request. When a vehicle enters a region, it signs a TACK request with a group signature to prove its authenticity and sends the request anonymously to the RSU. The issued TACK is only valid for a short period of time in a specific region to be used by the vehicle for V2V communication. Revocation in this scheme is similar to the database lookup protocol with no reliance on RSU. It is defined below.

- **Database lookup**. Similar to the first revocation method in (Chen et al., 2011), this revocation is known as VLR as revocation check is performed by message receiving vehicles in group signature. Using the revocation lists distributed by the TP, the receiving vehicle checks revocation status of a sender. Revoked vehicles whose identity is in the list will be rejected from further joining the network.

**Discussion**. It is computationally inefficient to solely rely on VLR for revocation as it poses a burden on vehicles during message verification phase when a large number of revoked vehicles exists in the revocation list.

#### 2.1.5.8 GSIS: A secure and privacy-preserving protocol for vehicular communications

Lin et al. (2007) proposed GSIS scheme that is based on group signature and the identity-based signature for secure and privacy-preserving protocol in VANETs. The group signature is adopted to secure the communication between vehicles (V2V) whereas the identity-based is used in between vehicles and infrastructures (V2I). RSU involvement is assumed in this scheme only to relay information such as to announce key update in executing revocation. This scheme proposes a hybrid membership revocation mechanism. VLR is adopted when revoked vehicles are less than a predefined threshold, meanwhile, credential update is used once it exceeds the threshold. This is similar to the revocation in TAA scheme (Chen et al., 2011) described earlier.

- **Database lookup**. The TP distributes the updated revocation list across the network. A message receiving vehicle performs revocation check by using the received CRLs to verify if the sending vehicle is revoked or not. If yes, the message will be discarded and the revoked vehicle would no longer be able to participate in the network.
- **Credentials Update**. Unlike TAA, GSIS requires only vehicles' credentials to be updated. The TP initiates the revocation by updating unrevoked vehicles' credentials. The new credentials are then made available to the vehicles. The revoked vehicles would not have their credentials updated, thus unable to continue generating valid signature.

**Discussion**. This scheme adopts two methods of revocation to enhance efficiency. This adoption is important because using VLR alone is not feasible to cater for high density network with a large number of revoked vehicles.

#### 2.1.5.9 Efficient and robust pseudonymous authentication in VANET

Calandriello et al. (2007) proposed a hybrid approach based on the group signature and PKC. In this scheme, a vehicle generates its own pseudonyms, which are public keys that does not reveal the vehicle's identity. A vehicle signs the self-generated pseudonyms using a group user key equipped in each vehicle by the TP, which essentially self certifying the pseudonyms. Revocation in this scheme is similar to the traditional distribution of CRLs to the verifiers which is a known as VLR in group signature. The protocol is described as follows.

- **Database lookup**. The TP issues and distributes the most recent revocation list across the network. A message receiving vehicle performs database lookup on the list to check whether the sender of the message exists in the list or not. The sender will be removed from the network if its identity is in the list.

**Discussion**. This protocol is efficient if the number of revoked vehicles is small in the revocation list. However, since the size of the list is expected to be large in a high density VANET, this revocation will lead to computation overhead to the receiving vehicles who need to verify received messages in VANETs.

## 2.2 Conclusion

We have presented an extensive analysis of different revocation protocols deployed in some recent announcement schemes based on various cryptographic primitives in VANETs in Section 2.1. We thoroughly discussed the advantages and limitations of each revocation protocol. We then summarize the adoption of these revocation protocols in Table 2.1. The "√" implies that revocation is achieved while the "X" implies the absence of revocation protocol in the system. The summary of different types of revocation protocols being adopted in different cryptographic primitives is depicted below:

- **Database Lookup.** The most common technique to revoke misbehaved vehicles is by running a database lookup on a distributed revocation list. This approach is adopted in "traditional" PKC, identity-based cryptography, reputation-based model and group signature. An entity who performs the database lookup may be a message receiving vehicle or a roadside infrastructure (RSU). The message receiving vehicle runs the database to perform message verification. Meanwhile, the RSU runs the database when authenticating vehicles that enter its domain. We denote this as **'database lookup (RSU reliance)'**. A revoked vehicle is filtered from joining the network when its identity is on the revocation list. The limitation of database lookup is its efficiency reduces as the revocation size gets larger.

| Primitives | Schemes | Revocation | Type of Protocols |
|---|---|---|---|
| "Traditional" PKC | Artail and Abbani (2016) | X | - |
| | Kounga et al. (2009) | √ | Database Lookup |
| | Papadimitratos et al. (2009) | √ | Database Lookup, RTPD, RCCRL, DRP |
| | Wasef et al. (2008) | √ | Database Lookup (RSU Reliance) |
| Identity-Based | He et al. (2015) | X | - |
| | Sun et al. (2010) | √ | Database Lookup |
| | C. Zhang, Lu, et al. (2008) | X | - |
| Symmetric Key | C. Zhang, Lin, et al. (2008) | X | - |
| | Xi et al. (2007) | X | - |
| | Choi et al. (2005) | X | - |
| Reputation-based | Malip et al. (2014) | √ | Implicit Revocation |
| | Q. Li et al. (2012) | √ | Implicit Revocation |
| | Park et al. (2011) | √ | Database Lookup (RSU Reliance) |
| Group Signature | Shao et al. (2016) | √ | Database Lookup (RSU Reliance) |
| | Zhu et al. (2014) | √ | Database Lookup (RSU Reliance) |
| | Hao et al. (2011) | √ | Database Lookup (RSU Reliance) |
| | Chen et al. (2011) | √ | Database Lookup, Credentials Update |
| | Wu et al. (2010) | X | - |
| | L. Zhang et al. (2010) | √ | Database Lookup (RSU Reliance) |
| | Studer et al. (2009) | √ | Database Lookup |
| | Lin et al. (2007) | √ | Database Lookup, Credentials Update |
| | Calandriello et al. (2007) | √ | Database Lookup |

**Table 2.1:** Summary of Revocation Protocols

- **Credentials Update.** This revocation protocol is commonly adopted in group signature as an additional protocol to address the limitation of database lookup operation. The TP announces credentials update operation when the size of revocation list exceeds a predefined threshold. A revoked vehicle is unable to join the network when its credential would not be updated by the TP which prevents the revoked vehicle from continuing generate valid signature.
- **RTPD, RCCRL, DRP.** These three protocols were introduced by (Raya et al., 2006) in "traditional" PKC since the efficiency of standard method to revoke certificate is arguable. RTPD requires the system to be able to locate a revoke vehicle before

deleting all its keys. RCCRL uses a compression technique on revocation list to reduce the size of CRL but it poses an overhead associated with compression processing time (Mitzenmacher, 2002). DRP allows neighbouring vehicle to detect any misbehaviours and temporarily revoke the misbehaved vehicles when the number of accumulated accusations exceeds a threshold.

- **Implicit Revocation.** Reputation-based model has an advantage to adopt implicit revocation in its system. Without the need of explicit mechanism, a vehicle is eventually revoked from the network when its reputation score decreases to zero or below a certain threshold deemed as low. A poor reputation score reflects that the vehicle has announced unreliable messages in the past. The TP will stop issuing new credentials for the revoked vehicle so that it would not be able to continue its participation in the network.

Furthermore, our review found the lack of revocation protocol being addressed in some of the schemes based on "traditional" public key, identity-based, symmetric key, and group signature, which denoted by – in Table 2.1. This gap in the literature implies that there are more rooms for future research.

We choose to address the gap of revocation in group signature over "traditional" PKC, identity-based and symmetric key due to various reasons. One of the reasons is the level of security and efficiency that group signature can provide compared to other cryptographic primitives. "Traditional" PKC poses a heavy burden on the TP to have large amount of storage and computing time in order to manage vehicular certificates. Meanwhile, identity-based cryptography who aims to solve the certificate management issue in "traditional" PKC suffers key escrow problem. The TP has to be completely trusted as it is in possession of the vehicles private keys. Lastly, it is undeniable that symmetric key is efficient in terms of computation overhead but it requires a frequent interactions between the TP and vehicles in the key establishment phase, which may not be feasible in a fast moving vehicles in VANETs. Even though group signature involves expensive computation, the level of security and safety over computation cost is more appealing in order to make VANET beneficial to vehicles. Therefore, our work steps in to fill in the gap of revocation for group signatures.

