Cryptography and Privacy in Vehicular Communication Networks

by

Pravek Sharma

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2023

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Wireless communication technologies can support dynamic networks between vehicles, pedestrians and roadside infrastructure called Vehicular Ad hoc Networks (VANETs). Wireless communication over VANETs allows for several communications scenarios — between vehicles, between vehicles and infrastructure, and between vehicles and pedestrians, among others — collectively known as Vehicle-to-Everything (V2X) communication.

Fast wireless communication allows vehicles to communicate over long distances, improving a driver's perception compared to relying on human senses alone. Computerised automated decisions made in response to a wireless message also allow for a lifesaving decision to be much faster than the average human's reaction time can allow. A report by the United Stated Department of Transport shows that applications which use V2X communication, such as Emergency Brake Warning, Left-turn Assist, and Lane-change Assist, can help reduce unimpaired vehicular collisions by as much as 80% [3]. Further, V2X applications like Cooperative Platooning and Emergency Vehicle Path Clearing offer improved fuel efficiency, traffic efficiency, and faster response times for emergency vehicles [67, 55]. For these reasons, V2X communication has garnered significant interest from the automotive industry, the research community and governments in recent years.

While V2X communication offers many benefits, unsecured V2X communication can also be exploited by adversaries to increase traffic congestion, track vehicles and people, and even induce vehicular crashes as we show in this thesis. For these reasons, it is necessary to secure VANETs and V2X communication. While security standards for V2X communication exist, their restrictive requirements can make implementing efficient applications difficult. Further, V2X application designers often design applications with little regard to security (incorrectly assuming that the standardised security measures provide adequate security regardless of the underlying application), resulting in applications that violate the security standards imposed restrictions, and leading to applications which are not secure. The Emergency Brake Warning application is one application affected by this disconnect between application designers and V2X security standards.

This thesis introduces the uninitiated reader to V2X communication, V2X applications, and V2X security standards while describing the necessary cryptography along the way. Then we discuss the working and limitations of current proposals for the Emergency Brake Warning application before describing EBW-PoF, a novel protocol for the same application, that overcomes these shortcomings. Finally, we discuss EBW-PoF's security, performance, and limitations.

Acknowledgements

First and foremost, I would like to thank my supervisors, Koray Karabina and Alfred Menezes. Their support and guidance over the last two years have been crucial for my growth as a researcher and for my professional development. This thesis would not be possible without them.

I want to thank Douglas Stebila for teaching me about cryptographic protocols in CO 789. CO 789 allowed me to learn about and research the use of pseudonymous certificates in vehicular networks; Section 4.2.1 and Section 4.3 of this thesis borrow content from a report I wrote for the same course.

I would like to thank the members of the team working on the "Quantum Secure Cryptographic Primitives with Applications to Vehicle-to-Vehicle Networks" collaborative project between the National Research Council of Canada and the University of Waterloo: Edward Eaton, Koray Karabina, Philippe Lamontagne, Sarah McCarthy, Michele Mosca, Geovandro Pereira, and Taufiq Rahman. I am grateful to the members of this fantastic team for their stimulating discussions and giving me the opportunity to help author an (as of yet unpublished) survey paper on V2X applications; the sections of this survey paper that I wrote lend themselves to Section 2.3 of this thesis.

Finally, I would like to thank David Jao and Douglas Stebila for reading my thesis.

The research presented in this thesis was supported by the National Research Council of Canada—University of Waterloo Collaborative Grant.

Table of Contents

Chapter 1

What is vehicular communication?

1.1 Introduction

Vehicular travel is an integral part of societal operations across the globe. Current data forecasts an escalating dependence, with the global vehicular count expected to rise from 1.32 billion in 2016 to a staggering 2.8 billion by 2036 [92]. Despite this increase in vehicles on the road, road safety has improved: the Nation Highway Traffic Safety Administration (NHTSA) reports a reduction in fatalities per 100,000 population in US resulting from motor accidents by 12.13% between 2005 and 2021 [65]. While a NHTSA report [41] attributes these trends to several factors, including enhanced road infrastructure and a reduction in vehicle ownership in urban areas, one of the key factors the report identifies is steady enhancement in vehicle safety, efficiency, and reliability over the years.

In recent decades, the automobile industry has undergone a significant transformation, underscored by an increased dedication of financial and technological resources toward "smart" vehicles [75, 50]. These smart vehicles promise a safer, superior driving experience. For instance, vehicle manufacturers have shown that integrating a camera and radar unit into a vehicle allows it to detect hazardous moving objects in its line of motion, which claim to reduce rear-end car crashes by up to 45% [66]. Modern automobiles feature an ever-increasing number of Electronic Control Units (ECUs)—embedded computers capable of sensing and actuating within the vehicle. Presently, standard models incorporate over 80 ECUs, while luxury versions can contain up to 150 [32, 91]. Astonishingly, the complexity of their software, measured in lines of code (LoC), surpasses that of the space shuttle, the F35 fighter jet, and the Hadron Collider, with a staggering 100 million LoC [51, 91]. The success of smart vehicles hinges on the fusion of hardware and software elements [92]: firstly, total integration of car sensors, known as sensor fusion; and secondly, the combination of high-definition mapping, high-accuracy navigation, artificial intelligence, and potent signal processing in information systems.

While automation systems are highly beneficial, they are not without limitations. Sensors may fail to detect objects hidden from the driver's and sensors' view or vehicles that behave unpredictably. In response to this issue, industry researchers and academic scholars have been exploring a technology called Vehicular Ad hoc Networks (VANETs). VANETs are wireless networks that can facilitate communication and collaboration among vehicles, pedestrians, and even roadside infrastructure such as traffic lights and dedicated road-side computational hardware called *Road-side Units* (RSUs). VANET-enabled communication[1], when coupled with embedded systems, like sensors and camera technologies that allow a vehicle to perceive and analyse its surrounding, can be used to design applications like Emergency Brake Warning Systems, Left-turn Assist Systems, and Cooperative Platooning Systems for enhancing road safety and vehicle efficiency. According to a US Department of Transport report, VANETs could potentially result in an impressive 80% decrease in vehicular collisions that result from unimpaired driving [3]. A report by the National Highway Traffic Safety Administration (NHTSA) predicts that the VANET enabled applications could prevent between 439,000 and 615,000 accidents every year thus saving 987 to 1366 lives and also preventing 537,000 to 746,000 property damage incidents annually [2]. A European Commission (EC) report similarly suggests that deploying VANETs could help reduce travel times and fuel consumption while enhancing traffic efficiency [1].

1.2 Roadmap

In Chapter 2 we explain the concept of VANETs and describe the use cases. Running V2X applications over unsecured VANETs leaves the applications and their users vulnerable to adversarial influence introducing a risk to user safety and privacy and a loss of efficiency; Chapter 2 precisely describes attacks that an adversary may mount against three popular V2X applications (Emergency Vehicle Path Clearing, Emergency Brake Warning, and Cooperative platooning) to highlight the importance of securing VANETs.

Thankfully, security standards to protect V2X applications and communication over VANETs exist. In Chapter 4, we give an overview of these standards and describe the cryptographic mechanisms these standards employ to protect V2X applications. (Chapter 3

[1] VANET-enabled communication is also often called Vehicle-to-Everything (V2X) communication. We describe V2X communication and similar forms of communication in Section 2.1.

overviews some relevant cryptography concepts for readers unfamiliar with cryptography to aid in understanding Chapter 4.)

While V2X security standards protect V2X applications from a broad class of attacks, they are not a silver-bullet solution for V2X security. Standardised V2X security mechanisms only operate at the physical[2] and the medium access control[3] layers; it is possible for a V2X application to make decisions at the application layer which compromise user security and privacy. Designing an efficient V2X application while remaining compliant with security standards can be tricky; Emergency Brake Warning is one application where this efficiency/security compromise is particularly evident. Chapter 5 describes the shortcomings of some proposed designs for Emergency Brake Warning systems and presents EBW-PoF, a new protocol for Emergency Brake Warning, which overcomes these shortcomings. We also discuss the security, performance, and limitations of EBW-PoF.

[2] The Open Systems Interconnection (OSI) model is an abstract model which splits communication on computer networks into seven layers and provides a basis for coordinating system connections and standards development. The lowest layer of the OSI model is the physical (PHY) layer which provides an interface to the physical medium of transmission handle transferring data between the medium of transmission and a device such as a Ethernet hub or a network switch.

[3] The medium access control (MAC) layer exists one layer above the PHY layer. This layer controls how devices in a network gain permission to transmit data over a medium of transmission.

Chapter 2

Introduction to VANETs and V2X Communication

2.1 VANETs

VANETs can be implemented using technologies such as DSRC[1] and 5G to enable several communication modes to automate the transfer of vehicular information:

- Vehicle-to-Vehicle (V2V): Direct communication between vehicles via 5G and DSRC.
- Vehicle-to-Infrastructure (V2I): Communication between vehicles and infrastructural components like traffic lights and road-side units (RSUs) via 5G and DSRC.
- Vehicle-to-Person/Pedestrian (V2P): Communication between vehicles and other road users, such as pedestrians or cyclists via 5G.
- Vehicle-to-Network (V2N): Communication between vehicles and network entities via a mobile network base station via 5G.
- Infrastructure-to-Network (I2N): Communication between an infrastructure unit and network entities via a mobile network via 5G.

[1] *Dedicated Short Range Communication* is a technology developed for vehicular communication which is similar to Wi-Fi. We discuss it further in Section 2.2.1.

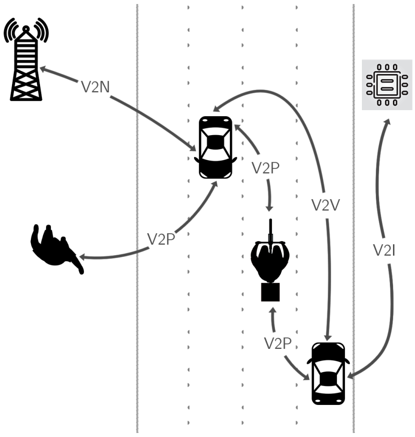


Figure 2.1: A schematic of a road depicting vehicles, a cyclist, and a pedestrian participating in the various forms of V2X communication.

V2X communication is a catch-all term which encompasses all the above modes of communication that VANETs enable (see Figure 2.1). Additionally, V2X communication refers to the various combinations of these modes of communications e.g. two vehicles communicating via a RSU which under the above categorisation would be neither V2V communication nor V2I communication. VANETs utilise these diverse communication modes to support a broad range of applications including emergency brake lights, pre-crash sensing, forward collision warning, left turn assist, lane-change warning, stop sign assist, and roadside service finder. Despite the varying nature and distinct communication needs of these applications, VANETs need to satisfy a set of general requirements to allow seamless V2X communication [84, 43, 78]:

Predictably Dynamic Topology VANETs must support an extremely dynamic network topology. At any given moment, a group of vehicles on the road, coupled with infrastructure and pedestrians, may form a VANET for V2X communication. Since vehicles can move at high speeds, the network's nodes can join and leave rapidly. While the influx and exit of nodes might appear random, transient nodes (vehicles and pedestrians) remain confined by road layouts and traffic regulations.

Large Network Size VANETs must support a high node density, such as during peak traffic periods. For instance, the network density on highways can reach up to 3000 nodes per square kilometre [14]. This requirement can pose a significant challenge due to the highly dynamic topology of VANETs.

Low Latency Highly critical applications like emergency brake lights, pre-crash sensing, blind intersection, and forward collision warning demand superior Quality of Service (QoS) compared to non-critical applications like left turn assist, lane-change warning, stop sign assist, and roadside service finder, which can operate sufficiently with more relaxed QoS parameters. Table 2.1 [92] lists various V2X applications and their network requirements.

Type	Application	Maximum latency (in ms)
Critical applications	Emergency brake warning	100
	Pre-crash sensing	20
	Blind intersection warning	100
	Forward collision	100
Non-critical applications	Left turn assist	100
	Lane-change warning	100
	Stop sign assist	100
	Roadside service finder	500

Table 2.1: Latency requirements of various critical and non-critical V2X-enabled applications [92].

Security and Privacy VANETs must guarantee the physical safety of drivers and pedestrians while ensuring that V2X communication does not compromise user security and privacy. We will delve deeper into these aspects later in this chapter.

To help ensure that VANETs can intercommunicate and to allow vehicles/pedestrians to participate in arbitrary VANET organisations, standards for V2X communication have been developed by organisations such as the Institute of Electrical and Electronics Engineers (IEEE) and the 3rd Generation Partnership Project (3GPP). Section 2.2 describes these standards with respect to the hardware technologies they employ to ensure compliant VANETs meet the latency, network size, latency, and topology requirements. We defer discussing how these standards meet the privacy and security requirements to Chapter 4.

2.2 Vehicular communication standards

In this section, we will discuss two competing standards for V2X communication developed by the Institute of Electrical and Electronics Engineers (IEEE) [6] and the 3rd

Generation Partnership Project (3GPP) [8], both designed to meet the requirements outlined in Section 2.1 that VANETs must satisfy.

2.2.1 IEEE

In 2010, the IEEE approved the amendment IEEE 802.11p [6] to standardise vehicular communication systems which was later incorporated in the IEEE 802.11 [9] standard in 2016. IEEE 802.11p modifies IEEE 802.11 to include a new operational mode known as Outside Context of a Basic Service Set (OCB). Unlike conventional 802.11 operation, the new OCB mode does not require authentication or association establishment. Furthermore, the absence of encryption implies that an adversary can transmit frames or monitor traffic in the vicinity at any time. This complete lack of security is intentional and designed to meet the low latency requirements of VANETs. IEEE 802.11p pertains to the PHY and MAC layers for WLAN-based V2V and V2I communications, and it assumes that security is provided at a higher layer (specifically by IEEE 1609 [12], which we will cover in Chapter 4). Dedicated Short-Range Communications (DSRC) and ETSI ITS-G5 [10] are two V2V/V2I communication protocols that comply with IEEE 802.11 in North America and Europe respectively.

DSRC and ITS-G5 are short-range wireless communications protocols operating in the 5.9-gigahertz (GHz) band. They support data transfer rates of about 6–27 megabits per second (Mbits/s) within a 300m range, with a latency time of less than 5 ms [93].

2.2.2 3GPP

Since 2014, the 3rd Generation Partnership Project (3GPP) has been standardising V2X communication on 4G LTE and later included 5G mobile cellular connectivity [8]. The PC5 interface (also known as the sidelink interface) offers an additional communication pathway, in addition to the existing Uu interface, between the User Equipment (UE) — the communication device used by vehicles and pedestrians — and the base mobile network station. This combination of short-range (PC5) and long-range (Uu) communications under the same system introduces a broad array of new use cases for cellular technology within the context of VANETs. This approach, leveraging 4G LTE or 5G technology for V2X communications is standardised under the 3GPP standard for Cellular V2X (C-V2X).

5G offers a peak bandwidth of approximately 20 Gbits/s and a sustainable download bandwidth of 1 Gbits/s. The sustainable upload bandwidth is around 10 Mbits/s with a peak bandwidth of 100 Mbits/s. Furthermore, 5G can achieve a latency of less than 1 ms [61].

2.2.3 DRSC/ITS-G5 vs C-V2X

The research community's understanding of what V2X communication is has evolved with time as researchers have proposed using different technologies for implementing VANETs thus changing their capabilities; earlier surveys offer a comprehensive overview of how V2X communication as an idea has evolved over the years [90, 91]. Vehicular communication standards, as proposed by IEEE, were initially based on V2V communication, where vehicles can communicate with other vehicles. Later, the standards were expanded to include V2I communication with infrastructure such as RSUs and traffic lights. When 3GPP proposed C-V2X, it introduced two new paradigms of V2X communication: V2P communication, allowing vehicles to communicate with pedestrians and V2N communication, allowing vehicles to communicate directly with mobile cellular networks. Adding V2N and V2P communication under the 3GPP standard was possible because C-V2X allows for both long-range and short-range communication under the same standard. Therefore, while both DSRC/ITS-G5 and C-V2X allow for V2X communication, the two standards target different communication scenarios by permitting different subsets of what is understood to be V2X communication.