# CHAPTER 3: CRYPTOGRAPHIC TOOLS

*In this chapter, we review the cryptographic primitive used in our work, particularly, group signatures. Then, we present the mathematical backgrounds required for the understanding of cryptographic tools used in this thesis.*

## 3.1 Group Signatures

A group signature, proposed by Chaum and van Heyst (1991) is a cryptographic primitive based on digital signature. It extends the "traditional" digital signature concept to a multi-party setting (Ramzan, 1999). It allows a member of a group to sign a message on behalf of the group without revealing which individual in the group signed the message. The verifier of the message can verify the validity of the signature but is not able to know who produced the signature. A group signature scheme consists of numerous group members and a group manager. The group manager is responsible for the formation of groups and has the ability to trace the identity of the group member in case of dispute.

### 3.1.1 Phases

A group signature scheme is composed of the following phases (Ateniese et al., 2000):

- **Setup**: This is the initial phase where the group manager chooses some security parameters and uses a probabilistic algorithm to calculate and get the group public key and the private key of the group manager.
- **Join**: In this phase, a user registers with the group manager to become a new group member. The user chooses its secret key and sends it to the group manager. The group manager then outputs a membership certificate to the user who becomes the new legitimate group member.

- **Sign**: This phase allows a group member with a valid membership certificate to generate a valid group signature of a message. The generated message is sent to a verifier for verification.
- **Verify**: The validity of a group signature of a message is verified in this phase. A verifier accepts the signature if the signature is valid. If it is not valid, the message is rejected.
- **Open**: Given a signature of a message, together with the group public key and group manager's private key, the identity of the signer can be identified by the group manager in case of dispute.

### 3.1.2 Properties

A group signature scheme satisfies the following properties (Bellare et al., 2003; Ateniese et al., 2000):

- **Correctness**. A signature generated by a legitimate group member using *Sign* will always be accepted by *Verify*.
- **Anonymity**. The identity of a member of a group who signed a message is unknown to the other members in the network except the group manager.
- **Unlinkability**. Activities cannot be linked to a source. It is computationally hard to determine whether two valid signatures are generated by the same or by different group members.
- **Traceability**. Given a message signed by a group member, the group manager is able to open the identity of a signer in case of dispute.
- **Unforgeability**. The signature can not be forged. Only a legitimate group member can produce a valid signature on behalf of the group.
- **Exculpability**. Neither a group member nor a group manager can generate a

signature on behalf of other users.

### 3.1.3 Variants of Group Signatures

Several variants of group signature have been proposed to enhance security and efficiency of previously introduced group signature (Chaum & van Heyst, 1991), which is based on discrete logarithm problem (DLP). One of the most widely used constructions is short group signature (Boneh et al., 2004), which proposes shorter signature size using Strong-RSA assumption. Other constructions include dynamic group signature (Chen & Pedersen, 1994), linkable group siganture (Nakanishi et al., 1999), and ID-based group signature (Park et al., 1997). This thesis focuses on linkable group signature as it is related to our research.

#### 3.1.3.1 Linkable Group Signature

A linkable group signature scheme (Nakanishi et al., 1999) is one of the variants of group signatures. In this scheme, a message verifier can distinguish the two signatures generated by the same signer even if the signer identity is anonymous. This feature helps to prevent a Sybil attack, that is, a type of attack where a single user in a network masquerades as multiple identities to send fake messages. However, the drawback is, it compromises the requirement of privacy due to the linkability of the signer identity.

Message-linkable group signature (MLGS) is a scheme proposed by Wu et al. (2010) that introduces a more secure version of linkable group signature by addressing the anonymity problem. The anonymity of a signer is preserved as long as the signer generates one signature on each message. Once the signer generates two or more signatures on the same message, a verifier can link the signatures to the same signer. Apart from the mentioned phases and properties of group signature, MLGS addresses an additional property, that is, message-linkability. In this property, two group signatures only becomes linkable if a signer generates a signature for the same message more than once.

## 3.2 Mathematical Background

This section provides some fundamental backgrounds concerning number theory and abstract algebra for a little insight in cryptography, followed by bilinear pairing and computational assumption on which the security of our work is based upon. The definition in this section is merely based from (Menezes et al., 1996). We refer the reader to (Menezes et al., 1996) for a more comprehensive understanding on cryptography as this section only touches the surface of the backgrounds to provide a basis for cryptographic tools adopted in the thesis.

### 3.2.1 Number Theory

Number theory is the study that explores the properties of numbers and the relationship between numbers. Applications of number theory in cryptography are crucial to construct public key cryptosystem such as the discrete logarithm problem (DLP) and RSA algorithm. We emphasize the topic of modular arithmetic in the number theory as it allows formation of group which is defined in the next section.

**Definition 3.2.1.** If $a$ and $b$ are integers, then $a$ is said to be congruent to $b$ modulo $n$, written as $a \equiv b(mod\ n)$, if $n$ divides $(a - b)$. The integer $n$ is called the *modulus* of the congruence (Menezes et al., 1996).

**Example 3.2.1.** *i)* $8 \equiv 3(mod\ 5)$ *since* $8 - 3 = 1 \cdot 5$.

*ii)* $-18 \equiv 3(mod\ 7)$ *since* $-18 - 3 = 3 \cdot 7$.

*iii)* $39 \equiv 4(mod\ 7)$ *since* $39 - 4 = 5 \cdot 7$.

**Definition 3.2.2.** (properties of congruences) For all $a, a_1, b, b_1, c \in \mathbb{Z}$, the following properties are true (Menezes et al., 1996):

- $a \equiv b(mod\ n)$ if and only if $a$ and $b$ leave the same remainder when divided by $n$.
- (Reflexivity) $a \equiv a(mod\ n)$.
- (Symmetry) If $a \equiv b(mod\ n)$ then $b \equiv a(mod\ n)$.
- (Transitivity) If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$.
- If $a \equiv a_1(mod\ n)$ and $b \equiv b_1(mod\ n)$, then $a + b \equiv a_1 + b_1(mod\ n)$ and $ab \equiv a_1b_1(mod\ n)$.

**Definition 3.2.3.** The integers modulo $n$, denoted $\mathbb{Z}_n$, is the set of (equivalence classes of) integers $\{0, 1, 2, ..., n - 1\}$. Addition, subtraction, and multiplication in $\mathbb{Z}_n$ are performed modulo $n$ (Menezes et al., 1996).

**Example 3.2.2.** $\mathbb{Z}_{20} = \{0, 1, 2..., 19\}$. *In* $\mathbb{Z}_{20}$*,* $13 + 16 = 9$*, since* $13 + 16 = 29 \equiv 9(mod\ 20)$. *Similarly,* $13 \cdot 16 = 8$ *in* $\mathbb{Z}_{20}$ *since* $13 \cdot 16 = 208 \equiv 8(mod\ 20)$.

### 3.2.2 Abstract Algebra

Abstract algrebra is the study of algebraic structures such as groups, rings and fields. We focus on group as it is one of the essential building blocks of cryptography. Also, group is the central concept of other algebraic structures.

**Definition 3.2.4.** A binary operation $*$ on a set $S$ is a mapping from $S \times S$ to $S$. That is, $*$ is a rule which assigns to each ordered pair of elements from $S$ an element of $S$ (Menezes et al., 1996).

**Definition 3.2.5.** A group, denoted by $(\mathbb{G}, *)$ consists of a set $\mathbb{G}$ with a binary operation $*$ on $\mathbb{G}$ satisfying the following three conditions (Menezes et al., 1996):

- The group operation is associative. That is, $a * (b * c) = (a * b) * c$ for all $a, b, c \in \mathbb{G}$.

- There is an element $1 \in \mathbb{G}$, called the identity element, such that $a * 1 = 1 * a = a$ for all $a \in \mathbb{G}$.
- For each $a \in \mathbb{G}$ there exists an element $a^{-1} \in \mathbb{G}$, called the inverse of $a$, such that $a * a^{-1} = a^{-1} * a = 1$.