2.3 V2X applications

This section explores how proposed V2X applications use VANETs to enhance driver safety, traffic efficiency, and environmental sustainability. We specifically focus on three V2X applications that have garnered significant attention from the engineering community and transportation industry in recent years and show great promise for future standardisation: Emergency Vehicle Path Clearing (EVPC), (Cooperative) Emergency Braking Warning (EBW), and Cooperative Platooning (CP).

Prior to the introduction of IEEE 1609, which provides data security mechanisms for IEEE 802.11p, some within the research community held the belief that, compromising the integrity of V2X messages could harm driver privacy and application efficiency but would not degrade the level of physical security enjoyed by vehicle drivers [25]. In other words, even unsecured V2X communication could only improve drivers' physical safety compared to the status quo of not employing VANETs and not reduce it. To motivate the need for

IEEE 1609 and securing V2X communication in general, we also describe concrete attacks against EVPC, EBW, and CP applications that leverage such a lack of data security to harm application efficiency, driver privacy, and driver safety.

The attacks described in this section will be discussed under the following assumptions:

Assumption 1. *There is a fixed set of vehicles and roadside units that maintain continuous connectivity with one another throughout the duration of their interaction.*

Assumption 2. *Vehicular systems are fully autonomous, meaning machines exclusively make driving decisions based on signals and data received via V2X communication and physical sensors. User input is not accepted.*

Assumption 3. *Cryptography is not deployed in the V2X network, thus not providing any encryption or digital signature mechanisms for the transmitted messages.*

These assumptions allow us to examine the possible security risks and vulnerabilities within VANETs, and how they could potentially impact the safety and the efficiency of these V2X applications: EVPC, EBW, and CP. The assumption of not deploying cryptography is necessary to demonstrate that secure communication mechanisms are integral to the design and safe operation of V2X application.

2.3.1 Emergency vehicle path clearing

Emergency vehicles such as police cars, ambulances, and fire trucks strive to minimise their response times to help save more lives. For instance, a UK study suggested that lowering the wait time from 14 minutes to 5 minutes for cardiac emergency care could reduce the fatality rate by 10-11% [71]. However, such faster response times often come at the cost of reduced visibility for other road users, sometimes resulting in collisions [16]. According to reports, when ambulances get involved in such accidents, it typically leads to an average delay of 9.4 minutes for a patient's arrival at the hospital, as another ambulance has to be dispatched [33].

V2X communication systems could potentially enhance visibility and decrease response times for emergency vehicles [55, 34, 46]. By having an emergency vehicle broadcast its location and destination, a V2X application could provision an "optimal" route for an emergency vehicle using a two pronged approach: minimise congestion by having non-emergency traffic move over to congested lanes and minimise wait times at traffic lights by coordinating their states ahead of the emergency vehicle's arrival [55]. Such an optimal route is designed at the cost of increased non-emergency vehicle travel time; an ideal Emergency Vehicle Path Clearing (EVPC) application should only minimally impact non-emergency vehicle traffic.

Both simulation-based methods and field studies have been used to assess the efficacy of proposed EVPC applications. One such study [64] performed micro-simulation experiments with a prototype V2V system guiding real drivers to “move left”, “move right”, or “stay put”. The study found that preempting traffic signals through V2I communication reduced the emergency vehicle’s travel time by 11-37%. Adding V2V communication to V2I further reduced travel time by 20-32%.

An EVPC Attack Scenario: In the EVPC attack scenario, the adversary is a vehicle owner who gathers V2V messages over time and creates a message library from emergency response vehicles. These could be obtained simply by driving or setting up receivers on busy roadsides. The adversary could then analyse the message structure, forge emergency vehicle messages, and replay them to deceive other vehicles and traffic lights into clearing their path, thereby creating traffic congestion. Because of the lack of message authentication, other vehicles would not be able to distinguish forged messages from genuine ones, leading to a successful attack.

2.3.2 Emergency brake warning

V2V communication can be leveraged to warn vehicles when another vehicle on the road unexpectedly brakes with an early warning signal – such a forewarning can be particularly useful in adverse weather conditions and more generally in conditions which impede road visibility. Since the wireless communication channels employed by V2X communication are much faster than the human reaction time, a so-called Emergency Braking Warning (EBW) system can potentially improve road safety. Such warning messages can be delivered directly from one vehicle to another as in the case of vehicle-to-vehicle (V2V) communication or by using additional infrastructure such as road-side units (RSUs) as intermediaries as in the case of vehicle-to-everything (V2X) communication.

A problem that EBW systems have to solve is that of precision i.e. if a vehicle receives a brake warning message it must be able to ascertain its relevance. A warning is only relevant to a vehicle if it is following the warning broadcaster i.e. the warning broadcaster and the vehicle are in the same lane and the broadcaster is travelling ahead of the vehicle. One approach to implementing EBW applications solve the precision problem by employing cameras and character recognition technology (OCR) [80] to identify the license plate numbers of vehicles. Such a system would use the leading vehicle’s speed, vehicle type, and vehicle colour to increase the accuracy of license plate identification. Each vehicle in a lane would identify and broadcast the license plate of the vehicle it is following, allowing every vehicle to maintain a list of leading in-lane vehicles. Thus, in addition to the safety message, a vehicle would also broadcast a list of subsequent in-lane vehicles. Now, if a vehicle brakes due to an emergency, a warning could exclusively be issued to the vehicles following it.

Two EBW attack scenarios: In our first EBW attack scenario, the adversary is a malicious party in the network that scans and collects V2I and V2V messages over a period of time and builds up a library of EBW messages. As in the case of the EVPC attack, the adversary can build this library naturally by driving on the road or planting receivers on busy roadsides.

As in the EVPC attack scenario, the adversary can forge EBW messages and replay them at a later time. Due to the lack of message authentication, other vehicles in the network would be unable to distinguish forged messages from genuine ones and would follow the protocol as usual. Hence, the adversary would cause other vehicles to unnecessarily brake, which could induce traffic congestion, degrade traffic flow, or cause accidents, especially if the adversary mounts their attack at a large scale by replaying forged messages through their maliciously planted roadside units when roads are busy and slippery.

Our second EBW attack scenario applies to an EBW application used by vehicles that employ the camera/OCR [80] based techniques to determine vehicles they share the lane with. An adversary could be any user in the network, and they may process broadcasted V2X messages to harvest license plate numbers in bulk alongside their timestamped geolocation information. For example, an adversary places a receiver on a busy road and collects an extensive number of messages with sensitive context. Many jurisdictions permit license plate look-ups, allowing members of the general public to find personal information of a vehicle owner, such as their name and address [69, 82, 39]. The adversary can collect V2V data over an extended period of time to infer private information about drivers, such as their home, workspace, routines, and habits [49, 42].

2.3.3 Cooperative platooning

Cooperative platooning (CP), particularly truck platooning, has been the subject of numerous research projects, including CHAUFFEUR [47], SARTRE [29], and Energy ITS [29]. CP applications enable vehicles to drive in synchronised platoons by coordinating vehicular parameters such as position, velocity, acceleration, etc. Such platoons offer several advantages:

1. At higher speeds, such as on highways, fuel consumption is primarily impacted by vehicular aerodynamics and air drag. By reducing the inter-vehicular distance, air drag is minimised, leading to better fuel economy with potential energy savings as high as 25% [67]. Lower fuel consumption also translates to a decrease in vehicular pollutant emissions [86].

2. Smaller inter-vehicular gaps can increase roadway capacity [85].

3. Platoons can enhance driving safety, as inter-vehicular coordination allows for faster engine/braking system actuation than human reaction times permit [85].

Existing Automated Cruise Control (ACC) systems used in trucks and domestic vehicles have similar goals. These systems use sensor data from odometers, radars, and LiDARs to automate vehicular velocity and acceleration [85]. However, ACCs have their limitations due to their reliance on sensor data. For instance, sensors have a limited range, only accounting for the behaviour of immediate neighbouring vehicles. Additionally, sensor accuracy can be highly weather-dependent, leading to inconsistent ACC performance.

Proposed CP applications like Cooperative Adaptive Cruise Control (CACC) aim to enhance ACCs by using V2V networks allowing platoon member to communicate wirelessly. Wireless communication is faster and more reliable than sensor-based technologies, enabling platoon members to drive closer together without an increased risk of collision, thereby further reducing air drag and improving fuel efficiency.

While platooning and CACC are closely related and often used interchangeably in the literature, there are subtle differences in their definitions, capabilities, and objectives. These differences aren't pertinent to the subject of this thesis; interested readers may refer to [67] for a more nuanced treatment of the matter.

The flow of wirelessly communicated information in a platoon can follow a variety of topologies [85], as seen in Figure 2.2. The information a vehicle receives significantly impacts how the CP application models the platoon's vehicular dynamics and its predictive capabilities. The information that any given vehicle in the platoon receives greatly affects how the CP application models the platoon's vehicular dynamics and the predictive capabilities of the CP application. While different platoon topologies model platoon dynamics differently [52, 74, 87], here we include an equation which describes the dynamics of a vehicle in a cooperative platoon with bidirectional communication [52]:

$$\begin{bmatrix} \dot{e}_i \\ \dot{v}_i \\ \dot{a}_i \\ \dot{u}_i \end{bmatrix} = \begin{matrix} A \begin{bmatrix} e_i \; v_i \; a_i \; u_i \end{bmatrix}^T \\ + \\ B \begin{bmatrix} v_{i-1} \; v_{i+1} \; a_{i+1} \; u_{i-1} \; u_{i+1} \; \dot{u}_{i+1} \end{bmatrix}^T \end{matrix},$$

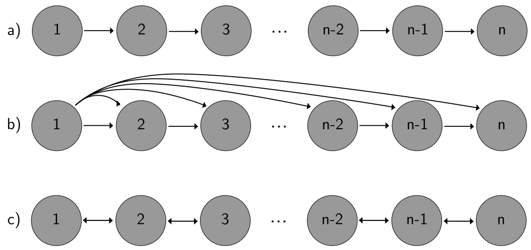


Figure 2.2: An n-vehicle platoon communication using various network topologies [85]: (a) predecessor following, (b) predecessor-leader following, and (c) bidirectional.

where e_i, v_i, a_i, and u_i represent respectively the error state, the velocity (m/s), the acceleration (m/s^2), and the desired acceleration of the preceding vehicle to the i^{th} vehicle in the platoon; A and B are vehicle-specific constant matrices of appropriate dimensions; and $\dot{x}$ is the rate of change of any parameter x. In particular, v_{i-1}, v_{i+1}, a_{i+1}, u_{i-1}, u_{i+1}, and $\dot{u_{i+1}}$ are entirely dependent on the information that a vehicle receives wirelessly and hence represent the effect that the neighbouring platoon members have on a particular vehicle's dynamics — causing it to speed up, slow down, or even halt. Consequently, controlling the information that a particular vehicle receives can allow one to control its dynamics in a mathematically precise sense.

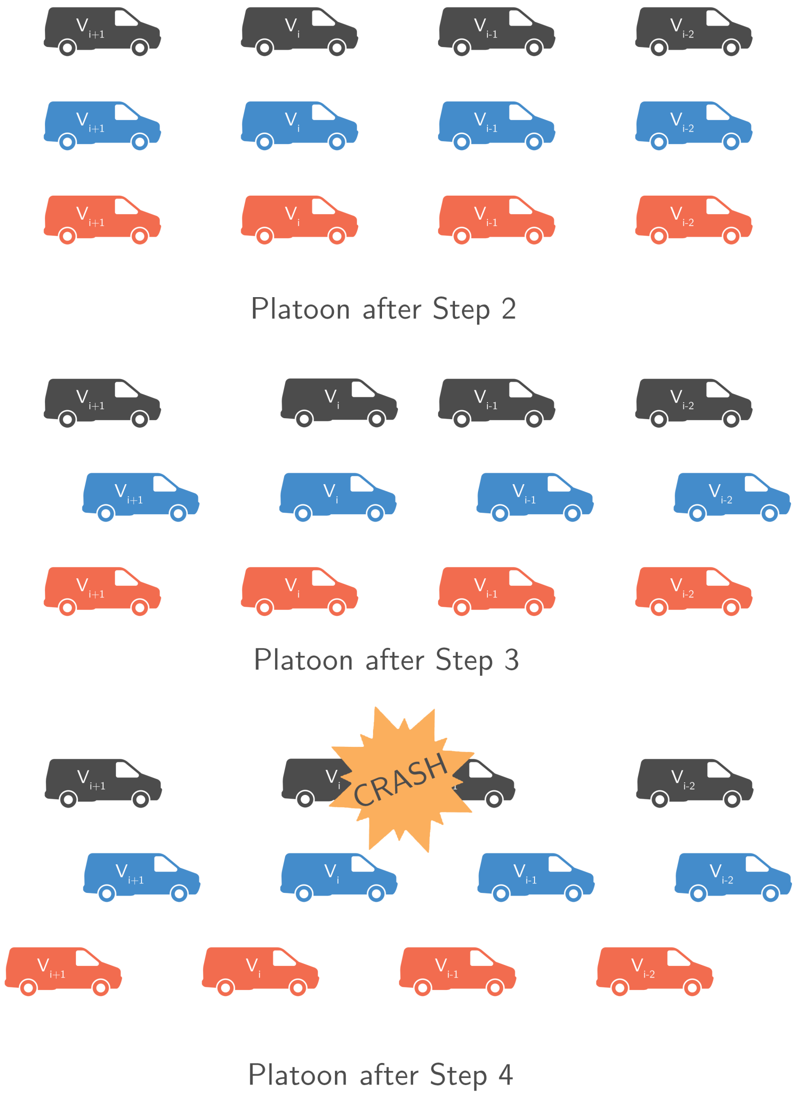
A CP attack scenario: In addition to Assumption 1, Assumption 2 and Assumption 3, our proposed CP attack makes the following assumptions.

Assumption 4. *Every V2X message received by a vehicle is perceived as genuine and is processed by its OBU; in the context of a CP application such a message would result in engine actuation.*

Since according to Assumption 3 VANETs don't employ cryptography, vehicles are unable to distinguish genuine messages from fraudulent/malicious ones and must treat all messages as genuine. The vehicle must then use the information it receives wirelessly to alter its acceleration in accordance with requirements of the platoon topology's underlying mathematical model.

Assumption 5. *The number of V2V messages a vehicle's OBU may process in any interval of time is limited; these messages are processed in a first-in-first-out manner.*

Since OBUs are computationally constrained they can only carry out a finite number of instruction per second. If the number of messages an OBU receives exceeds this limit the



Platoon after Step 2

Platoon after Step 3

Platoon after Step 4

Figure 2.3: This figure captures the state of the platoon after the various steps of the attack described in Section 2.3.3. The state of the platoon in the black, blue, and red rows is consistent with (a) the state of the platoon as it actually would be, (b) the state of the platoon as thought of by vehicle V_i, and (c) the state of the platoon as thought of by vehicle V_{i-1} respectively.

OBU must then be selective about which messages to process. We simplify our analysis by assuming an OBU processes the instructions it receives in a first-in-first-out manner.

Assumption 6. *A vehicle receives information from multiple channels – data from the vehicle's sensors and V2V data. When these channels are not in agreement, priority is given to V2V data over sensory data.*

Since designers of vehicle automation systems contend that proposed CP applications are more efficient and safer than ACC system because of additional V2V data being made available to a vehicle, we make the assumption that such conflicts are resolved in favour of V2V data. In other words, a vehicle "believes" the V2V data it receives more than it "believes" the data it receives from its sensors. We note that while this assumption is simplistic; engineers may employ heuristics to dynamically determine which channels of information to trust. Such heuristic mechanisms can be highly effective, however, analysing them is beyond the scope of this thesis. By making Assumption 6 we choose to focus on the role cryptography plays in the security of the CP application.

Under Assumption 4, Assumption 5 and Assumption 6, we now define the adversary's capabilities. The victim vehicle must treat every message sent by the adversary as genuine (Assumption 4); consequently each such fabricated message would result in engine actuation even though these fabricated messages may not be consistent with the sensor data received by the vehicle (Assumption 6). The adversary may inundate the victim vehicle with false messages by casting them at a high frequency; since the victim vehicle may process only a limited number of messages (Assumption 5) it becomes likely that the victim vehicle is forced to drop genuine messages in favour of forged ones. In this manner the adversary may actuate the victim vehicle's engine with greater frequency than legitimate platoon members — this attack models this as the adversary's ability to cause a victim vehicle to accelerate or decelerate.

While the adversary may assume various forms (malicious roadside units, a proximate vehicle external to the platoon, or even malicious drone perched atop a platoon member) for the sake of clarity we fix the adversary to be a collection of malicious roadside units appropriately positioned along the platoon's path. Now, consider the following attack scenario (see Figure 2.3):

1. The adversary observes a platoon and records the messages broadcasted by platoon members over period of time long enough to build a library of recorded messages and catalogue vehicle identifiers and discern V2V message structure. Equipped with this information, the adversary may now freely participate in the CP protocol by

broadcasting well-formed V2V messages (either by forging messages themselves or replaying recorded messages). Additionally, the adversary learns about the structure of the platoon, specifically its members and their order in the platoon.

2. The adversary targets vehicles V_i and V_{i-1} of an n-vehicle predecessor-following platoon: $V_n, V_{n-1}, \ldots, V_1$.

3. Masquerading as V_{i-1}, the adversary targets V_i with fraudulent messages which indicate a platoon speed-up. Consequently V_i accelerates to preserve platoon structure.

4. Masquerading as V_{i-2}, the adversary targets V_{i-1} with fraudulent messages which indicate a platoon slow-down. Consequently V_{i-1} decelerates to preserve platoon structure.

5. By sustaining the previously sent accelerate and decelerate commands for long enough the adversary may at least cause V_i and V_{i-1} to violate the minimum safety distance requirement if not induce a crash between them.

Thus, an adversary may exploit unauthenticated channels to compromise driver safety and a platoon's fuel saving efficiency.

Chapter 3

Preliminary Cryptography

3.1 Introduction

The attacks on the EVPC, EBW, and CP applications described in Chapter 2 directly result from the underlying V2X communication being unsecured. The V2X messages transmitted over the network are not confidential or authenticated and may be tampered with in transit. This chapter aims to be a primer on the cryptography used by the IEEE 1609.2 and ETSI C-ITS standards to provide confidentiality, data integrity, and authentication for V2X communication.

Generally speaking, cryptography is understood to be the study of mathematical techniques for securing communication and providing confidentiality, data integrity, entity authentication, and data origin authentication. While modern cryptography has grown as a field to accommodate more exotic goals such e-voting, homomorphic encryption, and multi-party computation, our focus in this chapter will be on cryptographic primitives which provide the following security properties:

Definition 1 (Confidentiality [60])**.** *Confidentiality is a service used to keep the content of information from all but those authorised to have it.*

Definition 2 (Data integrity [60])**.** *Data integrity is a service that addresses the unauthorised modification of data and allows one to detect data manipulation by unauthorised parties.*

Definition 3 (Authentication [60])**.** *Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a* *communication should identify each other. Information delivered over a channel should be authenticated as to origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).*

By using cryptographic primitives which provide confidentiality, data integrity, and authentication to VANETs, V2X security standards aim to protect user privacy in addition to securing V2X communication. While privacy is often conflated with confidentiality, we use the term in the following sense:

Definition 4 (Privacy [72])**.** *Privacy is an entity's ability to control, edit, manage, and delete information about themself and decide when, how, and to what extent this information is communicated to others.*

In this chapter, we describe the cryptographic primitives used to achieve these security properties and what it means for each of these cryptographic primitives to be secure. It is necessary to clarify that we will be assessing the security of these cryptographic primitives in the computational security framework as opposed to the information theoretic security framework. Primitives that are information theoretically secure are proven to be secure[1] against adversaries with unlimited time and computation resources. On the other hand, cryptographic primitives that are computationally secure differ in two ways:

- They are proven to be secure against an adversary bounded in time and computational resources. The computational resources available to an adversary are dependent on the reigning computational paradigm — the adversary may only have access to a classical computer capable of running probabilistic polynomial-time algorithms[2] or a quantum computer. For each of the cryptographic primitives we introduce towards providing a security property, we shall discuss classical and quantum-safe alternatives.

- An adversary may break them with some probability. For a primitive to be practical, this probability of failure must be sufficiently small. Typically, the probability of failure for a secure cryptographic primitive is bounded above by a function negligible in the primitive's security parameter:

[1] It is worth noting that what it means for a primitive to be "secure" or "broken" is unique to each primitive. We shall define these terms more formally for each primitive as we proceed.

[2] A probabilistic polynomial-time algorithm runs in time polynomial in its input and may use randomness to return results that may be non-deterministic.

Definition 5 (Negligible function [56])**.** *We say that a polynomial $p : \mathbb{R} \to \mathbb{R}$ is positive if for all $x \in \mathbb{R}$ we have $p(x) > 0$. A function $f : \mathbb{N} \to \mathbb{R}^+$ is negligible if for every positive polynomial p there exists a $N \in \mathbb{N}$ such that for all $n > N$ it holds $f(n) \leq \frac{1}{p(n)}$.*

3.2 Secret-key cryptography

Traditionally, confidentially of data is provided using secret-key cryptography by means of secret-key encryption schemes. In this setting, the communicating parties share a secret key — the sender encrypts the plaintext message under the shared secret key to obtain a ciphertext which is then later decrypted by the recipient. The sender and receiver must establish a secure channel to transmit the secret key prior to initiating communication.

Definition 6 (Secret-key encryption scheme [56])**.** *A secret-key encryption scheme is a triple of probabilistic polynomial-time algorithms (Gen, Enc, Dec[3]) such that:*

1. *The key generation algorithm Gen takes as input the security parameter 1^n and outputs a key k.*
2. *The encryption algorithm Enc takes as input a key k and a message $m \in \{0,1\}^*$ and outputs a ciphertext c.*
3. *The deterministic decryption algorithm Dec takes as input a key k and a ciphertext c, and outputs a message m or a special symbol $\perp$ denoting failure.*

It is required that, except with negligible probability over k output by $\mathsf{Gen}(1^n)$, we have $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ for all messages $m \in \{0,1\}^*$.

A secure encryption scheme would prevent any adversary from learning partial information about a plaintext. This notion of security is mathematically expressed[4] as ciphertext indistinguishability. We consider two types of adversaries which run in polynomial-time

[3] Note that while the decryption algorithm Dec is technically a probabilistic polynomial-time algorithm it doesn't make use of randomness and is entirely deterministic.

[4] More accurately, an encryption scheme that prevents any adversary from learning partial information about plaintexts is *semantically secure*. While semantic security and ciphertext indistinguishability are equivalent notions of security, they have distinct definitions. Interested readers may refer to [56] for a detailed discussion on the matter.

and exercise a partial degree of control over what an honest party encrypts and decrypts. The first notion of security, called IND-CPA security, is against a chosen plaintext attack where the adversary can influence which plaintexts the honest party encrypts; this ability is modelled by giving the adversary access to an encryption oracle. The first notion of security, called IND-CPA security, is against chosen plaintext attacks where the adversary can influence which plaintexts the honest party encrypts; this ability is modelled by giving the adversary access to an encryption oracle.

Definition 7 (IND-CPA [56])**.** *A secret-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to be indistinguishable under chosen plaintext attack (or IND-CPA secure) if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is is a negligible function* negl *such that*

$$\Pr[\mathsf{SecK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where $\mathsf{SecK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ *is the plaintext indistinguishability experiment (see Figure 3.1).*

```
$\mathsf{SecK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ [56]
1 : $\mathsf{Gen}(1^n)$ is run to obtain the key $k$.
2 : The adversary $\mathcal{A}$ is given $1^n$ and access to an encryption oracle $\mathsf{Enc}_k(\cdot)$, and
    outputs a pair of messages $m_0$ and $m_1$ of same length.
3 : A uniform bit $b \in \{0,1\}$ is chosen and then ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is
    computed and given to $\mathcal{A}$.
4 : $\mathcal{A}$ continues to interact with the encryption oracle and outputs a bit $b'$.
5 : The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise.
```

Figure 3.1: The chosen plaintext indistinguishability experiment $\mathsf{SecK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$.

The second notion of security, called IND-CCA security, is against chosen ciphertext attacks where the adversary can influence which plaintexts the honest party encrypts and also which ciphertexts the honest party decrypts; in addition to an encryption oracle the adversary also has access to a decryption oracle.

Definition 8 (IND-CCA [56])**.** *A secret-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to be indistinguishable under chosen ciphertext attack (or IND-CCA secure) if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is is a negligible function* negl *such that*

$$\Pr[\mathsf{SecK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where $\mathsf{SecK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ *is the plaintext indistinguishability experiment (see Figure 3.2).*

$\mathsf{SecK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ [56]

```
1 : $\mathsf{Gen}(1^n)$ is run to obtain the key $k$.
2 : The adversary $\mathcal{A}$ is given $1^n$ and access to oracles $\mathsf{Enc}_k(\cdot)$ and $\mathsf{Dec}_k(\cdot)$;
    $\mathcal{A}$ outputs a pair of messages $m_0$ and $m_1$ of same length.
3 : A uniform bit $b \in \{0,1\}$ is chosen and then ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ is
    computed and given to $\mathcal{A}$.
4 : $\mathcal{A}$ continues to interact with oracles $\mathsf{Enc}_k(\cdot)$ and $\mathsf{Dec}_k(\cdot)$ but may not request
     a decryption of $c$ itself. Finally, $\mathcal{A}$ outputs a bit $b'$.
5 : The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise.
```

Figure 3.2: The chosen ciphertext indistinguishability experiment $\mathsf{SecK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$.

While Definition 7 and Definition 8 define what it means for a secret-key encryption scheme to be secure, they do not inform us on how to construct such a scheme. Describing how to construct a secure secret-key encryption scheme is beyond the scope of this thesis; however, we do describe one mathematical primitive that cryptographers use to construct them — *pseudorandom functions*.

A pseudorandom function describes a distribution of functions such that sampling from it produces a "random-looking" function. In other words, a function from sampled from a pseudorandom function family should be hard to distinguish from a function sampled uniformly from the set of all functions [56]. Before describing a pseudorandom function, we introduce a helpful mathematical definition.

Definition 9 ([22])**.** *For a set X, $\mathsf{Funs}[X]$ is the set of all functions $f : X \to X$.*

Definition 10. *A pseudorandom function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is secure if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function negl such that*

$$\Pr[\mathsf{PRF}^{\mathsf{adv}}_{\mathcal{A},F}(n) = 1] \leq \mathsf{negl}(n),$$

where $\mathsf{PRF}^{\mathsf{adv}}_{\mathcal{A},F}$ is the pseudorandom function distinguishing experiment (see Figure 3.3).

Pseudorandom functions are instantiated using deterministic algorithms called block ciphers[5] such as the Advanced Encryption Standard (AES) which are then used to construct symmetric-key encryption schemes[6].

[5] More accurately, block ciphers instantiate *pseudorandom permutations.* A permutation from pseudorandom permutations is indistinguishable from uniformly random permutation.

[6] Symmetric-key encryption schemes are also constructed using a class of function families similar to

$\mathsf{PRF}^{\mathsf{adv}}_{\mathcal{A},F}(n)$ [22]

```
Let $f_0 = F(k, \cdot)$ where $k$ is uniformly sampled from $\{0,1\}^n$, and let $f_1$ be uniformly sampled from $\mathsf{Funs}[\{0,1\}^n]$.
A uniform bit $b \in \{0,1\}$ is chosen and the adversary $\mathcal{A}$ is given access to an $f_b$ oracle.
$\mathcal{A}$ continues to interact with the oracle outputs a bit $b'$.
The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise.
```

Figure 3.3: The pseudorandom function distinguishing experiment $\mathsf{PRF}^{\mathsf{adv}}_{\mathcal{A},F}(n)$.

3.3 Public-key cryptography

Public-key cryptography is the primary cryptographic mechanism used by V2X security standards to provide confidentiality, data integrity — public-key encryption schemes provide confidentiality and digital signature schemes provide data integrity and authentication. We briefly introduce public-key encryption and digital signature schemes before describing how to manage public-key cryptography at scale.

3.3.1 Public-key encryption

A *public-key encryption scheme* assigns an entity a public key and a private key. Anyone holding a public key can encrypt a plaintext message to a ciphertext. However, the ciphertext can only be decrypted by someone holding the corresponding private key. Assuming the entity holding the private key is the intended recipient, public-key encryption ensures the confidentiality of the plaintext message.

Definition 11 (Public-key encryption scheme [56])**.** *A public-key encryption scheme is a triple of probabilistic polynomial-time algorithms (*Gen*,* Enc*,* Dec[7]*) such that:*

1. *The key generation algorithm* Gen *takes as input the security parameter* 1^n *and outputs a pair of keys (pk, sk) called the public key and private key respectively.*

pseudorandom functions called *pseudorandom generators*. Pseudorandom generators are instantiated using stream cipher algorithms such as ChaCha20. We don't discuss pseudorandom permutations and stream ciphers here since they are not relevant to the discussion in this thesis. However, interested readers may refer to [56].

[7] Note that while the decryption algorithm Dec is technically a probabilistic polynomial-time algorithm it doesn't make use of randomness and is entirely deterministic.

2. *The encryption algorithm* Enc *takes as input a public key* pk *and a message* m *from the message space (the message space may depend on* pk*), and outputs a ciphertext* c*.*

3. *The deterministic decryption algorithm* Dec *takes as input a private key* sk *and a ciphertext* c*, and outputs a message* m *or a special symbol* $\perp$ *denoting failure.*

It is required that, except with negligible probability over $(pk,\, sk)$ *output by* $\mathsf{Gen}(1^n)$*, we have* $\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m$ *for all messages* m *from the message space corresponding to* pk*.*

Similar to secret-key encryption schemes, the security of public-key encryption schemes is evaluated by measuring indistinguishability of ciphertexts under chosen-plaintext and chosen-ciphertext attacks.

Definition 12 (IND-CPA [56])**.** *A public-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to indistinguishable under chosen plaintext attack (or IND-CPA secure) if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is is a negligible function* negl *such that*

$$\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where $\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ *is the plaintext indistinguishability experiment (see Figure 3.4).*

$\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ [56]

1 : $\mathsf{Gen}(1^n)$ is run to obtain keys $(pk,\, sk)$.

2 : The adversary $\mathcal{A}$ is given pk outputs a pair of messages m_0 and m_1 in the message space associated with pk.

3 : A uniform bit $b \in \{0, 1\}$ is chosen and then ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$.

4 : $\mathcal{A}$ outputs a bit b'. The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise.

Figure 3.4: The chosen plaintext indistinguishability experiment $\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$.

Definition 13 (IND-CCA [56])**.** *A public-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to indistinguishable under chosen ciphertext attack (or IND-CCA secure) if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is is a negligible function* negl *such that*

$$\Pr[\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ *is the plaintext indistinguishability experiment (see Figure 3.5).*

$\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ [56]

```
1 : $\mathsf{Gen}(1^n)$ is run to obtain keys $(pk, sk)$.
2 : The adversary $\mathcal{A}$ is given $pk$ and access to a decryption oracle $\mathsf{Dec}_{sk}(\cdot)$, and
    outputs a pair of messages $m_0$ and $m_1$ in the message space associated with $pk$.
3 : A uniform bit $b \in \{0, 1\}$ is chosen and then ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ is
    computed and given to $\mathcal{A}$.
4 : A continues to interact with the decryption oracle but may not request a
    decryption of $c$ itself. Finally, $\mathcal{A}$ outputs a bit $b'$.
5 : The output of the experiment is defined to be 1 if $b = b'$, and 0 otherwise.
```

Figure 3.5: The chosen ciphertext indistinguishability experiment $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$.

Unlike secret-key encryption schemes, public-key encryption schemes do not require the communicating parties to exchange a key prior to communicating. On the hand, other secret-key encryption schemes are faster than public-key encryption schemes and allow for reduced communication bandwidth. For these reasons, secret-key and public-key encryption are used together to make hybrid encryption schemes under the so-called KEM/DEM paradigm. Communicating parties can use a public-key encryption scheme as a Key Encapsulation Mechanism (KEM) to exchange a shared key; this shared key can then be used to encrypt messages with a secret-key encryption scheme called the Data Encapsulation Mechanism (DEM).

3.3.2 Digital signatures

Like public key encryption schemes, digital signature schemes provide entities with a pair of public and private keys. A sender can use their private key to sign a message; this signature can later be verified by anyone holding the corresponding public key. Assuming only the sender holds the private key associated with their identity, digital signatures provide data origin authentication. Additionally, digital signatures provide data integrity[8] — since a digital signature is created for a specific message, modifying the message in transit will cause the verification process to fail.