*Remark* 3.2.1. Multiplicative group notation has been used for the above group operation. If the group operation is addition, then the group is said to be an additive group, in which the identity element is denoted by 0, and the inverse of $a$ is denoted by $-a$. The group is abelian (or commutative) if, $a * b = b * a$ for all $a, b \in \mathbb{G}$ (Menezes et al., 1996).

**Definition 3.2.6.** A group $\mathbb{G}$ is finite if $|\mathbb{G}|$ is finite. The number of elements in a finite group is called its order (Menezes et al., 1996).

**Definition 3.2.7.** A group $\mathbb{G}$ is cyclic if there is an element $\alpha \in \mathbb{G}$ such that for each $b \in \mathbb{G}$ there is an integer $i$ with $b = \alpha^i$. Such an element $\alpha$ is called a generator of $\mathbb{G}$ (Menezes et al., 1996).

**Definition 3.2.8.** Every subgroup of a cyclic group $\mathbb{G}$ is also cyclic. In fact, if $\mathbb{G}$ is a cyclic group of order $n$, then for each positive divisor $d$ of $n$, $\mathbb{G}$ contains exactly one subgroup of order $d$ (Menezes et al., 1996).

### 3.2.3 Bilinear Pairings

Bilinear pairing has become an important tool in the construction of several cryptographic primitives such as identity based cryptography and group signature. It contains a set of three abstract algebraic groups which works under function $\hat{e}$, called bilinear map.

**Definition 3.2.9.** Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of the same prime order $q$. $\mathbb{G}_1$ is an additive group while $\mathbb{G}_2$ is a multiplicative group. A bilinear pairing on ($\mathbb{G}_1$,$\mathbb{G}_2$) is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ that satisfies the following properties (Menezes et al., 1996):

- Bilinearity: for all $P, Q \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- Non-degeneracy: there exists $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$, in other words, the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$.
- Computability: for any $P, Q \in \mathbb{G}_1$, there is an efficient algorithm to compute $\hat{e}(P, Q)$.

The map $\hat{e}$ is called an admissible bilinear map if it satisfies the three mentioned properties. Typically, $\mathbb{G}_1$ is a subgroup of the group of points on an elliptic curve over a finite field and $\mathbb{G}_2$ is a subgroup of the multiplicative group of a related finite field. The admissible bilinear map between these two groups can be constructed using the Weil and Tate pairings (Boneh & Franklin, 2003).

### 3.2.4 Computational Assumptions

Our work relies on several computational assumptions, that is, the Decisional Diffie-Hellman(DDH) assumption (Damgård, 1991), the Diffie-Hellman Knowledge (DHK) assumption (Damgård, 1991), and the Bilinear Diffie-Hellman (BDH) assumption (Boneh & Franklin, 2003). Let $\mathbb{G}$ be a finite cyclic group of prime order $p$ and $g$ be a generator of $\mathbb{G}$, the three assumptions are defined as follows.

#### 3.2.4.1 Decisional Diffie-Hellman (DDH) Assumption

Given $(g^x, g^y, g^r) \in \mathbb{G}$ such that $x, y, r \in \mathbb{Z}_p^*$, the DDH assumption states that for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, the probability of determining whether $r = xy$ is negligibly away from $\frac{1}{2}$. With a proper implementation, the DDH holds in $\mathbb{G}_1$ (Galbraith et al., 2008).

Informally, this assumption implies that there is no efficient probabilistic algorithm that outputs "true" if $r = xy$ and "false" otherwise with a proper implementation.

#### 3.2.4.2 Diffie-Hellman Knowledge (DHK) Assumption

Given $(g, g^x) \in \mathbb{G}$ for randomly chosen $x \in \mathbb{Z}_p^*$, for any PPT adversary $\mathcal{A}$, has only negligible probability of creating a Diffie-Hellman tuple $(g, g^x, g^r, g^{xr})$ from $(g, g^x)$ without knowing $r$.

In other words, the DHK assumption states that it is impossible to output a Diffie-Hellman tuple without knowing the discrete logarithm of one-tuple member with respect to another, that is, $r$.

#### 3.2.4.3 Bilinear Diffie-Hellman problem (BDH) Assumption

Let $\hat{e}$ be a bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$. Given $(g,g^x,g^y,g^r) \in \mathbb{G}_1$ with $x, y, r \in \mathbb{Z}_p^*$, compute $\hat{e}(g, g)^{xyr} \in \mathbb{G}_2$. The BDH assumption states that no PPT adversary $\mathcal{A}$ has a non-negligible advantage in solving the random choice of $x, y, r \in \mathbb{Z}_p^*$, and the random choice of $g \in \mathbb{G}_1$ in the BDH problem.

## 3.3 Conclusion

In this chapter, we have presented the cryptographic primitive adopted in our work, that is, group signature. We have also introduced some mathematical backgrounds for understanding of the cryptographic tools used in this thesis. In particular, we provided a brief overview of number theory, abstract algebra, bilinear pairing and computational assumption of which security is relied upon. These are the building blocks necessary for the design of the group signature.

# CHAPTER 4: REVOCATION PROTOCOL FOR GROUP SIGNATURE SCHEMES IN VANETS

*In this chapter, we formulate a generic abstraction of revocation for group signatures. We then use the abstraction as a guideline to design a new secure and efficient revocation protocol for group signatures. The proposed protocol addresses the issue of revocation in group signature scheme, namely MLGS and other schemes with similar construction.*

## 4.1 Introduction

This thesis fills in the gap of revocation in group signature schemes. We focus to solve the revocation issue in MLGS scheme proposed by Wu et al. in (2010). The proposed revocation protocol may also be adopted by other group signature scheme of similar construction to MLGS.

In MLGS (Wu et al., 2010), message broadcast phase is independent of RSUs and tracing information is generated by the vehicles themselves and submitted to the TP for registration purposes. Due to this setup, revocation protocol discussed in Section 2.1.5 may not be suitable solutions to be implemented in MLGS. Revocation in (Calandriello et al., 2007; Studer et al., 2009) has inefficiency issues. Meanwhile, revocation in (Shao et al., 2016; Zhu et al., 2014, 2013; Hao et al., 2011; L. Zhang et al., 2010) relies on RSUs when broadcasting messages which conflicts with MLGS. Lastly, MLGS has challenges to update credentials compared to (Chen et al., 2011; Lin et al., 2007) due to its self-generated tracing information.

Our work will solve this revocation issue by designing a new revocation protocol which combines the use of VLR with an additional technique of updating credentials together with tracing information. We emphasize that this revocation protocol is adaptable to other group signature schemes of similar construction.

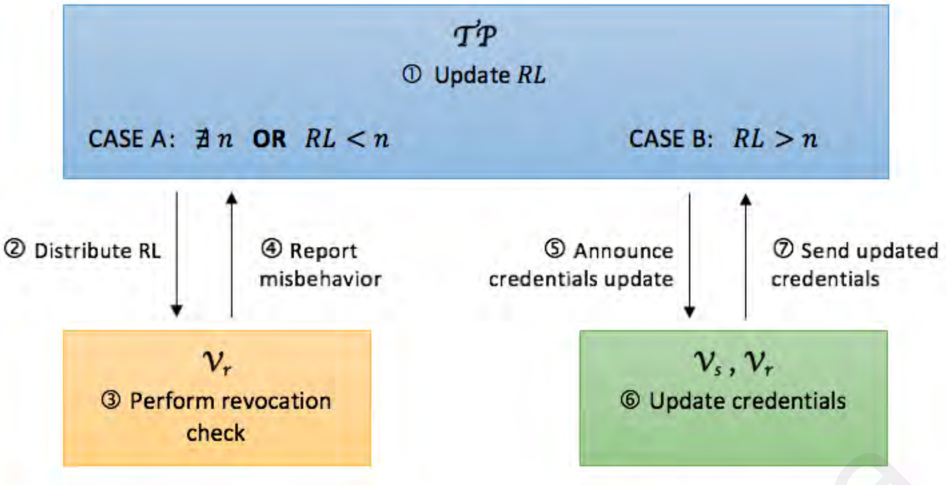
$\mathcal{TP}$
① Update $RL$
CASE A: $\nexists n$ OR $RL < n$
CASE B: $RL > n$
② Distribute RL
④ Report misbehavior
⑤ Announce credentials update
⑦ Send updated credentials
$\mathcal{V}_r$
③ Perform revocation check
$\mathcal{V}_s$, $\mathcal{V}_r$
⑥ Update credentials

**Figure 4.1:** Generic Revocation Construction

## 4.2 Abstraction of Revocation Protocols for Group Signatures

In this section, we present our generic abstraction of revocation protocols for group signature schemes in VANETs. The generic abstraction is formulated based on our observation of different revocation protocols used in some existing group signature schemes presented in Section 2.1.5. We analyse those protocols and generalize them into seven steps as demonstrated in Figure 4.1.

Before describing the abstraction, we review the main role of each entity in the network which consists of a trusted party ($\mathcal{TP}$), and vehicles ($\mathcal{V}$).

1. **Trusted Party ($\mathcal{TP}$).**

   a) A $\mathcal{TP}$ is responsible for the distribution and management of the revocation list (RL). This $\mathcal{TP}$ is commonly known as a trusted authority ($\mathcal{TA}$) in (Zhu et al., 2014; Studer et al., 2009), a tracing manager ($\mathcal{TM}$) in (Wu et al., 2010; Shao et al., 2016; L. Zhang et al., 2010), a certificate authority ($\mathcal{CA}$) in (Calandriello et al., 2007; Hao et al., 2011), a membership manager ($\mathcal{MM}$) in (Lin et al., 2007), and an issuer ($\mathcal{I}$) in (Chen et al., 2011).

2. **Vehicle ($\mathcal{V}$).** $\mathcal{V}$ has two roles in VANETs:

a) A sending vehicle $\mathcal{V}_s$ sends messages in the network. A $\mathcal{V}_s$ is further divided into two categories; unrevoked vehicles $\mathcal{V}_{s_u}$ and revoked vehicles $\mathcal{V}_{s_r}$.

b) A receiving vehicle $\mathcal{V}_r$ receives and verifies the messages. In some schemes such as in (Hao et al., 2011; L. Zhang et al., 2010; Shao et al., 2016; Zhu et al., 2014) revocation check is not performed during message verification phase, but it is performed during authentication phase by RSUs whenever a vehicle sends a message request to acquire a short-term group key. In such situation, we refer RSUs as $\mathcal{V}_r$. We do not distinguish between revoked and unrevoked vehicles in $\mathcal{V}_r$ since the task of receiving messages could cost no harm to the network.

### 4.2.1 Description of the Generic Revocation Construction

The generic abstraction shown in Figure 4.1 is composed of seven steps that generalises revocation protocols in group signatures. The steps are described as follows:

① Firstly, $\mathcal{TP}$ updates the revocation list (RL). There are two cases to be considered after updating the RL.

- CASE A: Either a threshold method is not adopted in the mechanism, denoted by $\nexists\, n$ in Figure 1 (such as RSU reliance revocation, VLR without threshold or traditional distribution of RL) or if it does, the number of revoked vehicles $\mathcal{V}_{s_r}$ in the RL is less than a predefined threshold $n$, denoted by $RL < n$.
- CASE B: The number of revoked vehicles $\mathcal{V}_{s_r}$ in the RL exceeds the threshold $n$, denoted by $RL > n$.

**For CASE A:**

② $\mathcal{TP}$ distributes the updated RL to $\mathcal{V}_r$ via the wireless channel.

③ $\mathcal{V}_r$ uses the received RL to perform revocation check in order to verify if a vehicle is revoked or not. If there is an identity matched, $\mathcal{V}_r$ rejects the message. If not, the message is accepted, provided the message originates from a legitimate sender.

④ If $\mathcal{V}_r$ experiences any misbehaviours, it may lodge a report and send it to $\mathcal{TP}$ via the wireless channel.

**For CASE B:**

⑤ $\mathcal{TP}$ announces a credential update via the wireless channel. If the credential update is performed by $\mathcal{TP}$, the process is simple as $\mathcal{TP}$ only updates unrevoked vehicle, $\mathcal{V}_{s_u}$'s credential and makes it available to $\mathcal{V}_{s_u}$. However, if the credential update is performed by vehicles; $\mathcal{V}_s$ and $\mathcal{V}_r$, thus step ⑥ and ⑦ follow.

(Note that, there is a circumstance where $\mathcal{TP}$'s credential also should be updated. Such update will be performed by $\mathcal{TP}$.)

*The last two steps can be discarded if the credential update is performed by $\mathcal{TP}$.*

⑥ $\mathcal{V}_s$ and $\mathcal{V}_r$ update its own credential using a unique value distributed by $\mathcal{TP}$.

⑦ $\mathcal{V}_s$ and $\mathcal{V}_r$ send to $\mathcal{TP}$ its updated credential for authentication or tracing purposes.

## 4.3 A Secure and Efficient Revocation Protocol for Group Signatures in VANETs

We propose a new revocation protocol for group signatures schemes in VANET which addresses the issue of revocation, or the lack thereof, in MLGS scheme (Wu et al., 2010) and other group signature schemes of similar setup and construction.

### 4.3.1 MLGS Scheme Overview

First and foremost, we provide an overview of MLGS scheme (Wu et al., 2010). There are three different roles of authorities in this scheme, which are a vehicle manufacturer

($\mathcal{VM}$), a group registration manager ($\mathcal{RM}$), and a tracing manager ($\mathcal{TM}$). To enroll into a VANET system, each vehicle signs a contract with the $\mathcal{VM}$ to confirm the vehicle ownership. Then, $\mathcal{V}$ registers to the $\mathcal{RM}$ to become a legitimate group member. During registration, $\mathcal{V}$ also sends a tracing information $T = g_2^y$ to the $\mathcal{TM}$ so that $\mathcal{TM}$ can trace the vehicle if in case of dispute. When $\mathcal{V}$ has successfully registered to the system, $\mathcal{V}$ will receive a sign on its public key from the $\mathcal{RM}$ and use the signature as a group certificate to announce safety messages. $\mathcal{VM}$, $\mathcal{RM}$, and $\mathcal{TM}$ are assumed as semi-trusted parties since they have no access to the private key of vehicles. Each vehicle generates its own public key $Y = U_1^y$ for a random value $y \in \mathbb{Z}_p^*$, where $y$ is the secret key. Table 4.1 shows the lists of some notations related to our work which was adopted from MLGS (Wu et al., 2010) to ease the reading throughout this thesis.

| Notation: Description |
|---|
| $\mathcal{VM}$: Vehicle manufacturer |
| $\mathcal{RM}$: Registration manager |
| $\mathcal{TM}$: Tracing manager |
| $\mathcal{V}$: Vehicle |
| $T = g_2^y$: Tracing information of $\mathcal{V}$ |
| $(Y, y)$: $\mathcal{V}$'s public-private key pair |
| $(A, Z)$: $\mathcal{RM}$'s public-private key pair |
| $m$: A message |
| $\sigma$: A signature on message $m$ |
| $\sigma_i$: The $i$-th component of $\sigma$ |
| $M = (m, \sigma)$: A message appended with a signature |
| $H_1()$: A cryptographic hash function from $\{0, 1\}^*$ to $\mathbb{G}_1$ |
| $\mathbb{G}_i (i = 1, 2, 3)$: Finite cyclic group of prime order $p$ |
| $g_i$: A random generator of $\mathbb{G}_i$ |
| $U_2, h_2 \in \mathbb{G}_2$: Public system parameters |
| $\phi$: An isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ |
| $U_1 = \phi(U_2)$: Public system parameter |
| $h_1 = \phi(h_2)$: Public system parameter |
| $K_v = (K_1, K_2)$: $\mathcal{V}$'s group certificate |

**Table 4.1:** Notations and Descriptions

The goal of MLGS scheme is to provide an efficient trustworthy system with a balanced public safety and vehicle privacy. Threshold authentication is used to satisfy the trustworthiness property. (Say $n$) MLGS signatures are generated by $n$ distinct registered vehicles on messages of the same content. A receiver verifies $n$ signatures using the $\mathcal{RM}$'s public key, $A$ to validate the group certificates. If these $n$ signatures are valid and if $n$ satisfies the threshold, the message is considered trustworthy. Meanwhile, to protect the privacy of vehicles, this scheme allows each vehicle to generate only one message-link identifier $\sigma_4 = H_1(m)^y$ for the same message. This approach enables a vehicle to remain anonymous if it generates one signature on each message but this vehicle can be traced once it produces two signatures on the same message as the two signatures share the same component $\sigma_4$. Thus, anonymity is preserved as long as the vehicle does not misbehave by generating two signatures on the same message. However, vehicle's safety is compromised when no revocation technique was proposed in MLGS. In the next section, we show our construction of a revocation scheme that can be efficiently deployed in MLGS.