Definition 14 (Signature scheme [56]). *A signature scheme consists of three probabilistic polynomial-time algorithms (*Gen*,* Sign*,* Vrfy*) such that:*

1. *The key generation algorithm* Gen *takes as input the security parameter* 1^n *and outputs a pair of keys (pk, sk) called the public key and private key respectively.*

2. *The signing algorithm* Sign *takes as input a private key sk and a message* m *from the message space (the message space may depend on pk) and outputs a signature* σ*.*

3. *The deterministic verification algorithm* Vrfy *takes as input a public key pk, a message* m*, and a signature* σ*; and outputs* 1 *if the signature is valid, and 0 otherwise.*

It is required that, except with negligible probability over (pk, sk) output by $\mathsf{Gen}(1^n)$*, we have* $\mathsf{Vrfy}_{pk}(m, \mathsf{Sign}_{sk}(m)) = 1$ *for all messages* m *from the message space corresponding to pk.*

Signature schemes are designed to prevent forgeries. A forgery is a pair consisting of a message m and σ, a valid signature on m under the secret key sk, where m was not previously signed by the holder of sk. The notion of security is mathematically expressed as (weak) existential unforgeability — an adversary is unable to produce a forgery despite obtaining many valid signatures from the signer on messages of the adversary's choosing.

Definition 15 (EUF-CMA2 [56]). *A signature scheme* $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *is said to be (weakly) existentially unforgeable under adaptive chosen message attack (or EUF-CMA2 secure) if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, there is a negligible function* negl *such that*

$$\Pr[\mathsf{Sig}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n),$$

where $\mathsf{Sig}_{\mathcal{A},\Pi}$ *is the (weak) existential unforgeability experiment (see Figure 3.6).*

[8] Secret-key primitives such as authenticated encryption schemes and Message Authentication Codes also provide data origin authentication and data integrity. However, we don't describe them here as the discussion in later chapters of this thesis doesn't depend on these constructions. Instead readers may refer to [56] for an introduction to these primitives.

$\mathsf{Sig}_{\mathcal{A},\Pi}(n)$ [56]

```
$\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).
The adversary $\mathcal{A}$ is given $pk$ and access to a signing oracle $\mathsf{Sign}_{sk}(\cdot)$. Let
  $\mathcal{Q}$ denote the queries that $\mathcal{A}$ makes to the oracle
$\mathcal{A}$ outputs $(m, \sigma)$.
The experiment outputs 1 if $\mathsf{Vrfy}_{sk}(m, \sigma) = 1$ and $m \notin \mathcal{Q}$, else it outputs 0.
```

Figure 3.6: The (weak) existential unforgeability experiment $\mathsf{Sig}_{\mathcal{A},\Pi}(n)$.

3.3.3 Constructing public-key cryptosystems

The security of public-key cryptosystems, such as encryption schemes and signature schemes, hinges on the assumed hardness of certain mathematical problems. Widely used cryptosystems such as RSA, DSA, ECDSA, Diffie-Hellman, and ECDH assume the intractability of integer factoring, the Diffie-Hellman problem, and the discrete log problem in certain groups. Since the hardness of these problems is only assumed and not proven, no unconditional proofs of security are known for these cryptosystems. Despite this, these cryptosystems have wide usage since no known algorithms for efficiently solving these problems are known. However, the situation changes when adversaries have access to quantum computers; Shor's algorithm allows quantum computers to solve these problems efficiently, thus breaking modern cryptosystems.

The recent National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization is a program by NIST to update cryptographic standards to support quantum-safe cryptography. While, like classical cryptography algorithms, these newer post-quantum algorithms do not have unconditional proofs of security their security proofs assume the hardness of mathematical problems which cannot be solved efficiently by any known quantum algorithm. We present the eight unbroken algorithms that were selected in 2022 by NIST and those that were selected for round 4 [79, 19]:

Lattice-based [23, 37, 40] Lattice-based cryptosystems rely on the hardness of a few mathematical problems for their security: the LWE and SIS problems and their variants. The Kyber KEM was selected by NIST in 2022; it offers IND-CCA security. The Dilithium and Falcon signature schemes were selected by NIST in 2022 as well.

Code-based [20, 59, 15] The security of code-based KEMs depends on the hardness of decoding a general linear code. The ciphertext in such systems is a codeword with some added errors; only the holder of the secret key can remove these errors. Classic McEliece was selected as one of the winners by NIST in 2022; HQC and BIKE are a part of Round 4 of the standardisation process which was started in July 2022 and continues into July 2023. Classic McEliece and HQC offer IND-CCA security while BIKE offer IND-CPA security.

Hash-based [21] Hash-based signature schemes, like other signature schemes, are constructed using a cryptographic hash function, and their security depends on the collision resistance of that hash function. The SHPINCS+ signature scheme is hash-based and was selected as a winner by NIST in 2022.

3.3.4 Public-key infrastructure

While public-key cryptography allows users to communicate securely without having to negotiate a key over a secure channel, it can only be used in practice if its users trust the authenticity of public keys. Alice might encrypt a message under Bob's public key, but if the authenticity of Bob's key is not guaranteed, the adversary Eve may have replaced Bob's key with their own key at some point since cryptographic keys are not tied to entities in any way. Alice could establish a secure channel with Bob directly to get their key, thus establishing direct trust in the key. However, relying solely on direct trust would make public-key cryptography impractical and considerably slow communication.

Public Key Infrastructures (PKIs) offer a solution to this problem. PKIs create public repositories of data structures called cryptographic certificates; certificates tie cryptographic keys to entities by encoding the following information [26]:

Identity The entity to which the public key in the certificate is bound. This identity may also be pseudonymous.

Public Key The public key bound to the entity.

Algorithm The cryptographic algorithms with which the public is to be used.

Serial Number The serial number of the certificate.

Valid Period The time period within which the certificate is valid.

Issuer The identity of the certificate issuer.

Now, Alice can access Bob's public-key certificate from a PKI and choose to use the encoded public key if they trust the issuer. Such trusted certificate issuers are called Certificate Authorities (CAs) in the context of PKIs. Certificates are signed by the CA and can be verified using the CA's public key. Thus, instead of having to rely on direct trust to communicate with Bob, Oscar, and Eve, Alice can now rely on the CA and expect the CA to verify the authenticity of each party's public keys. To scale better with the number of users PKIs are often hierarchically implemented with multiple CAs [26] — every CA is verified by another CA, establishing a chain of trust that culminates in a single trust anchor.

In addition to providing trust, PKIs handle the administrative responsibilities associated with managing cryptographic certificates [26]:

Bootstrapping devices Enrolling devices into the PKI and providing them with the necessary information to communicate with the PKI and other devices enrolled in the PKI.

Provisioning certificates Generating cryptographic keys, issuing certificates to bootstrapped devices, and issuing new certificates when a device's certificate expires.

Revoking certificates Revoking issued certificates that are still valid to enforce device blockage and mitigate effects of private-key compromise.

Chapter 4

Security Standards for V2X Communication

4.1 Introduction

Vehicle-to-Everything (V2X) communication promises to improve road safety and efficiency dramatically. However, it also introduced tough challenges concerning safeguarding users' physical security and privacy.

As discussed in Chapter 2, ensuring the authenticity of V2X messages is a serious concern. Without cryptographic authentication, adversaries can forge and replay V2X messages, impacting V2X application efficiency and endangering user safety. This problem is not new. A historical example of a similar issue is faced by Controller Area Network (CAN) buses, which are integral components in modern vehicles and responsible for communication between various Electronic Control Units (ECUs). Notably, CAN buses do not employ any security mechanisms including cryptographic encryption and authentication, leaving them susceptible to potential security breaches [63]. Researchers have shown that the absence of cryptographic authentication and software flaws in ECUs can be exploited in real-world scenarios, severely compromising the safety of vehicles and their occupants [31, 57]. Further, even a small number of compromised vehicles can severely disrupt road safety and infrastructure [83]. This issue is particularly relevant to VANETs as the wireless, long-distance nature of V2X communication would add to adversarial power, making it easier to mount such attacks.

Privacy is equally essential in VANETs. Without privacy protection, vehicles can be remotely tracked, and data about drivers can be gathered without permission. For instance, previous work by Hoh et al. [49] showed that a vehicle's trip's start and end points are often linked to the owner's home address. Additionally, analysis of US Census data [42] showed that narrowing down a person's home and work addresses to a block level effectively removes their anonymity. While such forms of tracking are currently possible using cameras, the wireless nature of V2X communication would only make such unauthorised tracking easier.

These issues highlight the need for V2X communication technologies to guarantee data integrity, authenticity, and user privacy. Researchers have proposed two categories of solutions towards meeting these goals: certificate-based techniques and certificateless techniques [77, 48]. While the certificateless approach is novel (leading to new constructions such as Non-Bilinear Conditional Privacy-Preserving Authentication [48]), this thesis will focus on certificate-based techniques as they form the basis of the the standards which aim to secure V2X communication [12, 10]. In particular, we will study the IEEE 1609.2 [12] and ETSI C-ITS [10] standards — the current proposals to secure V2X communication over VANETs in the USA and EU. We don't discuss the security architecture for 3GPP-CV2X as it hasn't been standardised yet [7].

4.2 Security management systems

The IEEE 1609.2 and ETSI C-ITS standards address security and privacy challenges within V2X communication by implementing so-called Security Credential Management Systems (SCMSs). Both SCMSs implement a Public Key Infrastructure (PKI) to manage cryptographic certificates for end-entities (vehicles, pedestrians, and RSUs) by bootstrapping, provisioning, and revoking certificates [25] (see Section 3.4). End-entities with certificates can then use public-key cryptography to enjoy the trust services associated with a PKI: confidentiality, integrity, and authenticity. The SCMS thus helps ensure user safety and counters potential attacks that could disrupt traffic flow or degrade communication efficiency. IEEE 1609.2 and ETSI C-ITS also detail the cryptographic data services available for securing V2X application messages (data signing and verification processes for authentication and integrity, encryption and decryption procedures for confidentiality using asymmetric public keys) that applications can invoke to ensure end-to-end security. When using these cryptographic security services, V2X applications must adhere to specific message formats and processing described by the same standards.

As mentioned earlier, these SCMSs must also support detecting misbehaving end-entities (devices publishing authenticated malicious messages that result in false warnings) and revoking their certificates. The various end-entities enrolled in the SCMS are responsible for detecting and identifying device misbehaviour or malfunction at a local level. Once detected, this information is reported to the SCMS; the SCMS then revokes the certificates associated with the misbehaving devices. Revocation is enforced by the SCMS through the distribution of a Certificate Revocation List (CRL). This list contains updated entries that indicate which certificates have been revoked. Devices rely on the CRL to identify and reject messages coming from these revoked devices, effectively blocking their communication. Furthermore, the SCMS maintains its own internal blacklists to deny any future certificate requests made by these devices.

While such a PKI-based system is in many ways a natural choice for securing V2X communication over a VANET, it introduces two challenges with regard to user privacy [25]:

Attacks on user privacy from outsiders: The very nature of V2X communication opens up users to being tracked. An adversary may attack the privacy of an end-entity by recording all V2X messages linking its cryptographic identity to the location where a specific message was recorded thus tracking the end-entity over physical distances.

Attacks on user privacy from insiders: Since the SCMS is responsible for revoking certificates, all the information required to resolve the identity of an end-entity using specific cryptographic credentials must necessarily be stored on the SCMS. An adversary with privileged access to the SCMS or associated infrastructure where this information is stored, such as an employee, may exploit this identity resolution information to link a cryptographic identity to a specific end-entity and track it. A naive implementation of the SCMS would maintain a list of certificates issued to each device making such an insider attack trivial to implement.

We describe the measures taken by the designers of the IEEE 1609.2 and ETSI C-ITS SCMSs to mitigate such attacks against user privacy.

4.2.1 Protecting user privacy from SCMS outsiders

Communicating using V2X messages over VANETs naturally opens up vehicles to being tracked. An adversary can record all the V2X messages transmitted by a vehicle and attempt to reconstruct its path using the location data the messages may include. Alternatively, the adversary may choose to gather statistical data by recording V2X messages at select locations in an attempt to learn about the habits of drivers [27]. Such attacks are not prevented by deploying a traditional PKI, in fact, it is quite the opposite. A cryptographic signature on a message mathematically guarantees that the source of the message is authentic with high probability; this guarantee is enjoyed by both honest vehicles in the

VANET and adversaries eavesdropping on the network. An adversary who observes messages signed by the same credentials originating at distinct locations knows that a single vehicle must have travelled to those various locations.

To be clear, driver privacy is already vulnerable to such attacks—adversaries can physically tail vehicles to track them or use cameras equipped with Automatic License Plate Reader technology [36] to gather statistical data about specific locations—however, using VANETs for vehicular communication would make such attacks more accessible to malicious entities. Deploying a network of radio equipment to record wireless messages is cheaper and more inconspicuous than high-resolution cameras and human private investigators, thus, making such attacks easier to scale. In this section, we discuss the measures taken by the SCMS to mitigate the advantages that a VANET might confer to an adversary attacking user privacy.

Pseudonyms

In the attacks outlined earlier, the adversary successfully tracks down the vehicle by linking its actions across a physical distance — the adversary can tell whether messages recorded at two physically distant locations originated at the vehicle. To prevent such attacks against user privacy, the longer the time and distance between two message transmissions, the harder it should be for an adversary to determine if the transmissions originated at the same source. We would like for V2X messages transmitted by a vehicle to be unlinkable as defined by Pfitzmann and Hansen [73][1]:

Unlinkability Messages transmitted by vehicles enrolled within a VANET are unlinkable if an adversary cannot link them to a common source vehicle.

The SCMS aims to achieve this desired unlinkability through pseudonymity: a pseudonymous credential allows a device to authenticate its actions without containing any information linking the pseudonym to its long-term identity. Clearly, messages transmitted under the same pseudonym can be linked. However, a vehicle can cycle through the many pseudonyms provisioned to it by the SCMS, thus achieving message unlinkability and rendering the vehicle anonymous among the set of vehicles enrolled in the SCMS. In addition to unlinkability, a report by Schaub et al. [76] identifies the following privacy properties that pseudonyms must satisfy:

[1] Here, we restrict Pfitzmann and Hansen's more general definition of unlinkability of items of interest in a network (subjects, messages, actions, etc.) to the context of VANETs.

Minimum disclosure Pseudonyms must only reveal information about the vehicle that minimally satisfies the requirements for the normal functioning of V2X applications.

Conditional anonymity The SCMS must be able to resolve the long-term identity of a vehicle from the pseudonyms issued to the vehicle in the interest of blocking misbehaving vehicles from participating in the network and may also be needed to comply with requests from law enforcement agencies.

Perfect forward secrecy The resolution of a pseudonymous credential to a long-term identity must not reduce the unlinkability of the vehicle's other credentials.

These requirements balance user privacy (minimum disclosure and perfect forward secrecy) and user accountability (conditional anonymity). The IEEE 1609.2 and ETSI C-ITS SCMS pseudonym systems are designed with the following properties to satisfy the above requirements [25]:

Time-limit To ensure the unlinkability of messages across time, the pseudonym certificates provisioned to devices by the SCMS come with an expiry date which imposes a time limit on the validity of the pseudonym certificate.

Availability Devices are provided with a large batch of pseudonym certificates at once to guarantee the availability of a fresh pseudonym in case of a pseudonym change is needed.

Link to other identifiers When a device changes pseudonyms, it must also change all other network identifiers (such MAC address, IP address etc.) to ensure unlinkability of messages.

Pseudonym change block The ability to reject the pseudonyms issued to a misbehaving vehicle and block it from being provisioned with fresh pseudonyms.

While we restrict our discussion here to the PKI-based IEEE 1609.2 and ETSI C-ITS SCMS pseudonym systems in this thesis, all pseudonyms systems must satisfy this conflicting set of requirements between user privacy and accountability, leading to several similarities between their design and implementation. Petit, Schaub, Feiri, and Kargl [72] distil these similarities into the pseudonym lifecycle — issuance, use, change, resolution, and revocation. While pseudonym systems are not explicitly divided into these five stages at the time of design, we shall use the framework provided by the pseudonym lifecycle to describe the design and functioning of the IEEE 1609.2 and ETSI C-ITS SCMS pseudonym systems.