### 4.3.2 Our Proposed Construction

Our proposed revocation protocol has minimal reliance on RSUs. The involvement of the RSUs is only needed to relay information and to provide a gateway between a trusted party and vehicles. Furthermore, we adopted the generic abstraction presented in Section 4.2 that defines the structure of our revocation protocol.

#### 4.3.2.1 VLR Adoption

The construction begins with the adoption of VLR method (Boneh & Shacham, 2004). This is a common approach for group signature schemes in VANETs (Chen et al., 2011; Studer et al., 2009; Lin et al., 2007; Calandriello et al., 2007). VLR is used in the revocation check during the verification of a signature. According to Bringer in (Bringer

& Patey, 2011), the verification phase should be divided into two parts; ‘revocation check’ and ‘signature check’. The former is to verify if the signing vehicle has been revoked or not whereas the latter is to check if the signing vehicle is a legitimate member in the network. When analysing the MLGS scheme, we found its verification phase only applies ‘signature check’ without being curious to identify if the vehicles have been revoked from the system or not. Hence, the adoption of VLR is applicable in MLGS since there is no ‘revocation check’ being implemented. Nevertheless, due to the downside of VLR discussed in Chapter 2, we choose to apply VLR when a number of revoked vehicles in RL is below a certain threshold, and credential update when the number of revoked vehicles in RL exceeds the threshold.

We use the generic abstraction of revocation presented in Section 4.2 to describe the detailed mechanism of VLR adoption for MLGS as below.

① $\mathcal{TM}$ updates the the Revocation List, $RL = \{Y_{v_1}, ..., Y_{v_i}\}$.

② $\mathcal{TM}$ distributes the revocation list to $\mathcal{V}$ when $i < n$ is a predefined threshold.

③ Upon receiving a message $m$ that contains a signature $\sigma_{v_i}$, $\mathcal{V}$ first performs revocation check operation by checking $\sigma_2 = K_2(h_1Y_i)^s$ for each $Y_i$ in the RL. If there is a matched $Y_i$, the message will be discarded. If not, the message is considered as valid and the $\mathcal{V}$ continues to perform signature check operation to validate the signature.

④ $\mathcal{V}$ also lodges a report to $\mathcal{TM}$ when repetition of $\sigma_4$ is found as it indicates an attempt of misbehavior in MLGS.

#### 4.3.2.2 Credentials Update

We apply an additional revocation mechanism when the number of revoked vehicles exceeds the predefined threshold. Similar technique was also adopted in (Chen et al., 2011; Lin et al., 2007). In MLGS, since the $\mathcal{RM}$'s key is used by the verifiers during the verification phase, updating both its $\mathcal{RM}$'s key and vehicles' credentials is necessary for revocation. However, updating vehicles' credentials is an issue in MLGS since the vehicles generate their own tracing information which was sent to the $\mathcal{TM}$ during the registration phase. Our proposed revocation protocol includes the process of updating the tracing information, thus solving the issue in MLGS.

Since we consider the use of threshold limit for revoked vehicles, the revocation construction follows until the last step of the generic abstraction presented in Section 4.2.

⑤ $\mathcal{TM}$ announces a credential update to be performed by $\mathcal{V}$. At the same time, $\mathcal{RM}$ updates its credential. The $\mathcal{RM}$ has public-private key pair $(A, Z)$ where $A = e(Z, g_2)$. To update its key, the $\mathcal{RM}$ first updates its private key $Z$ to a new value $\dot{Z} \in \mathbb{Z}_p^*$. The $\mathcal{RM}$ then updates its public key $A$ to $\dot{A} = e(\dot{Z}, g_2)$. The $\mathcal{RM}$ can now publish its new public key $\dot{A}$ to be used across the network via the RSU while its secret key is kept private. The detailed algorithm is illustrated in Algorithm 1.

**Algorithm 1** Register Manager ($\mathcal{RM}$)

```
Initially: $(pk_{RM}, sk_{RM}) = (A, Z) = (e(Z, g_2), Z)$

Update: $(\dot{pk}_{RM}, \dot{sk}_{RM}) = (e(\dot{Z}, g_2), \dot{Z})$ where $\dot{Z} \in \mathbb{Z}_p^*$

Publish: $\dot{A}$, while $\dot{Z}$ is kept secret
```

⑥ $\mathcal{V}$ updates its credential (shown in Algorithm 2) in which tracing information is also updated in this process. Since the credential update is performed by $\mathcal{V}$ in MLGS, the $\mathcal{TM}$ distributes a new value $x \in \mathbb{Z}_p^*$ to $\mathcal{V}$ in the system. $\mathcal{V}$'s public-private key pair is $(Y, y)$ where $Y = U_1^y$. By having the new value $x$, $\mathcal{V}$ updates its private key $y$ first to $\dot{y} = y^x$. Then, $\mathcal{V}$ updates its public key $Y$ to $\dot{Y} = (U_1^y)^x$. Now, $\mathcal{V}$ has its new key pair $(\dot{Y}, \dot{y}) = ((U_1^y)^x, y^x)$ and can use $\dot{Y}$ across the network. Using the new key, $\mathcal{V}$ computes a new tracing information $\dot{T} = (g_2^y)^x$.

**Algorithm 2** Vehicle ($\mathcal{V}$)

**Initially**: $(pk_V, sk_V) = (Y, y) = (U_1^y, y)$

**Update**: $(\dot{pk_V}, \dot{sk_V}) = ((U_1^y)^x, y^x)$ where $x \in \mathbb{Z}_p^*$

**Publish**: $\dot{Y}$, while $\dot{y}$ is kept secret

**For tracing purpose**:
$\mathcal{V}$ computes $\dot{T} = (g_2^y)^x$

$$\mathcal{V} \xrightarrow{\sigma_{VM}(Y),\dot{Y},\dot{T}} \mathcal{TM}$$

$\mathcal{TM}$ verifies:

- $\sigma_{VM}(Y)$
- $\dot{Y}$
- $e(\dot{Y}, g_2) = e(U_1, T)$ where $e((U_1^y)^x, g_2) = e(xU_1, x\dot{T})$

$$\mathcal{TM} \xrightarrow{\sigma_{TM}(\dot{Y})} \mathcal{V} \xrightarrow{\sigma_{TM}(\dot{Y})} \mathcal{RM}$$

$\mathcal{RM}$ verifies:

- $\sigma_{TM}(\dot{Y})$

$$\mathcal{RM} \xrightarrow{K_v=(K_1,K_2)} \mathcal{V}$$

⑦ $\mathcal{V}$ sends its new tracing information together with the old signature of $\mathcal{VM}$ on $Y$ and the new $\dot{Y}$ to $\mathcal{TM}$. Upon receiving the information, $\mathcal{TM}$ first verifies the legitimacy of $\mathcal{V}$ by checking the signature and the new key. Then, $\mathcal{TM}$ verifies the traceability of $\mathcal{V}$ in case of dispute by checking the new tracing information if $e(\dot{Y}, g_2) = e(U_1, \dot{T})$ where $e((U_1{}^y)^x, g_2) = e(xU_1, x\dot{T})$. If both checks hold, $\mathcal{TM}$ generates a signature on $\dot{Y}$ and sends it to $\mathcal{V}$. Then $\mathcal{V}$ sends the received signature to $\mathcal{RM}$ to acquire a new group certificate $K_v = (K_1, K_2)$. Upon receiving the signature $\mathcal{RM}$ checks its validity. If the check holds, $\mathcal{RM}$ generates $K_v$ to $\mathcal{V}$.

$\mathcal{TM}$ will be able to identify a revoked vehicle if it attempts to update its credential by sending its tracing information. $\mathcal{TM}$ will not sign its key nor will it validate the tracing information sent. This prevents revoked vehicles from further contacting $\mathcal{RM}$ to acquire a new group certificate, thus no longer be able to continue its future participation in the network. The detailed algorithm of the last two steps are illustrated in Algorithm 2.