Pseudonym lifecycle

Issuance While the authentication scheme employed by the SCMS enforces message unlinkability through pseudonymity, vehicles must have a long-term identity called Vehicle Identifier that allows the vehicle to authenticate itself when requesting pseudonym certificates from the SCMS [12]. This long-term identity can be thought of as a digital licence plate for the vehicle; just as a vehicle registration authority oversees vehicle licence plate registry, the assigning of long-term identities to vehicles enrolled in the SCMS is overseen by the Enrollment Authority (EA). While long-term identities are essential for vehicles to be issued pseudonym certificates, the issuance of long-term identities itself is a separate process independent of the pseudonym lifecycle.

The actual issuance of pseudonyms to vehicles enrolled in the IEEE 1609.2 SCMS is overseen by multiple SCMS components: Linkage Authorities (LAs), Pseudonym Certificate Authority (PCA), and the Registration Authority (RA) [25]. These SCMS components issue pseudonym certificates to enrolled vehicles while retaining escrow information to allow resolving long-term identities of enrolled vehicles; long-term identity resolution is necessary for blocking misbehaving vehicles from participating in the SCMS and may also be needed to comply with requests from law enforcement agencies. Section 4.2.2 describes how this escrow information is spread across the LAs, the PCA, and the RA to protect user privacy from insider attacks.

The number of messages signed by a vehicle under a pseudonym must be kept to a minimum in the interest of fulfilling the unlinkability property of V2X messages. Pseudonym certificates issued by the SCMS are assigned an expiry date, so the certificates only have a limited validity period of 1 week [12]. Consequently, vehicles must be issued with a large number of pseudonym certificates to ensure they always have access to a fresh pseudonym. Certificate issuance in a traditional PKI would require the requester to upload a different public key for each certificate request. Since vehicles can request certificates to last them for as long as three years at once, this method does not scale well with the needs of the SCMS. Especially since vehicles may have to make certificate requests under sub-optimal network conditions, causing requests with a large upload size to fail. Instead, the SCMS employs a cryptographic technique called *butterfly key expansion* which allows vehicles to request an arbitrary number of certificates by uploading a single public-key seed [25].

Butterfly key expansion uses elliptic curve cryptography but can be implemented using any form of discrete-log-based cryptography. The requester chooses a base point G of prime order ℓ in an elliptic curve E and sends the certificate issuing authority a *caterpillar public key* $A = aG$ for an integer a (with the corresponding private key a

only known to the requester). For a pseudorandom permutation on the integers mod ℓ, $f(\cdot)$, the issuing authority generates ℓ distinct *cacoon public keys* $B_i = A + f(i) \times G$ (with corresponding private keys $b_i = a + f(i)$ only known to the requester) for $1 \leq i < \ell$. Thus, the certificate issuing authority provisions the requester with ℓ certificates which include the public keys B_i. The butterfly key expansion construction when instantiated with E as the cryptographically secure elliptic curve NISTp256 and $f(\cdot)$ as AES is secure [25]: an adversary given a polynomial number of butterfly public keys can recover any one of the butterfly private keys with at most negligible probability.

While it may seem desirable to provision a vehicle with an arbitrarily large number of certificates at once, doing so may have undesirable consequences. A misbehaving vehicle may employ several pseudonymous identities to mount a Sybil attack [35]: a single vehicle masquerading as a group of vehicles by simultaneously signing messages using multiple distinct certificates. The misbehaving vehicle could then promote a false narrative (for instance, congestion on a freeway) to gain an advantage. To prevent Sybil attacks, the SCMS imposes a strict cap on the number of pseudonyms that can be issued to a vehicle at once [12]: a vehicle can be issued no more than three years' worth of pseudonyms at once (vehicles change pseudonyms at least once a week).

Use Once a vehicle obtains pseudonyms from the SCMS, they are stored on and managed by a Hardware Security Module (HSMs) [25]. HSMs are tamper resistant and designed to mitigate the possibility of a Sybil attack by a vehicle using multiple certificates to sign messages at once. The vehicles' OBUs use these pseudonyms once obtained to communicate — OBUs can sign outgoing messages with their pseudonym certificate and use the pseudonym certificates embedded in incoming messages to verify their authenticity. The elliptic curve signature schemes standardised for V2X communication by IEEE 1609.2 and ETSI C-ITS protect messages from being tampered with in transit and replayed. However, a malicious vehicle enrolled in the SCMS may still transmit false data; the SCMS employs complimentary misbehaviour detection techniques to verify the consistency of data transmitted by enrolled vehicles.

Change Vehicles must regularly discard the pseudonym in use for a fresh one since messages broadcasted under the same pseudonym are linkable. Further, a pseudonym change must be accompanied by a change in identity across all network layers to prevent an adversary from trivially linking messages by tracking MAC or IP addresses. The desired level of privacy dictates the frequency of pseudonym change. Changing the pseudonym with greater frequency limits the number of messages an adversary can link, thus providing greater anonymity — an extreme measure would be to change pseudonyms with every transmitted message. More frequent pseudonym changes come at the cost of needing to request the SCMS for fresh pseudonym certificates more often. IEEE 1609.2 and ETSI C-ITS require that vehicles change pseudonyms at least once a week [12, 10].

Resolution The SCMS must be able to resolve the long-term identity of a pseudonym user. Identity resolution is necessary to revoke access to the SCMS for misbehaving users and to furnish information that law enforcement agencies may need. The IEEE 1609.2 SCMS achieves this by retaining escrow information that maps pseudonyms to long-term identities. This escrow information is spread out across multiple components of the SCMS to prevent abuse from SCMS insiders and protect user privacy; this mechanism is described in greater detail in Section 4.2.2.

Revocation In the context of the PKI-based SCMSs described IEEE 1609.2 and ETSI C-ITS, revoking a device's access means blocking it and not providing it with fresh pseudonym certificates. Further, the pseudonyms already issued to the vehicle are added to a Certificate Revocation List (CRL), which is distributed to enrolled vehicles for the period of the contained pseudonyms' validity.

4.2.2 Protecting user privacy from SCMS insiders

Since the SCMS must support pseudonym revocation, the SCMS must necessarily store all the information required to resolve a pseudonym to a device's long-term identity. Thus it is impossible to prevent an adversary with privileged access to the entirety of the SCMS's infrastructure from using this information to resolve pseudonyms to long-term identities and track devices. While it is not possible to entirely eliminate the possibility of such insider attacks against user privacy, the IEEE 1609.2 SCMS is designed to make such insider attacks harder — it divides its operations among multiple components so that separate organisations manage each component. No single organisation knows or can create a set of data that would allow tracking an enrolled device. As a consequence of this organisational separation, two or more organisations must necessarily collude in order to gather meaningful information towards tracking a device. In this section we describe the architectural structure of IEEE 1609.2 SCMSs which make such organisational separation possible.

Organisational separation allows the SCMS to protect user privacy by distributing the information required to resolve a pseudonym to a long-term identity across multiple components of the SCMS at the time of certificate provisioning (note that the SCMS as a whole must be able to link pseudonymous identities to long-term identities in order to support pseudonym revocation). The Registration Authority, the Pseudonym Certificate Authority, and multiple Linkage Authorities are the key components of the SCMS responsible for certificate provisioning [25]:

Linkage Authority (LA) The SCMS has two linkage authorities, LA_1 and LA_2. These linkage authorities generate pre-linkage values; these pre-linkage are individually generated by LA_1 and LA_2 as hash-chains. A pair of pre-linkage values from both LA_1 and LA_2 are used to construct a single linkage value which is embedded in certificates to support efficient revocation. When a misbehaving vehicle is identified, the reporter sends the linkage value embedded in the misbehaving vehicle's certificate back to the SCMS.

Pseudonym Certificate Authority (PCA) The PCA issues short-lived pseudonym certificates to devices. The PCA doesn't know the recipient of the pseudonym certificates it creates and whether any two certificates go to the same device.

Registration Authority (RA) The RA validates requests from the device and ensures that revoked devices are not issued new pseudonym certificates. It splits a single batch request into multiple requests and shuffles requests from all devices before sending them to the Pseudonym Certificate Authority (PCA); the shuffling of requests prevents the PCA from determining if two pseudonym certificates went to the same device.

The certificate provisioning process begins with a device requesting a batch of pseudonym certificates from the RA. Each batch pseudonym request includes the device's long-term identity, a caterpillar public encryption key H (with corresponding private key h), and a caterpillar public signing key A (with corresponding private key a). The RA splits the device's single batch pseudonym request into multiple individual pseudonym requests, with each request including:

1. A cacoon public encryption key $J_i = H + f(i) \times G$ (with the corresponding private key $j_i = h + f(i)$ as derived from the initial caterpillar public encryption key);
2. A cacoon public signing key $B_i = A + f(i) \times G$ (with the corresponding private key $b_i = a + f(i)$ as derived from the initial caterpillar public signing key); and
3. A pair of pre-linkage values that the RA receives from LA_1 and LA_2 (these pre-linkage values are encrypted for the PCA and are not known to the RA).

The RA shuffles the requests from all devices before sending them to the PCA; this shuffling of requests prevents the PCA from determining if any two pseudonym certificates it generates go to the same device.

The PCA processes each pseudonym request and returns the generated certificate to the RA. The PCA generates a random integer c_i to obtain the point $C_i = c_iG$ and includes the public signing key $D_i = B_i + C_i$ (with the corresponding private key $d_i = b_i + c_i$); if the PCA directly included the public signing key B_i in the certificate, the RA, which knows the cacoon public signing keys corresponding to a device's batch pseudonym request, could track the device. The PCA decrypts the pair of pre-linkage values it receives from the RA and XORs them to construct the secret linkage value which it embeds in the certificate. Finally, the PCA includes c_i in its response to the RA so that the device can construct d_i from b_i. The PCA encrypts its response under J_i; the encryption is necessary as without it the RA can link the pseudonym certificate to the device's long-term identity and track it.

The organisational separation in the SCMS prevents any single component from tracking devices. While the RA delivers pseudonym certificates to devices and is aware of their long-term identity, it cannot read the contents of the certificates since the PCA encrypts them. The PCA, on the other hand, is responsible for creating each pseudonym certificate but cannot link pseudonym certificates assigned to the same device. The LAs generate hash-chained pre-linkage values; when combined, the produced linkage value that can identify a device and revoke its certificates. However, a single LA cannot track devices. Both LAs, the PCA, and the RA must collaborate to track a device and revoke its certificates. When a vehicle finds a neighbouring device to be misbehaving it reports the linkage value embedded in the misbehaving vehicle's certificate; the LAs, the PCA, and the RA resolve the long-term identity of the misbehaving vehicle from the linkage value and add it to the CRL.

While the LAs, PCA, and RA play a critical role in issuing pseudonym certificates to devices, they don't comprise the entirety of the SCMS and are supported by the following components:

SCMS Manager The role of the SCMS Manager is twofold: firstly, to ensure the SCMS operates both efficiently and fairly; secondly, to define the organisational and technical protocols and policies. The Manager further sets criteria for examining revocation requests and misbehaviour detection, thus ensuring that the procedures are both fair and accurate.

Certification Services Certification Services delineate the process of certification and describe which classes of devices are permitted to acquire digital certificates.

Device An end-entity (EE) unit, or a device, may transmit and receive V2X messages. Such devices can take the form of On-Board Unit (OBU), an after-market safety device (ASD), or a Road-Side Unit(RSU).

Device Configuration Manager (DCM) The DCM operates to assert to the Enrollment Certificate Authority (ECA) that a device is eligible for acquiring enrollment certificates. It acts as a buffer during the certificate bootstrapping process, providing relevant configuration settings and certificates.

Electors The electors form the cornerstone of trust within the SCMS. They sign ballots endorsing or revoking a Root Certificate Authority (RCA) or another elector. These ballots are then disseminated to all SCMS components, thus fostering trust relationships.

Root Certificate Authority (RCA) The RCA is the apex of a certificate chain within the SCMS and a trust anchor. It issues certificates for ICAs and other SCMS components. RCA certificates are stored in a Trust Store, and chain-validation of certificates is used to verify any certificate.

Intermediate CA (ICA) The ICA is a buffer for the root CA and shields it from potential traffic and attacks. The RCA issues the ICA certificate.

Enrolment CA (ECA) ECAs are responsible for issuing enrolment certificates, which function as a device's long-term identity and are used to request pseudonym certificates.

Location Obscurer Proxy (LOP) The LOP plays a crucial role in preserving privacy by disguising the location of the requesting device by preventing the RA from linking its network address to its physical location.

Policy Generator (PG) The PG oversees, and signs updates to the Global Policy File (GPF) and the Global Certificate Chain File (GCCF), both of which contain global configuration information and all trust chains of the SCMS, respectively.

CRL Store The CRL Store stores and broadcasts the current Certificate Revocation List (CRL) to enrolled devices.

In the interest of brevity, the description of the SCMS included in this thesis is restricted its privacy-preserving mechanisms and how its components enforce these mechanisms. For a complete study of IEEE 1609.2 and ETSI C-ITS SCMS architecture including details about device enrolment and misbehaviour detection interested readers may refer to [12, 10].

This section describes the architecture choices made in the IEEE 1609.2 SCMS. While the structure of the ETSI C-ITS SCMS is similar to that of the IEEE 1609.2 SCMS the former lacks the level of ownership and organisational separation the latter exhibits. The ETSI C-ITS SCMS requires further design and implementation to protect user privacy to the same degree that the IEEE 1609.2 SCMS does [91].

4.3 Evaluating security standards

An SCMS aims to secure V2X communication over VANETs as efficiently as possible to meet the high quality of service standards required by critical V2X applications. Additionally, the SCMS aims to protect user privacy and hold misbehaving users accountable. Meeting these seemingly contradictory requirements to design the perfect SCMS is a hard problem. As such, the IEEE 1609.2 and ETSI C-ITS SCMSs are not perfect; we discuss some of their shortcomings in this section.

Verification efficiency There is an inherent asymmetry between the number of messages a vehicle must sign and the number of messages a vehicle must verify — a vehicle must verify all the messages transmitted by neighbouring vehicles. Due to the limited hardware of OBUs, there is a cap on the number of messages a vehicle can verify per second. In dense traffic situations, the number of messages that a vehicle receives can exceed this limit[2] leaving a vehicle with two alternatives [54]: either process messages without verifying their authenticity or simply not processing them. The former choice can leave V2X communication vulnerable to adversarial influence, while the latter limits the efficiency of V2X applications.

The academic community has offered some solutions towards improving messages verification efficiency without compromising the safety of vehicles:

- **Implicit certificates [18]:** A traditional (explicit) certificate requires that signed messages be transmitted along with a certificate for the signing public key. Implicit certificates collapse the signature and the certificate into a single value, thus reducing the message transmission cost. Further, the signature

[2] While the exact cap on the number of messages an OBU can verify per second would depend on the specific hardware of the OBU, [54] show via a simulation that the queue of messages waiting to be processed can grow in excess of $25,000$ once an OBU is communicating with over 500 VANET nodes.

and certificate verification processes are combined into a single, faster process. Consequently, vehicle OBUs can verify a greater number of messages per second when messages are signed using implicit certificates.

- **Batch verification [24]:** The idea behind batching operations is to verify multiple signatures/certificates at once. The batch verification process reduces the amortised number of required elliptic curve arithmetic operations required to verify a signature — verifying the signatures in batches is faster than verifying them individually. The greater the batch size, the more time one shaves off of the baseline for verifying a single signature.
- **Smarter verification policy [54]:** Not all V2X messages are equally important; for instance, a message warning of an imminent crash should be processed before a routine safety message. Since missed messages are inevitable under heavy traffic conditions, dropping lower-priority messages in favour of higher-priority messages improves road safety. By having vehicles assign V2X messages a priority rating between 1 and 3, the message verification policy proposed in [54] promises to achieve a lower message-miss ratio for high-priority messages as opposed to the standardised first-in-first-out approach.

Pseudonym change While the standards recommend that vehicles regularly change pseudonyms at least once every week, pseudonym change by itself may be insufficient to guarantee message unlinkability. For instance, an OBU's before and after having changed pseudonyms change can be trivially linked if there are no neighbouring vehicles. More generally, an adversary may employ statistical traffic analysis to re-identify vehicles [27]. This has led to the development of more sophisticated strategies for changing pseudonyms [72]:

- **Fixed time change:** IEEE 1609.2 and ETSI C-ITS recommend that OBUs change pseudonyms following a fixed timetable. The length of the timetable's slots determines the level of privacy conferred to the user. However, an adversary can reconstruct the timetable after extended observation, rendering pseudonym use redundant.
- **Random change [70]:** Changing pseudonyms at random intervals helps overcome the issue of timetable reconstruction. However, a vehicle can still be re-identified when changing pseudonyms under isolated conditions.
- **Silent period between change [28]:** A vehicle remaining silent, i.e. it does not transmit messages, after changing its pseudonym can confound re-identification strategies that use statistical analysis [16]. However, this improved privacy

comes at the cost of reduced road safety — remaining silent prevents other vehicles from predicting the silent vehicle's movements. Stretches of reduced vehicular speed, when the risk of vehicular collisions is minimal, can be leveraged by vehicles to introduce random silent periods when changing pseudonyms to improve privacy while only minimally decreasing road safety.

- **Motion-based approaches [58]:** Since statistical vehicle re-identification techniques often make use of information related to vehicle motion, a vehicle changing pseudonyms when changing speed or direction can confound statistical re-identification techniques.

While these techniques are not perfect — a vehicle changing pseudonyms while isolated can still be re-identified under each of the pseudonym change schemes — they offer superior privacy compared to the "fixed time change" strategy proposed by IEEE 1609.2 and ETSI C-ITS. Further, these techniques can offer even better privacy protection when combined together [72].

Quantum safety IEEE 1609.2 and ETSI C-ITS secure V2X communication sign and encrypt messages using elliptic curve cryptography which is known to be vulnerable to attacks using quantum computers. While cryptographically relevant quantum computers have yet to be realised, this may no longer be the case in the next 15 years [62]. Vehicles vulnerable to cryptographic attacks by quantum computers would no longer enjoy the benefits of cryptography, thus making the attacks described in Section 2.3 feasible. Since vehicles can have a lifespan of as long as 20 years [68], vehicles being manufactured to support V2X communication must be outfitted with hardware capable of supporting the transition to post-quantum cryptography.

In principle, one could swap out the cryptographic primitives used to design the SCMS with quantum-safe alternatives (public key encryption [79], digital signature schemes [79], and butterfly key exchange [17]) to get a quantum-safe SCMS. However, it is unclear whether this quantum-safe SCMS would meet the quality of service requirements needed by V2X communication. While batch verification and implicit certification can help speed up classical cryptography, these techniques do not have equivalents for quantum-safe cryptography. Further, post-quantum signature schemes also have large key sizes and signature sizes (as an extreme example, switching from elliptic curve cryptography to code-based cryptography would cause public key sizes to blow up from 0.1KB to 190KB [91]). These increases in public key and signature sizes can make it challenging to provision storage-limited vehicles with sufficiently many pseudonyms and fit quantum-safe certificates into restrictively sized V2X message formats. To conclude, while the groundwork for quantum-safe

V2X communication has been laid, further work is needed before we can expect a practical quantum-safe SCMS.

Privacy vs. Efficiency Privacy requirements imposed on applications by SCMS can often lead to less efficient safety applications. In particular, the SCMS only provides security and privacy at the PHY and MAC layers; it does not prevent the tracking of vehicles via data made available to adversaries at the application layer. Consider the case of an Emergency Brake Warning (EBW) message (see Section 2.3.2) being broadcasted by a vehicle on a multi-lane road. An EBW message is classified as a De-centralized Environmental Notification Message (DENM) by ETSI C-ITS [10] and cannot contain any information that links it back to the broadcasting vehicle. Consequent to these requirements, a DENM must not contain any location information and must be signed by a fresh pseudonym so the source of the EBW message remains anonymous. Now, vehicles that receive the EBW message have no way of determining whether they are following the broadcasting vehicle. These vehicles cannot determine whether to brake or not, and lack the information necessary to make a decision that may prevent an accident. Earlier analyses [30] suggest that the privacy requirements put forth by IEEE 1609.2 and ETSI C-ITS must be reconsidered. As an alternative solution, we introduce a new Emergency Brake Warning protocol in Chapter 5 which is effective and also compliant with the requirements of ETSI C-ITS.

Hardware security ISO/SAE 21434 [11], a joint work between ISO and SAE, specifies minimum cybersecurity engineering criteria for road vehicles. While the standard is comprehensive in that it discusses all phases of vehicular communication from a hardware security perspective, its discussion remains abstract and does not provide implementation details or prescribe best practices. Further, the hardware security requirements of non-vehicle units such as RSUs is outside the scope of this standard [91].

Chapter 5

Privacy Preserving Emergency Brake Warning

5.1 Introduction

V2V communication can be leveraged to warn vehicles when another vehicle on the road unexpectedly brakes with an early warning signal – such a forewarning can be particularly useful in adverse weather conditions and more generally in conditions which impede road visibility. Since the wireless communication channels employed by V2X communication are much faster than the human reaction time, a so-called Emergency Braking Warning (EBW) system can potentially improve road safety. Such warning messages can be delivered directly from one vehicle to another as in the case of vehicle-to-vehicle (V2V) communication or by using additional infrastructure such as road-side units (RSUs) as intermediaries as in the case of vehicle-to-everything (V2X) communication.

A naive EBW system could can be very easy to implement — a braking vehicle can broadcast a warning signal which could then be processed by nearby vehicles to be appropriately prepared. However, such a naive EBW is imprecise; an emergency brake warning which would only be relevant to vehicles following the braking vehicle is now delivered to and processed by vehicles in neighbouring lanes and possibly other roads as well (the dedicated short range communication devices proposed to be used by vehicles for V2X communication have a communication range of 300m). Implementing an un-targeted EBW system is undesirable for two reasons:

1. Needless braking of vehicles due to irrelevant EBW messages would degrade the flow of vehicular traffic on roads; and

2. The on-board units (OBUs) on vehicles which process V2X messages received by vehicles can only process a limited number of messages per second due to limited computational resources — a vehicle may process an irrelevant EBW message in favour of a more relevant but conflicting message (for instance, clearing the roadway for an emergency response vehicle).

The naive EBW system can be improved by incorporating geo-location data into the EBW message emitted by the braking vehicle. Now, vehicles can choose to stop in accordance with EBW messages they receive if the embedded geo-location data suggests that they are in the same lane as the braking vehicle or choose to ignore it otherwise. While a GPS based approach would be inadequate because GPS data isn't accurate enough to provide "lane-level" accuracy [80] and let vehicles determine their lane, there exist alternatives: technologies such as Differential GPS [4] and Wide Area Augmentation technology [5] augment GPS data to improve its accuracy or using 5G technology which claims to provide locations accurate to within a centimetre. However, since there exists no viable solutions to authenticating GPS data this approach is vulnerable to location spoofing in two ways:

1. GPS data isn't authenticated at source and a malicious adversary could feed spurious GPS data to vehicles;

2. A malicious vehicle could intentionally spoof their location despite having access to un-tampered GPS data.

The second concern can be dealt with by having the OBUs implemented on tamper-proof Trusted Execution Environment (TEE). The first concern, however, is harder to deal with. A malicious adversary can use spoofed GPS data to produce spurious EBW warning messages which is undesirable. Further, such an approach is fundamentally incompatible with V2X security standards such as ETSI C-ITS which require that an EBW message be broadcasted as a De-centralized Environmental Notification Message (DENMs) (see Section 4.3); since the source of a DENM must remain anonymous they cannot contain the broadcasters location.

One of the current proposals for precise EBW applications has vehicles use cameras in tandem with optical character recognition to process the license plate numbers of the vehicles they follow and thus filter out irrelevant EBW messages [80]. Unlike the GPS-based approach, such camera-based EBW systems are resilient against adversarial location spoofing. In addition to the EBW message, each vehicle would also broadcast a list of the license plates of vehicles it follows, allowing preceding vehicles to build a list of vehicles they follow recursively. If a vehicle brakes due to an emergency and broadcasts an EBW message, vehicles in neighbouring lanes could choose to ignore it. While this approach can circumvent the issue of adversaries spoofing location data, it comes at the cost of user privacy — proper functioning of the EBW system would require cars' license plates to be broadcasted over the V2X network, making this information accessible to malicious network members at no cost.

Many jurisdictions permit license plate look-ups, allowing members of the general public to find personal information of a vehicle owner, such as their name and address. For instance, the Ontario Ministry of Transportation allows third parties to query information about the recent vehicle owner associated with a license plate number [69]. Alternatively, such services may be offered by non-government entities such as [82, 39] in the United States of America. The adversary can collect V2V data over an extended period to infer private information about drivers, such as their homes, workspaces, routines and habits. Earlier work by Hoh et al. [49] shows that the start and end points of a vehicle's trips are strongly correlated to the vehicle owner's home address. Further, analysis of U.S. Census data shows that approximating the average person's home and work addresses down to a block level effectively de-anonymises that person and allows one to identify them uniquely [42]. Thus, an EBW system that requires broadcasting a vehicle's license plate compromises user privacy. Again, this loss of privacy aligns with the fact that this approach to building an EBW system is incompatible with V2X security standards; the EBW message is a DENM and cannot contain personally identifying information like the broadcasting vehicle's license plate number.

Both solutions described above are inadequate because they don't tie the vehicle's digital identity (cryptographic credentials) to its physical identity (location) while remaining compliant with V2X security standard requirements. A recent work by Xu, Li, Pan, Lazos, Li, and Ghosh [89] introduces the *proof-of-following* protocol which does precisely that and allows a vehicle to tie its cryptographic credentials to its current location. The proof-of-following protocol was originally used in the context of platooning — an appointed verifier admits a candidate into the platoon if, using the proof-of-following protocol, the candidate can prove to the verifier that they closely follow the platoon. In this chapter, we show how a modified proof-of-following protocol can let a candidate prove its location with lane-level accuracy and thus construct a precise, privacy-preserving EBW protocol.

The rest of this chapter proceeds as follows: Section 5.2 introduces the proof-of-following protocol PoF, discusses its security, and describes how to tweak it to suit the needs of an EBW system; Section 5.3 describes how to construct EBW-PoF, a precise and privacy-preserving EBW system, using the proof-of-following primitive. Section 5.4 discusses the cost of implementing and running EBW-PoF. Finally, Section 5.5 discusses the limitation of EBW-PoF and how it falls short of an ideal EBW system.

5.2 Radio signals as a geo-spatial fingerprint

The proof-of-following primitive uses the constantly evolving radio environment shared by vehicles to prove that they are close to each other (separated in space by some distance threshold d at any instance of time). Received radio signal strength (RSS) (measured in dB) attenuates due to long-distance propagation and large-object induced diffraction [89]. Consider entities A and B receiving radio signals being broadcasted from a common source; when A and B are close together, the radio signals they receive are similarly attenuated by environmental factors, so we can expect A and B's measured signals strengths to be more correlated than if A and B were further apart. More precisely, for a radio signal being broadcasted, the signal strengths as measured by vehicles A and B, separated by a distance of d, are widely accepted to have an average correlation ρ_d [44, 45]:

$$\rho_d = e^{-\frac{d}{d_{\text{corr}}}}, \tag{5.1}$$

where d_{corr}, the de-correlation distance, is an environment-specific constant. In other words, if vehicles A and B driving along the same path within d of each other measure N distinct RSS samples $\Gamma_A = \{\gamma_A(i)\}_{1 \leq i \leq N}$ and $\Gamma_B = \{\gamma_B(i)\}_{1 \leq i \leq N}$ at times i for $1 \leq i \leq N$ then their M-smooth Pearson correlation coefficient ρ computed as

$$\rho = \frac{\sum_{i=1}^{N}(\overline{\gamma}_A(i) - \overline{\gamma}_A)(\overline{\gamma}_B(i) - \overline{\gamma}_B)}{\sqrt{\sum_{i=1}^{N}(\overline{\gamma}_A(i) - \overline{\gamma}_A)^2}\sqrt{\sum_{i=1}^{N}(\overline{\gamma}_A(i) - \overline{\gamma}_A)^2}} \tag{5.2}$$

(where $\overline{\gamma}_A(i)$ and $\overline{\gamma}_B(i)$ are M-point moving averages[1] and $\overline{\gamma}_A$ and $\overline{\gamma}_B$ are the mean values of the N RSS samples collected by A and B respectively) satisfies the relation $\rho_d \leq \rho$. The proof-of-following primitive works by comparing the threshold ρ_d against the average correlation of smoothed RSS values collected by a candidate and a verifier, A and B, respectively, to validate if A and B are within distance d of each other.

Simultaneously collected RSS values are useful for authenticating vehicle location because appropriately correlated RSS values are hard to forge:

[1] We work with smoothed RSS values to filter out small-scale fading and extract large-scale fading since the model in Equation 5.1 works with large-scale fading.

Assumption 7. *Spatial correlation between RSS values decreases with distance, i.e. RSS values collected at two locations are less correlated if the locations are further apart.*

Assumption 8. *Temporal correlation between RSS values decreases with time, i.e. RSS values collected at the same location but at different times are less correlated if the collection times are further apart.*

As a consequence of Assumption 7 and Assumption 8, two entities must be in close proximity at similar times to have appropriately correlated RSS values. While Assumption 7 and Assumption 8 are assumptions, in that they are not proven mathematical theorems, they have been experimentally verified by Xu, Li, Pan, Lazos, Li, and Ghosh in [89] using a setup with two cars in a variety of environments such highways, freeways, and urban environments. Further, [89] also validates the model described by Equation 5.1 using the same experimental setup.

5.2.1 Definitions

Before describing the proof-of-following primitive in Section 5.2 we introduce some necessary definitions in this section.

Definition 16 (n-route [89])**.** *A n-route $\mathcal{L}_X$ of an object X is a collection of n ordered pairs $\mathcal{L}_X = \{(\ell_X(i), t_X(i))\}_{1\leq i\leq n}$ such that $\ell_X(i)$ represents X's location coordinates at time $t_X(i)$ and $t_X(i) < t_X(j)$ for all $i < j$.*

Definition 17 (d-follow [89])**.** *Suppose that objects $\mathcal{V}$ and $\mathcal{C}$ move along n-routes $\mathcal{L}_\mathcal{V}$ and $\mathcal{L}_\mathcal{C}$ respectively. Then $\mathcal{C}$ is said to d-follow $\mathcal{V}$ if $t_\mathcal{V}(i) = t_\mathcal{C}(i)$ and $\|\ell_\mathcal{V}(i) - \ell_\mathcal{C}(i)\| \leq d$ for all $1 \leq i \leq n$.*

The distance descriptor "d" may be dropped and the term "d-following" may be shortened to simply "following" when "d" is either apparent from context or is irrelevant to the point being made. Note that rather than describing the notion of "following" in the traditional sense of the word, d-following describes continued proximity between objects $\mathcal{V}$ and $\mathcal{C}$ along an n-route. For example:

- Objects $\mathcal{V}$ and $\mathcal{C}$ move along 3-routes $\mathcal{L}_\mathcal{V} = \{((0,0),1),((0,0),2),((0,0),3)\}$ and $\mathcal{L}_\mathcal{C} = \{((1,0),1),((1,0),2),((1,0),3)\}$. Here, $\mathcal{C}$ 1-follows $\mathcal{V}$ even though both objects don't actually move.

- Objects $\mathcal{V}$ and $\mathcal{C}$ move along 3-routes $\mathcal{L}_{\mathcal{V}} = \{((0,0),1),((1,0),2),((2,0),3)\}$ and $\mathcal{L}_{\mathcal{C}} = \{((1,0),1),((2,0),2),((3,0),3)\}$. Here, $\mathcal{C}$ 1-follows $\mathcal{V}$ even though $\mathcal{C}$ moves "ahead" of $\mathcal{V}$.