### 4.3.3 Analysis

We analyse both the security and the performance of our revocation protocol to verify its secure and efficient adoption in VANETs. Both analysis are presented in the following section.

#### 4.3.3.1 Security Analysis

Some schemes in the literature (Raya & Hubaux, 2007; Q. Li et al., 2012; Wu et al., 2010; Malip et al., 2014; Chen et al., 2011) highlighted the following three security requirements are critical concerns to be met towards VANETs deployment:

- **Trustworthiness**. To view a message as trustworthy, it must be sent unmodified by a legitimate vehicle. Moreover, the message sent must reflect the actual event.
- **Privacy**. The identity of the sending vehicle should be protected unless it misbehaved. Furthermore, if two different messages are generated by the same sender, they cannot be linked to each other.
- **Accountability**. If misbehaviour arise, the misbehaved vehicles can be traceable. Moreover, they must satisfy non-repudiation, that is, the assurance that they are the message originator. Lastly, the misbehaved vehicle can be revoked from the network.

We show that our revocation construction completes the security requirement of accountability in MLGS. The requirement of trustworthiness and privacy have been achieved by the fact of using threshold method and group signature, respectively, in MLGS system.

As discussed, accountability can only be achieved if it satisfies traceability, non-repudiation and revocation properties. Traceability is satisfied in MLGS when a malicious vehicle who produces two or more signatures on the same message can be traceable since $\mathcal{V}$ can only generate one identifier, indicated by $\sigma_4$ for the same message. Non-repudiation is provided by the fact that each vehicle generates its own secret key $y$ without being known by other entities, including semi-trusted entities ($\mathcal{VM}$, $\mathcal{TM}$, $\mathcal{RM}$). However, revocation is not supported in MLGS since there is no explicit revocation mechanism presented in the scheme. Thus, the requirement of accountability is not achieved in MLGS. By adopting our proposed revocation protocol presented in this thesis, the accountability requirement is now satisfied.

| Schemes | Traceability | Non-repudiation | Revocation |
|---|---|---|---|
| TAA (Chen et al., 2011) | √ | √ | √ |
| GSIS (Lin et al., 2007) | √ | X | √ |
| Hybrid (Calandriello et al., 2007) | √ | X | √ |
| TACK (Studer et al., 2009) | √ | X | √ |
| HMAC (Zhu et al., 2014) | √ | X | √ |
| HMAC v2 (Zhu et al., 2013) | √ | X | √ |
| CMAP (Hao et al., 2011) | √ | X | √ |
| Signcryption (L. Zhang et al., 2010) | √ | X | √ |
| MLGS (Wu et al., 2010) | √ | √ | X |
| Our work | √ | √ | √ |

**Table 4.2:** Comparison of Accountability Analysis

We compare the functionalities of accountability requirement with other group signature schemes in VANETs (illustrated in table 4.2). All schemes satisfy the traceability property. However, only MLGS and TAA achieve non-repudiation since the vehicle in both of these schemes is the sole holder of its secret key. Lastly, looking at the revocation column in table 4.2, MLGS is the only scheme that does not achieve revocation property, but with our proposed revocation construction, the issue is solved.

#### 4.3.3.2 Performance Analysis

This section presents comparison of performance efficiency between our proposed revocation protocol in MLGS with revocation protocols adopted in GSIS (Lin et al., 2007), and TAA (Chen et al., 2011) schemes. We do not compare our work with revocation protocols in (Zhu et al., 2014; Hao et al., 2011; L. Zhang et al., 2010; Shao et al., 2016) since the schemes rely on RSU. Meanwhile, revocation protocols in (Calandriello et al., 2007; Studer et al., 2009) only adopted VLR mechanism which is known to be inefficient if a large number of revoked vehicles exists in the revocation list. Thus, only GSIS and TAA are suitable schemes for a comparison.

Here we only evaluate the performance of verification phase because this is the phase where 'revocation check' and 'signature check' are being conducted. Before presenting the analysis, we give an informal description of the computational assumptions on which our proposed revocation is based, which is on the bilinear Diffie-Hellman problem (BDHP) (Menezes, 2009). Since the credential is constructed using the BDHP, this description intents to show how the performance analysis being extracted.

The BDHP is described as follows. Let $e$ be a bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$ and $P$ be a generator of $\mathbb{G}_1$. Given $< P, aP, bP, cP > \in \mathbb{G}_1$ with $a, b, c \in \mathbb{Z}_q^*$, then $e(P, P)^{abc} \in \mathbb{G}_2$. First, compute $g = e(P, P)$, followed by $g^{ab} = e(aP, bP)$ and $g^c = e(P, cP)$. The shared key $g^{abc} = e(P, P)^{abc}$ should be computed using the DHP algorithm. For further details, we refer the readers to (Menezes, 2009).

Table 4.3 summarizes the comparison of the performance efficiency for $t = 1$ as GSIS does not support a threshold method. In this table, $r.\mathbb{G}_1$ indicates $r$ scalar multiplications in $\mathbb{G}_1$, $s.P$ indicates $s$ pairing operations and $n$ in the fifth column denotes the size of the revocation list. To achieve security level $l = 80$ bits, we set $q = 160$ bits and the element in

|  | Computational Cost |  | Computation Time |  |
|---|---|---|---|---|
|  | Revocation Check | Signature Check | Revocation Check (ms) | Signature Check (ms) |
| GSIS (Lin et al., 2007) | $2.P$ | $5.\mathbb{G}_1 + 1.P$ | $9.0 \times n$ | 7.5 |
| TAA (Chen et al., 2011) | $1.\mathbb{G}_1$ | $7.\mathbb{G}_1 + 5.P$ | $0.6 \times n$ | 26.7 |
| Our work | $1.P$ | $6.\mathbb{G}_1 + 1.P$ | $4.5 \times n$ | 8.1 |

**Table 4.3:** Comparison of Performance Analysis

$\mathbb{G}_1$ = 161 bits by choosing an appropriate curve such as NIST curve (Brown, Hankerson, López, & Menezes, 2001). Specifically, we conduct our comparison in two categories: computational cost and computation time.

**Computational cost.** We consider the two most expensive operation, particularly scalar multiplication and pairing evaluation. If exponentiation is used, it will be changed into scalar multiplication to ease the comparison. According to (Chen et al., 2011), in usual implementation, one exponentiation in $\mathbb{G}_T$ ($\mathbb{G}_3$ in MLGS) costs about 4 scalar multiplication in $\mathbb{G}_1$. We use this trick to transform our observation of operation used in (Wu et al., 2010; Chen et al., 2011; Lin et al., 2007) into the operation presented in computational cost column of Table 4.3. In addition, a multi-base pairing is similar to a single-base pairing as they almost have the same overhead (Boyen & Waters, 2006). Now, we add both 'revocation check' and 'signature check' operations to get a full operation of verification phase. We then have $5.\mathbb{G}_1 + 3.P$ for GSIS, $8.\mathbb{G}_1 + 5.P$ for TAA, and $6.\mathbb{G}_1 + 2.P$ for the improved MLGS. Here, we see that the computational cost for our work is comparable to GSIS and more costly efficient compared to TAA.

**Computation time.** Based on the set value of $q = 160$ bits and $\mathbb{G}_1 = 161$ bits, one pairing evaluation and one scalar multiplication in $\mathbb{G}_1$ can be done within 4.5 ms and 0.6 ms respectively. Using this information, we calculated the computation time of operations tabulated in the computational cost column of Table 4.3. For instance, we take 'revocation check' operation in our work, i.e $1.P$, then we multiply it by 4.5 ms × $n$, where $n$ is the length of the revocation list to obtain 4.5 ms × $n$. Similarly for the 'signature check', i.e.

$6.\mathbb{G}_1$ and $1.P$, we multiply each of them with 0.6 ms and 4.5 ms respectively before adding them up together to obtain 8.1 ms as a total. We present the rest of the calculation result in Computation Time column of Table 4.3.

From the above analysis, we observe that our revocation check is twice as fast as GSIS but it is slower than TAA. However, TAA takes three times significantly longer to perform signature check, thus making the overall verification process less efficient. Even though GSIS competes the signature check, its revocation check is the longest compare with other schemes. We note that the difference of signature check between GSIS and our work differ by less than 1 ms. Therefore, our work is better than 1) TAA in signature check 2) GSIS in revocation check. In conclusion, our work achieves comparable performance to GSIS and TAA.

## 4.4 Conclusion

In this chapter, we have presented a secure and efficient revocation protocol for group signature schemes in VANETs. We have shown that our revocation protocol can be deployed in MLGS (Wu et al., 2010), thus completing its construction. While it was proposed to address the gap in MLGS, our revocation protocol is adaptable to other schemes of similar setup and construction. Our generic abstraction may assist to provide guidelines to design future revocation protocol based on group signatures. As far as we know, this is the first generic abstraction for revocation in group signatures exists in the literature.

# CHAPTER 5: CONCLUSION

*This chapter concludes the contributions of this thesis and discuss the directions for future work.*

## 5.1 Summary of Contributions

VANET has become one of the emerging technologies in wireless networks to improve transportation safety and efficiency. This technology allows vehicles to share various information regarding road and traffic conditions such as traffic jams, vehicular collision, slippery roads, and emergency braking so that other neighbouring vehicles get warned of any potential dangers and thus able to take appropriate actions to avoid such dangers. Driver may also able to shift to other alternative routes when receiving notifications on traffic jams ahead of time.

There are some security challenges associated to this technology which makes its complete adoption to be challenging. Vehicles in VANETs are susceptible to adversarial attacks when they join the wireless network. The adversaries may control the vehicle system, send fake messages, and track vehicles activities, thereby causing harm on road users. This thesis focuses on the attacks performed by internal adversaries since most of external attacks are preventable by enforcing privacy and enhancing authenticity of the system.

In this thesis, we designed a new secure and efficient revocation protocol for group signatures in VANETs as we acknowledged the importance of revocation to eliminate internal adversaries from the network. We analysed some existing revocation protocol based on various cryptographic primitives in VANETs. We discussed the advantages and disadvantages of each protocol. We then identified the absence of revocation protocol in some schemes in group signature, "traditional" public key, identity-based and symmetric key. We addressed the issue of revocation in group signature as its level of security is more appealing compared to other cryptographic primitives.

We formulated an abstract model for revocation protocols in group signatures which defines the general concept of the existing revocation protocols. To the best of our knowledge, this is the first abstract model in the literature that generalised revocation protocol for group signatures. We then used the formulated abstraction as a framework to design our new revocation protocol. We constructed our revocation protocol for a group signature scheme, called MLGS which did not present any revocation in its construction. Our generic revocation protocol is applicable to other group signature schemes with similar construction. Our proposed protocol employed VLR method when the number of revoked vehicles in the network is below a certain threshold. When the number exceeds the threshold, the method of updating credentials with tracing information was adopted. We analysed and compared security and performance of our revocation protocol to other relevant schemes in the literature. The protocol fulfilled VANET security requirements and achieved comparable performance to the existing schemes.

## 5.2 Directions for Future Work

There are several research directions that can be followed beginning from the work presented in this thesis. Some of the possible extensions are defined as follows.

- While this research focuses on revocation protocol for group signature, it might be interesting to design revocation protocol based on other cryptographic primitives such as "traditional" public key cryptography, identity-based cryptography, and symmetric key cryptography.
- It might be worthwhile to formulate abstract model of revocation protocols based on other cryptographic primitives. This may reduce the possibility of overlooking

some important features to design a practical revocation protocol.

- It might be interesting to explore other cryptographic tools that can vastly improve the performance efficiency for a secure revocation protocol. At the same time, the system model shall not compromise other security requirements.
- Our protocol can only be utilised by group signature schemes with similar setup and construction. It might be useful to further extend the protocol to where it can be utilised by other group signature schemes in the literature. How this may be done without compromising other security requirements is the subject of future research.

# REFERENCES

Abu-Zidan, F. M., & Eid, H. O. (2015). Factors affecting injury severity of vehicle occupants following road traffic collisions. *Injury*, *46*(1), 136–141.

Alam, M., & Ahmed, F. (2013). Urban transport systems and congestion: a case study of indian cities. *Transport and Communications Bulletin for Asia and the Pacific*, *82*, 33–43.

Artail, H., & Abbani, N. (2016). A pseudonym management system to achieve anonymity in vehicular ad hoc networks. *IEEE Trans. Dependable Sec. Comput.*, *13*(1), 106–119.

Ateniese, G., Camenisch, J., Joye, M., & Tsudik, G. (2000). A practical and provably secure coalition-resistant group signature scheme. *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, 255–270.

Bellare, M., Micciancio, D., & Warinschi, B. (2003). Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, 614–629.

Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, *13*(7), 422–426.

Boneh, D., Boyen, X., & Shacham, H. (2004). Short group signatures. *Crypto*, *3152*, 41–55.

Boneh, D., & Franklin, M. K. (2003). Identity-based encryption from the weil pairing. *SIAM J. Comput.*, *32*(3), 586–615.

Boneh, D., & Shacham, H. (2004). Group signatures with verifier-local revocation. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*, 168–177.

Boyen, X., & Waters, B. (2006). Compact group signatures without random oracles. *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Confer-*

*ence on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, 427–444.

Bringer, J., & Patey, A. (2011). Backward unlinkability for a VLR group signature scheme with efficient revocation check. *IACR Cryptology ePrint Archive*, *2011*, 376.

Brown, M., Hankerson, D., López, J., & Menezes, A. (2001). Software implementation of the NIST elliptic curves over prime fields. *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings*, 250–265.

Calandriello, G., Papadimitratos, P., Hubaux, J.-P., & Lioy, A. (2007). Efficient and robust pseudonymous authentication in VANET. *Proceedings of the Fourth International Workshop on Vehicular Ad Hoc Networks, VANET 2007, Montréal, Québec, Canada, September 10, 2007*, 19–28.

Chaum, D., & van Heyst, E. (1991). Group signatures. *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, 257–265.

Chen, L., Ng, S.-L., & Wang, G. (2011). Threshold anonymous announcement in vanets. *IEEE Journal on Selected Areas in Communications*, *29*(3), 605–615.

Chen, L., & Pedersen, T. P. (1994). New group signature schemes (extended abstract). *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, 171–181.

Choi, J. Y., Jakobsson, M., & Wetzel, S. (2005). Balancing auditability and privacy in vehicular networks. *Q2SWinet'05 - Proceedings of the First ACM Workshop on Q2S and Security for Wireless and Mobile Networks, Montreal, Quebec, Canada, October 13, 2005*, 79–87.

Damgård, I. (1991). Towards practical public key systems secure against chosen ciphertext attacks. *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, 445–456.

Galbraith, S. D., Paterson, K. G., & Smart, N. P. (2008). Pairings for cryptographers. *Discrete Applied Mathematics*, *156*(16), 3113–3121.

Golle, P., Greene, D. H., & Staddon, J. (2004). Detecting and correcting malicious data in vanets. *Proceedings of the First International Workshop on Vehicular Ad Hoc Networks, 2004, Philadelphia, PA, USA, October 1, 2004*, 29–37.

Han, D., & Yang, H. (2008). The multi-class, multi-criterion traffic equilibrium and the efficiency of congestion pricing. *Transportation Research Part E: Logistics and Transportation Review*, *44*(5), 753 - 773.

Hao, Y., Cheng, Y., Zhou, C., & Song, W. (2011). A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on Selected Areas in Communications*, *29*(3), 616–629.

Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). Vanet security challenges and solutions: A survey. *Vehicular Communications*, *7*, 7 - 20. doi: https://doi.org/10.1016/j.vehcom.2017.01.002

He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Information Forensics and Security*, *10*(12), 2681–2691.

Kounga, G., Walter, T., & Lachmund, S. (2009). Proving reliability of anonymous information in vanets. *IEEE Trans. Vehicular Technology*, *58*(6), 2977–2989.

Kroh, R., Kung, A., & Kargl, F. (2006). *VANETs security requirements final version* (Tech. Rep.). Secure Vehicle Communication (SeVeCom).