Definition 18 (d-proof-of-following protocol [89])**.** *A d-proof-of-following protocol is executed between a verifier $\mathcal{V}$ and a candidate $\mathcal{C}$ travelling along n-routes $\mathcal{L}_{\mathcal{V}}$ and $\mathcal{L}_{\mathcal{C}}$. $\mathcal{V}$ outputs ACCEPT if $\mathcal{C}$ d-follows $\mathcal{V}$, otherwise $\mathcal{V}$ outputs REJECT.*

An adversary to the proof-of-following protocol aims to have a verifier output ACCEPT without actually following the verifier. We follow the adversarial model described in [89]; the adversary can control communication by replaying, or dropping messages arbitrarily. Adversaries can be one of three types:

Remote adversary The adversary is stationary and is located at a distance d' (greater than the threshold distance d) away from $\mathcal{V}$ and is aware of $\mathcal{V}$'s route $\mathcal{L}_{\mathcal{V}}$ ahead of time. The adversary uses the existing V2X infrastructure to communicate with $\mathcal{V}$ in real time.

Following-afar adversary The adversary d'-follows $\mathcal{V}$ with $d' > d$.

Partially-following adversary The adversary follows $\mathcal{V}$ for a fraction of time before falling back and transitioning to being a following-afar adversary or remote adversary.

We formalise the above with the $\mathsf{Following}$ experiment. Let Π be a d-proof-of-following protocol, d the threshold distance, $\mathcal{V}$ the verifier, $\mathcal{A}$ an adversary, and λ the security parameter:

$\mathsf{Following}_{\mathcal{A},\mathcal{V},\Pi}(\lambda, d, t)$

```
The verifier $\mathcal{V}$ holds $1^\lambda$ and intends to travel along the route $\mathcal{L}_{\mathcal{V}}$ starting at time $t$.
Prior to time $t$ the adversary $\mathcal{A}$ is free to travel anywhere but may not $d$-follow $\mathcal{V}$ after time $t$.
(The distance threshold $d$, the start time $t$, and route $\mathcal{L}_{\mathcal{V}}$ are known to $\mathcal{A}$.)
Once $\mathcal{V}$ is at the end of $\mathcal{L}_V$, $\mathcal{A}$ outputs a transcript $\mathsf{trans}_{\mathcal{A}}$.
$\mathcal{V}$ runs $\Pi(\mathsf{trans}_{\mathcal{A}})$ and outputs either ACCEPT or REJECT.
The experiment outputs 1 if $\mathcal{V}$ ACCEPTs else the experiment outputs 0 if $\mathcal{V}$ REJECTs.
(If $\mathsf{Following}_{\mathcal{A},\mathcal{V},\Pi}(\mathsf{Params}, d, t) = 1$ we say that $\mathcal{A}$ succeeds.)
```

We now define what it means for a d-proof-of-following protocol to be secure [2]:

Definition 19. *A d-proof-of-following protocol* Π *is secure if for a given verifier* $\mathcal{V}$*, distance threshold* d*, start time* t*, and security parameter* λ*, all adversaries* $\mathcal{A}$ *satisfy*

$$\Pr[\mathit{Following}_{\mathcal{A},\mathcal{V},\Pi}(\lambda, d, t) = 1] \leq \mathsf{negl}(\lambda)$$

for a negligible function negl.

5.2.2 Proof-of-following

With the preliminary setup out of the way, we present PoF [89], a proof-of-following protocol (see Definition 17) conducted between a candidate $\mathcal{C}$ and verifier $\mathcal{V}$ with synchronised clocks[3]. PoF makes use of several publicly known parameters, N, η, f, M, K, and α (we introduce each parameter over the course of the description of PoF) which we abbreviate as the ordered tuple $\mathsf{Params} := (N, \eta, f, M, K, \alpha)$. The following stages of the protocol are conducted over an authenticated and confidential channel[4]:

Initialization stage

1. $\mathcal{C}$ initiates the protocol by sending $\mathcal{V}$ a request message REQ.
2. $\mathcal{V}$ replies to $\mathcal{C}$ with the message REPLY_t which includes the start time t.

Collection stage

1. $\mathcal{V}$ and $\mathcal{C}$ collect N RSS samples $\gamma_V(i)$ and $\gamma_C(i)$ by sampling the radio frequency f at rate η samples/second starting at time t to construct

$$\Gamma_{\mathcal{V}} = \{\gamma_{\mathcal{V}}(i)\}_{1 \leq i \leq N},$$

[2] While the candidate/verifier paradigm that we evaluate the security of the proof-of-following protocol under assumes honest verifiers and thus restricts adversarial analysis to candidates, the situation can be more complex in practice. For instance, a verifier (say, a driver in a truck platoon) may be presented with a financial incentive to ACCEPT spurious requests from dishonest candidates (thus, admitting malicious actors into the platoon).

[3] By synchronised clocks we mean that the candidate $\mathcal{C}$'s and the verifier $\mathcal{V}$'s clocks are aligned to the same reference allowing them to coordinate their actions. Thus, corresponding RSS samples $\gamma_{\mathcal{C}}(i)$ and $\gamma_{\mathcal{V}}(i)$ collected by $\mathcal{C}$ and $\mathcal{V}$ respectively, are collected at the same instance in time.

[4] $\mathcal{V}$ and $\mathcal{C}$ can achieve confidentiality and authentication by using public-key cryptography.

$$\Gamma_{\mathcal{C}} = \{\gamma_{\mathcal{C}}(i)\}_{1 \leq i \leq N}.$$

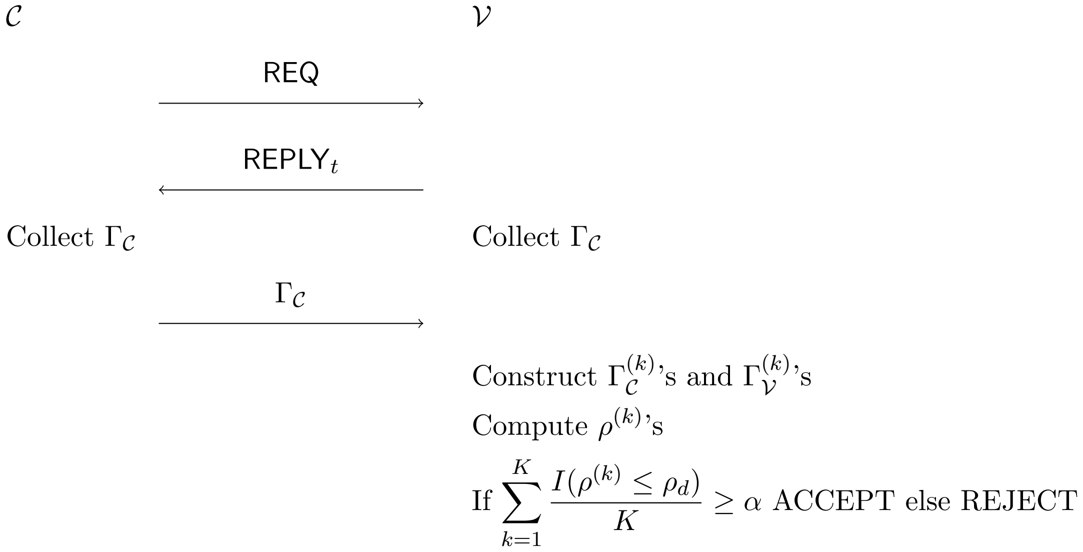
(Note that $\gamma_{\mathcal{V}}(i)$ and $\gamma_{\mathcal{C}}(i)$ are sampled at the same instance in time because $\mathcal{V}$ and $\mathcal{C}$ have synchronised clocks.)

2. $\mathcal{C}$ sends $\Gamma_{\mathcal{C}}$ to $\mathcal{V}$.

Verification stage

1. $\mathcal{V}$ splits $\Gamma_{\mathcal{V}}$ and $\Gamma_{\mathcal{C}}$ into K subsets of equal size[5] $\Gamma_{\mathcal{V}} = \sqcup_{k=1}^{K} \Gamma_{\mathcal{V}}^{(k)}$ and $\Gamma_{\mathcal{C}} = \sqcup_{k=1}^{K} \Gamma_{\mathcal{C}}^{(k)}$.
2. V computes the M-smoothed Pearson correlation coefficients, $\rho^{(k)}$, of $\Gamma_{\mathcal{C}}^{(k)}$ and $\Gamma_{\mathcal{V}}^{(k)}$ for all $1 \leq i \leq K$.
3. V compares $\rho^{(k)}$ against the passing threshold $\rho_d = e^{-\frac{d}{d_{\text{corr}}}}$. If at least a fraction α of the tests pass, i.e. $\sum_{k=1}^{K} \frac{I(\rho^{(k)} \leq \rho_d)}{K} \geq \alpha$ (where $I(\cdot)$ is the indicator function[6]), V outputs ACCEPT, else V outputs REJECT.

$\mathsf{PoF}_{(\mathsf{Params},d)}$ [89]



$\mathcal{C}$

$\mathcal{V}$

REQ

REPLY_t

Collect $\Gamma_{\mathcal{C}}$

Collect $\Gamma_{\mathcal{C}}$

$\Gamma_{\mathcal{C}}$

Construct $\Gamma_{\mathcal{C}}^{(k)}$'s and $\Gamma_{\mathcal{V}}^{(k)}$'s

Compute $\rho^{(k)}$'s

If $\displaystyle\sum_{k=1}^{K} \frac{I(\rho^{(k)} \leq \rho_d)}{K} \geq \alpha$ ACCEPT else REJECT

[5] Since the correlation model in Equation 5.1 is for average correlation ρ will fluctuate around ρ_d due to environmental factors and thus a single long test as opposed to multiple shorter tests would only provide a weak probabilistic guarantee that $\mathcal{V}$ and $\mathcal{C}$ will are within distance d of each other. To counter this, PoF splits $\Gamma_{\mathcal{V}}$ and $\Gamma_{\mathcal{C}}$ into smaller subsets and conducts multiple shorter tests.

[6] The indicator function $I(\cdot)$ operates on Boolean expressions. $I(X)$ evaluates to 1 if X is *true* else, $I(X)$ evaluates to 0 if X is *false*)

Security of PoF

The security of $\mathsf{PoF}_{(\mathsf{Params},d)}$ hinges on the adversary being unable to produce an "appropriate" transcript of RSS samples which passes the verifier's correlation check. For a given $\mathsf{PoF}_{(\mathsf{Params},d)}$ verifier $\mathcal{V}$, we define what we mean by an appropriate transcript:

Definition 20 ($\mathcal{V}_{\mathsf{Params},d,t}$-transcript)**.** *Let $\mathcal{V}$ travel along the route $\mathcal{L}_\mathcal{V}$ starting at time t. Starting at t, $\mathcal{V}$ and $\mathcal{C}$ collect their RSS samples $\Gamma_\mathcal{V}$ and $\Gamma_\mathcal{C}$ respectively as in $\mathsf{PoF}_{(\mathsf{Params},d)}$. We say that $\Gamma_\mathcal{C}$ is a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript if $\sum_{k=1}^{K} \frac{I(\rho^{(k)} \leq \rho_d)}{K} \geq \alpha$ computed as in $\mathsf{PoF}_{(\mathsf{Params},d)}$.*

While $\mathsf{PoF}_{(\mathsf{Params},d)}$ is designed to be d-proof-of-following protocol in practice the performance of the protocol depends on the choice of parameters Params and d. Depending on the choice of Params and d there may exist a probability of a false accepts — an adversary (either remote, following-afar, or partially-following) may be able to produce a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript. Xu, Li, Pan, Lazos, Li, and Ghosh demonstrate in [89] how, for a given d, to select the parameters Params appropriately so as to bring the probability of such false accepts close to 0 against remote adversaries and following-afar adversaries. The situation is more complicated when considering partially-following adversaries — a partially-following adversary can initiate a successful protocol run by following $\mathcal{V}$ for a fraction of time greater than the public parameter α. These findings suggest that for a given $\mathsf{PoF}_{(\mathsf{Params},d)}$ verifier $\mathcal{V}$ one can choose Params such that producing a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript without d-following is a hard problem. Consider the $\mathsf{Radio\text{-}Following}$ experiment:

$\mathsf{Radio\text{-}Following}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}, d, t)$

1 : Starting at time t, the verifier travels along the route $\mathcal{L}_\mathcal{V}$ and collects RSS samples $\Gamma_\mathcal{V}$.

2 : The adversary $\mathcal{A}$ outputs a set of RSS samples $\Gamma_\mathcal{A}$.
(Note that while the parameters (Params and d), the route $\mathcal{L}_\mathcal{V}$ and time t are known to $\mathcal{A}$, $\mathcal{A}$ is not d-following $\mathcal{V}$.)

3 : The experiment outputs 1 if and only if $\Gamma_\mathcal{A}$ is a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript.

Based on our trust in Assumption 7, Assumption 8, and the experimental findings of [89] we make the following strong assumption to aid in our analysis of PoF:

Assumption 9. *For a verifier $\mathcal{V}$, a distance threshold d, and security parameter λ, there exist parameters Params_λ such that for all $\mathsf{PoF}_{\mathsf{Params}_\lambda,d}$ adversaries $\mathcal{A}$ and start times t there is a negligible function negl which satisfies*

$$\Pr[\mathsf{Radio\text{-}Following}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}_\lambda, d, t) = 1] \leq \mathsf{negl}(\lambda).$$

Under Assumption 9 we can show that PoF is a secure d-proof-of-following protocol.

Theorem 1. *Under Assumption 9, there exists parameters Params such that $\mathsf{PoF}_{\mathsf{Params},d}$ is a secure d-proof-of-following protocol.*

Proof. We shall proceed by contradiction. For a given verifier $\mathcal{V}$, distance threshold d, and security parameter λ say there exists an adversary $\mathcal{A}$ which can break $\mathsf{PoF}_{\mathsf{Params},d}$ for all parameters Params at some start time t with non-negligible probability. Such an adversary $\mathcal{A}$ can then produce a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript so that $\Pr[\mathsf{Radio\text{-}Following}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}_\lambda, d, t) = 1]$ with non-negligible probability which contradicts Assumption 9. □

Although the experimental results of [89] are demonstrated in urban, highway, and freeway settings these environments are not exhaustive in the set of conditions people drive in. Experimental validation of the $\mathsf{PoF}_{(\mathsf{Params},d)}$ protocol in additional environmental conditions is necessary to understand how its performance and security are dependent on the environment. With that said, we continue to rely on Assumption 9 to aid our analysis of PoF and similar protocols that we construct in this chapter.

PoF On-the-Fly

$\mathsf{PoF}_{(\mathsf{Params},d)}$ requires the candidate and verifier exchange three messages. The first two messages are necessary to initiate the protocol and negotiate a start time for both parties to collect RSS samples. In this section, we present $\mathsf{PoF\text{-}OtF}$, a proof-of-following protocol conducted between a candidate $\mathcal{C}$ and verifier $\mathcal{V}$ with synchronised clocks. $\mathsf{PoF\text{-}OtF}$ is an on-the-fly version of the PoF protocol where the candidate and verifier passively collect RSS samples to avoid the initial REQ and REPLY messages, thus bringing the total cost of communication down from 3 messages to 1 message. Similar to PoF, $\mathsf{PoF\text{-}OtF}$ makes use several publicly known parameters, N, η, f, M, K, and α (our choice of parameters is similar to that of PoF, we introduce each parameter over the course of the description of $\mathsf{PoF\text{-}OtF}$) which we abbreviate as the ordered tuple $\mathsf{Params} := (N, \eta, f, M, K, \alpha)$. The following stages of the protocol are conducted over an authenticated and confidential channel[7]:

Initialization/Collection stage

[7] $\mathcal{V}$ and $\mathcal{C}$ can achieve confidentiality and authentication by using public-key cryptography.

1. The candidate $\mathcal{C}$ and verifier and $\mathcal{V}$ sample radio frequency f, collecting η samples/second. Thus, $\mathcal{C}$ and $\mathcal{V}$ maintain constant-size pools of RSS samples $\Gamma_{\mathcal{C}}$ and $\Gamma_{\mathcal{V}}$ respectively,
$$\Gamma_{\mathcal{C}} = \{\gamma_{\mathcal{C}}(i)\}_{1 \le i \le N},$$
$$\Gamma_{\mathcal{V}} = \{\gamma_{\mathcal{V}}(i)\}_{1 \le i \le N}.$$
$\mathcal{C}$ and $\mathcal{V}$ discard older samples as they collect new ones.