Lee, J. F., Wang, C. S., & Chuang, M. C. (2010). Fast and reliable emergency message dissemination mechanism in vehicular ad hoc networks. *2010 IEEE Wireless Communication and Networking Conference*, 1-6.

Lee, K. C., Lee, U., & Gerla, M. (2010). Survey of routing protocols in vehicular ad hoc networks. *Advances in vehicular ad-hoc networks: Developments and challenges*, 149–170.

Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular technology magazine*, *2*(2), 12–22.

Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A reputation-based announcement scheme for vanets. *IEEE Trans. Vehicular Technology*, *61*(9), 4095–4108.

Lin, X., Sun, X., Ho, P., & Shen, X. (2007). GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Vehicular Technology*, *56*(6), 3442–3456.

Liu, B., Chiang, J. T., & Hu, Y.-C. (2010). Limits on revocation in VANETs. *Pre-proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS 2010)*, 38-52.

Malip, A., Ng, S.-L., & Li, Q. (2014). A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks. *Security and Communication Networks*, *7*(3), 588–601.

Menezes, A. (2009). An introduction to pairing-based cryptography. In I. Luengo (Ed.), (p. 47-65). Recent trends in cryptography, American Mathematical Society.

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of applied cryptography. In (p. 49-86). CRC Press.

Mitzenmacher, M. (2002). Compressed bloom filters. *IEEE/ACM Trans. Netw.*, *10*(5), 604–612.

Mohanty, M., & Gupta, A. (2015). Factors affecting road crash modeling. *Journal of Transport Literature*, *9*(2), 15–19.

Moya-Gómez, B., & García-Palomares, J. C. (2017). The impacts of congestion on automobile accessibility. what happens in large european cities? *Journal of Transport Geography*, *62*, 148–159.

Nakanishi, T., Fujiwara, T., & Watanabe, H. (1999, jul). A linkable group signature and its application to secret voting. *Transactions of Information Processing Society of Japan*, *40*(7), 3085-3096.

Ning, P., Schwebel, D. C., Huang, H., Li, L., Li, J., & Hu, G. (2016). Global progress in road injury mortality since 2010. *PLoS ONE*, *11*(10), e0164560.

Papadimitratos, P., Buttyán, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., & Hubaux,

J. (2009). Secure vehicular communication systems: Design and architecture. *CoRR*, *abs/0912.5391*.

Park, S., Aslam, B., & Zou, C. C. (2011). Long-term reputation system for vehicular networking based on vehicle's daily commute routine. *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, 436-441.

Park, S., Kim, S., & Won, D. (1997). Id-based group signature. *Electronics Letters*, *33*(19), 1616-1617.

Porwal, V., Patel, R., & Kapoor, D. R. (2014). Review of internal security attacks in vehicular adhoc networks (vanets). *International Journal of Engineering Research & Technology (IJERT), ISSN*, 2278–0181.

Qu, F., Wu, Z., Wang, F. Y., & Cho, W. (2015). A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, *16*(6), 2985-2996.

Ramzan, Z. A. (1999). *Group blind digital signatures: Theory and applications* (Master's thesis, Massachusetts Institute of Technology). Retrieved from `http://groups.csail.mit.edu/cis/theses/ramzanms.pdf` (Last accessed 23 August 2017)

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.

Raya, M., Papadimitratos, P., & Hubaux, J. (2006). Securing vehicular communications. *IEEE Wireless Commun.*, *13*(5), 8–15.

Schoch, E. (2012). *EU-US OEM harmonization security workshop.* C2C-CC Security Design. Retrieved from `https://www.car-2-car.org/fileadmin/user_upload/OEM_Workshop_WOB/Security-Workshop_security-design.pdf`

Schrank, D., Eisele, B., & Lomax, T. (2012). *TTI's 2012 urban mobility report.* Texas A&M Transportation Institute. The Texas A&M University System. Retrieved from `https://www.pagregion.com/Portals/0/documents/HumanServices/2012MobilityReport.pdf` (Last accessed on 27 August 2017)

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August*

*19-22, 1984, Proceedings*, 47–53.

Shao, J., Lin, X., Lu, R., & Zuo, C. (2016). A threshold anonymous authentication protocol for vanets. *IEEE Trans. Vehicular Technology*, *65*(3), 1711–1720.

Studer, A., Shi, E., Bai, F., & Perrig, A. (2009). *Tacking together efficient authentication, revocation, and privacy in vanets.*

Sun, J., Zhang, C., Zhang, Y., & Fang, Y. (2010). An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.*, *21*(9), 1227–1239.

TAC. (2015). *Report on study of road traffic congestion in Hong Kong.* Transport Advisory Committee. Retrieved from `http://www.thb.gov.hk/eng/boards/transport/land/Full_Eng_C_cover.pdf` (Last accessed on 15 August 2017)

Toh, C. K. (2001). *Ad hoc wireless networks: Protocols and systems* (1st ed.). Upper Saddle River, NJ, USA: Prentice Hall PTR.

Toulni, H., Nsiri, B., Boulmalf, M., Bakhouya, M., & Sadiki, T. (2014). An approach to avoid traffic congestion using vanet. *2014 International Conference on Next Generation Networks and Services (NGNS)*, 154-159.

Tyagi, P., & Dembla, D. (2014). A taxonomy of security attacks and issues in vehicular ad-hoc networks (vanets). *International Journal of Computer Applications*, *91*(7).

UNRSC. (2011). *Global plan for the decade of action for road safety 2011-2020.* World Health Organization. Retrieved from `http://www.who.int/roadsafety/decade_of_action/plan/plan_english.pdf` (Last accessed on 15 August 2017)

Wasef, A., Jiang, Y., & Shen, X. (2008). ECMV: efficient certificate management scheme for vehicular networks. *Proceedings of the Global Communications Conference, 2008. GLOBECOM 2008, New Orleans, LA, USA, 30 November - 4 December 2008*, 639–643.

Wegman, F. (2017). The future of road safety: A worldwide perspective. *IATSS Research*, *40*(2), 66–71.

WHO. (2015). *Global status report on road safety 2015.* World Health Organization. Retrieved from http://www.who.int/violence_injury_prevention/road_safety_status/2015/GSRRS2015_Summary_EN_final.pdf (Last accessed on 15 August 2017)

Wischhof, L., Ebner, A., & Rohling, H. (2005). Information dissemination in self-organizing intervehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, *6*(1), 90-101.

Wu, Q., Domingo-Ferrer, J., & González-Nicolás, Ú. (2010). Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Trans. Vehicular Technology*, *59*(2), 559–573.

Xi, Y., Sha, K., Shi, W., Schwiebert, L., & Zhang, T. (2007). Enforcing privacy using symmetric random key-set in vehicular networks. *International Symposium on Autonomous Decentralized Systems (ISADS 2007), 21-23 March 2007, Sedona, AZ, USA*, 344–351.

Xue, L., Yang, Y., & Dong, D. (2017). Roadside infrastructure plans scheme for the urban vehicular networks. *Transportation Research Procedia*, *25*, 1380–1396.

Zhang, C., Lin, X., Lu, R., & Ho, P. (2008). RAISE: an efficient rsu-aided message authentication scheme in vehicular communication networks. *Proceedings of IEEE International Conference on Communications, ICC 2008, Beijing, China, 19-23 May 2008*, 1451–1457.

Zhang, C., Lu, R., Lin, X., Ho, P., & Shen, X. (2008). An efficient identity-based batch verification scheme for vehicular sensor networks. *INFOCOM 2008. 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA*, 246–250.

Zhang, L., Wu, Q., Solanas, A., & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. *IEEE Trans. Vehicular Technology*, *59*(4), 1606–1617.

Zheng, Y. (1997). Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, 165–179.

Zhu, X., Jiang, S., Wang, L., & Li, H. (2014). Efficient privacy-preserving authentication for vehicular ad hoc networks. *IEEE Trans. Vehicular Technology*, *63*(2), 907–919.

Zhu, X., Jiang, S., Wang, L., Li, H., Zhang, W., & Li, Z. (2013). Privacy-preserving authentication based on group signature for VANETs. *IEEE Global Communications Conference (GLOBECOM)*, 4609-4614.

Zhuang, Y., Pan, J., Luo, Y., & Cai, L. (2011). Time and location-critical emergency message dissemination for vehicular ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, *29*(1), 187-196.