2. $\mathcal{C}$ sends the initial $\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}$ to $\mathcal{V}$. This message includes $\Gamma_{\mathcal{C}}$ and t, the timestamp of the oldest RSS sample in $\Gamma_{\mathcal{C}}$. (Note that $\gamma_{\mathcal{V}}(i)$ and $\gamma_{\mathcal{C}}(i)$ are sampled at the same time because $\mathcal{V}$ and $\mathcal{C}$ have synchronised clocks.)

Verification stage

This stage is identical to the verification stage of the $\mathsf{PoF}_{(\mathsf{Params},d)}$ protocol.

$\mathsf{PoF\text{-}OtF}_{(\mathsf{Params},d)}$

$\mathcal{C}$		$\mathcal{V}$
Collect $\Gamma_{\mathcal{C}}$		Collect $\Gamma_{\mathcal{V}}$
	$\xrightarrow{\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}}$	
		Construct $\Gamma_{\mathcal{C}}^{(k)}$'s and $\Gamma_{\mathcal{V}}^{(k)}$'s
		Compute $\rho^{(k)}$'s
		If $\sum_{k=1}^{K} \frac{I(\rho^{(k)} \le \rho_d)}{K} \ge \alpha$ ACCEPT else REJECT

Interestingly, the candidate $\mathcal{C}$'s actions aren't dependent on the parameters M, K, α, or d and instead depend only on N. The verifier $\mathcal{V}$ can then run the $\mathsf{PoF\text{-}OtF}_{(\mathsf{Params},d)}$ verification stage with any parameters M, K, α, and d of their choosing, independent of how $\mathcal{C}$ constructs $\Gamma_{\mathcal{C}}$. We shall make use of this fact in Section 5.3 when we use $\mathsf{PoF\text{-}OtF}_{(\mathsf{Params},d)}$ to design our privacy-preserving EBW protocol. We formalise the verification stage of $\mathsf{PoF\text{-}OtF}_{(\mathsf{Params},d)}$ as follows:

$\mathsf{PoF\text{-}Verify}_{(\mathsf{Params},d)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathcal{V}})$
Construct $\Gamma_{C}^{(k)}$'s and $\Gamma_{V}^{(k)}$'s
Compute $\rho^{(k)}$'s
If $\sum_{k=1}^{K} \frac{I(\rho^{(k)} \le \rho_d)}{K} \ge \alpha$ ACCEPT else REJECT

Security of PoF-OtF

We argue that PoF-OtF is as effective as PoF at detecting remote, following-afar, and partially-following adversaries. While PoF-OtF modifies the structure of PoF to reduce the total number of messages transmitted between $\mathcal{V}$ and $\mathcal{C}$, the core security mechanism, RSS correlation computation, hasn't changed. We analyse the security of PoF-OtF under the same adversary model for PoF.

We formalise the security of PoF-OtF by modifying the Radio-Following experiment as follows:

```
$\mathsf{Radio\text{-}Following\text{-}OtF}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}, d, t)$
The adversary $\mathcal{A}$ outputs a set of RSS samples $\Gamma_{\mathcal{A}}$ and the timestamp $t$ of the oldest RSS sample in $\Gamma_{\mathcal{A}}$.
The experiment outputs 1 if and only if $\Gamma_{\mathcal{A}}$ is a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript.
```

Theorem 2. *Under Assumption 9 for a given verifier $\mathcal{V}$, distance threshold d, start time t, and security parameter λ, there exist parameters Params_λ such that for all $\mathsf{PoF\text{-}OtF}_{\mathsf{Params}_\lambda,d}$ adversaries $\mathcal{A}$ there is a negligible function negl which satisfies*

$$\Pr[\mathsf{Radio\text{-}Following\text{-}OtF}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}_\lambda, d, t) = 1] \leq \mathsf{negl}(\lambda).$$

Proof. We proceed by contradiction. For a given verifier $\mathcal{V}$, distance threshold d, start time t, and security parameter λ say there exists an adversary $\mathcal{A}$ such that for all parameters Params we have $\mathsf{Radio\text{-}Following\text{-}OtF}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}, d, t) = 1$ with non-negligible probability. Such an adversary $\mathcal{A}$ can then produce a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript with non-negligible probability which contradicts Assumption 9. □

Theorem 3. *Under Assumption 9, there exists parameters Params such that $\mathsf{PoF\text{-}OtF}_{\mathsf{Params},d}$ is a secure d-proof-of-following protocol.*

Proof. We shall proceed by contradiction. For a given verifier $\mathcal{V}$, distance threshold d, and start time t say there exists a adversary $\mathcal{A}$ which can break $\mathsf{PoF}_{\mathsf{Params},d}$ for all parameters Params with non-negligible probability. Such an adversary $\mathcal{A}$ can then produce a $\mathcal{V}_{\mathsf{Params},d,t}$-transcript so that $\mathsf{Radio\text{-}Following\text{-}OtF}_{\mathcal{A},\mathcal{V}}(\mathsf{Params}_\lambda, d, t) = 1$ with non-negligible probability which contradicts Theorem 2. □

5.3 Precise privacy-preserving EBW

We shall now use PoF-OtF to construct an efficient privacy-preserving EBW protocol EBW-PoF. In addition to the vehicles on the road, RSUs participate in the protocol. When a vehicle brakes, it sends its RSS values to two RSUs on the left and right sides of the road, acting as PoF-OtF verifiers. The braking vehicle uses its sampled RSS values to prove that it is d-following the verifier on the left side of the road and d'-following the verifier on the right side of the road for some distances d and d' less than the width of the road. Since the braking vehicle is close to both the left and right edges of the road, it must be travelling in some lane on the road. If the braking vehicle produced valid RSS transcripts, the RSUs broadcast a warning message to the vehicles behind the braking vehicle.

This section describes the privacy-preserving EBW protocol and explains how the left and right verifiers can precisely determine which lane the candidate/braking vehicle travels in. Since EBW-PoF is conducted along a road, we first define what we mean by a road and its lanes.

Definition 21 (Roads). *A road R is a rectangle of arbitrary length and width.*

Definition 22 (Lanes). *A road R can be divided along its width into equal-width rectangles of width equal to d_{lane} (each lane of R is as long as R). We denote an n-lane road L as $L = (l_1|l_2|\cdots|l_n)$. We say that l_i is the i^{th} lane of R.*

Definition 23 (Sections). *A road R can be divided along its length into equal-length rectangles of length equal to d_{sep} sections (each section of R is as wide as L). We denote a m-section road R as $R = (s_1|s_2|\cdots|s_n))$. We say that s_i is the i^{th} lane of R.*

EBW-PoF is designed to operate on an n-lane road (see Figure 5.1) with lanes that are d_{lane} wide. The protocol participants consist of the following time-synchronised entities:

1. **RSUs.** RSUs are placed in a grid-like manner on both sides of the road. RSUs are placed at a distance d_{gap} from the road, at regular intervals of d_{sep}. RSU's are centred along the length of the section they correspond to. Each section of the road has an RSU to its left and right; we label the RSUs on the left and right side of the i^{th} section of the road $\mathsf{RSU}_i^{(L)}$ and $\mathsf{RSU}_i^{(R)}$ respectively. We assume that RSUs are honest when participating in the protocol.

2. **Vehicles.** All vehicles travelling along the road, registered with V2X network may participate in the protocol. Any vehicle may determine which lane and section of the

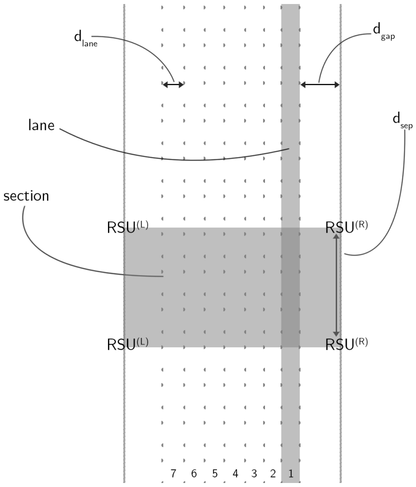


Figure 5.1: A schematic of a 7-lane road equipped to run EBW-PoF.

road it is in by using augmented GPS data or otherwise. Vehicles in lane i and all sections leading up to section j stop moving when they receive a $\mathsf{STOP}_{i,j}$ signed by an RSU. Vehicles may be dishonest when participating in the protocol.

An adversary to EBW-PoF aims to have an RSU output $\mathsf{STOP}_{i,j}$ for some lane i while not travelling in lane i and section j. Additionally, we assume such an adversary can control communication by modifying and dropping messages.

The protocol is able to detect dishonest vehicles by employing PoF. While a successful run of PoF is able to narrow the location of a candidate vehicle down to a sphere around the verifier, EBW-PoF employs two PoF verifiers to narrow a braking vehicle's location down to the intersection of two spheres, i.e. a single lane. EBW-PoF makes use of a number of publicly known parameters, N, η, f, M, K, and α which we abbreviate as the ordered tuple $\mathsf{Params} \coloneqq (N, \eta, f, M, K, \alpha)$. Additionally, EBW-PoF uses the publicly known parameters n, d_{lane}, d_{sep}, and d_{gap}, and the function $f(i) = d_{\text{gap}} + i \times d_{\text{lane}}$. EBW-PoF uses $\mathsf{PoF\text{-}Verify}_{(\mathsf{Params},d)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathcal{V}})$ as a sub-routine which we abbreviate as $\mathsf{PoF}_d(\Gamma_{\mathcal{C}}, \Gamma_{\mathcal{V}})$. The following stages of the protocol are conducted over an authenticated and confidential channel[8]:

Initialization/Collection stage:

1. All vehicles and RSUs sample radio frequency f, collecting η samples/second. Thus,

[8] Vehicles and RSUs can achieve confidentiality and authentication by using public-key cryptography.

entity X maintains a constant size pool of RSS samples Γ_X,

$$\Gamma_X = \{\gamma_X(i)\}_{1 \leq i \leq N}.$$

X continues discarding older RSS samples as it collects new ones.

2. During an emergency braking event, the braking vehicle $\mathcal{C}$ broadcasts $\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}$ containing its RSS samples and t, the timestamp of the oldest RSS sample in $\Gamma_{\mathcal{C}}$.

Lane determination stage[9]**:** We shall consider how the left and right RSU's closest to $\mathcal{C}$ at the time it broadcasts $\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}$ (these would be $\mathsf{RSU}_i^{(L)}$ and $\mathsf{RSU}_i^{(R)}$ if $\mathcal{C}$ is in section i at the time of broadcast) respond:

1. $\mathsf{RSU}_i^{(R)}$ runs $\mathsf{PoF}_{f(i)}(\Gamma_C, \Gamma_{\mathsf{RSU}_i^{(R)}})$ for $1 \leq i \leq n$ and computes $\mathsf{lane}_R = i$ as the smallest i for which $\mathsf{PoF}_{f(i)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathsf{RSU}_i^{(L)}})$ succeeds.

2. $\mathsf{RSU}_i^{(L)}$ runs $\mathsf{PoF}_{f(i)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathsf{RSU}_i^{(L)}})$ for $1 \leq i \leq n$ and computes $\mathsf{lane}_L = i$ as the smallest i for which $\mathsf{PoF}_{f(i)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathsf{RSU}_i^{(L)}})$ succeeds.

Verification stage:

1. $\mathsf{RSU}_i^{(R)}$ sends lane_R to $\mathsf{RSU}_i^{(L)}$.

2. If $(n-1) - \mathsf{lane}_L \overset{?}{=} \mathsf{lane}_R$ $\mathsf{RSU}_i^{(L)}$ broadcasts a plaintext $\mathsf{STOP}_{\mathsf{lane}_L}$ to all vehicles.

[9] The lane determination stage forms the backbone of EBW-PoF and must necessarily be accurate. While we haven't been able to experimentally verify the feasibility of executing this stage accurately due to lack of appropriate hardware, we note that the idea of using radio-waves for lane determination is not inherently infeasible — 5G, a radio-based technology, allows position determination with a degree of accuracy to within a metre even in dense urban environments [38].

```
$\mathsf{EBW\text{-}PoF}_{(\mathsf{Params},n,d_{\mathrm{lane}},d_{\mathrm{sep}},d_{\mathrm{gap}})}$
$\mathbf{RSU}_i^{(L)}$                                   $\mathcal{C}$                                   $\mathbf{RSU}_i^{(R)}$
Collect $\Gamma_{\mathsf{RSU}_i^{(L)}}$                  Collect $\Gamma_C$                              Collect $\Gamma_{\mathsf{RSU}_i^{(R)}}$

                     $\xleftarrow{\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}}$            $\xrightarrow{\mathsf{REQ}_{\Gamma_{\mathcal{C}},t}}$

$\mathsf{lane}_L = \perp$                                                                                $\mathsf{lane}_R = \perp$
for $j \in [N]$ do                                                                                       for $j \in [N]$ do
  if $\mathsf{PoF}_{f(j)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathsf{RSU}_i^{(L)}})$                            if $\mathsf{PoF}_{f(j)}(\Gamma_{\mathcal{C}}, \Gamma_{\mathsf{RSU}_i^{(R)}})$
    $\mathsf{lane}_L = j$                                                                                    $\mathsf{lane}_R = j$
    break                                                                                                    break
  endif                                                                                                    endif
endfor                                                                                                   endfor

                              $\xleftarrow{\mathsf{lane}_R}$

if $(n-1) - \mathsf{lane}_L \stackrel{?}{=} \mathsf{lane}_R$
  Broadcast $\mathsf{STOP}_{\mathsf{lane}_L,i}$
endif
```

5.3.1 Security of EBW-PoF

We analyse the security of EBW-PoF using the Lane-Brake experiment:

$\mathsf{Lane\text{-}Brake}_{\mathsf{RSU}_j^{(L)},\mathcal{A},\mathsf{RSU}_j^{(R)}}(\mathsf{Params}, n, d_{\mathrm{lane}}, d_{\mathrm{sep}}, d_{\mathrm{gap}}, t)$

1 : $\mathcal{A}$ outputs a transcript of RSS samples $\Gamma_{\mathcal{A}}$ and the timestamp t of the oldest RSS sample in $\Gamma_{\mathcal{A}}$.

2 : The experiment outputs 1 if and only if two conditions are satisfied:
$\Gamma_{\mathcal{A}}$ is a $(\mathsf{RSU}_j^{(L)})_{\mathsf{Params},f((n-1)-i),t}$-transcript and a $(\mathsf{RSU}_j^{(R)})_{\mathsf{Params},f(i),t}$-transcript for some i; and $\mathcal{A}$ is not in lane i and section j simultaneously.
(We say that $\mathcal{A}$ succeeds if the experiment outputs 1.)

Theorem 4. *Let R be an n-lane road with lanes that are d_{lane} wide. RSUs are placed at regular d_{sep} intervals to the left and right of R at a distance of d_{gap} from R. We run the Lane-Brake experiment on road R.*

Under Assumption 9, for a given time t and security parameter λ there exist parameters Params_λ such that for all $\mathsf{EBW\text{-}PoF}_{(\mathsf{Params}_\lambda,n,d_{lane},d_{sep},d_{gap})}$ adversaries $\mathcal{A}$ there is a negligible *function* **negl** *which satisfies*

$$\Pr[\textsf{\textit{Lane-Brake}}_{\textsf{\textit{RSU}}_j^{(L)},\mathcal{A},\textsf{\textit{RSU}}_j^{(R)}}(\textsf{\textit{Params}}, n, d_{lane}, d_{sep}, d_{gap}, t) = 1] \leq \textsf{\textit{negl}}(\lambda).$$

Proof. We proceed by contradiction. For a given time t, and security parameter λ say there exists an adversary $\mathcal{A}$ such that for all parameters $\textsf{Params}$ we have $\textsf{Lane-Brake}_{\textsf{RSU}_j^{(L)},\mathcal{A},\textsf{RSU}_j^{(R)}}$ $(\textsf{Params}, n, d_{\text{lane}}, d_{\text{sep}}, d_{\text{gap}}, t) = 1$ with non-negligible probability. Such an adversary $\mathcal{A}$ can then break $\textsf{PoF-OtF}_{\textsf{Params, f((n-1)-i)}}$ and $\textsf{PoF-OtF}_{\textsf{Params, f(i)}}$ for some $1 \leq i \leq n$ against verifier $\textsf{RSU}_j^{(L)}$ and $\textsf{RSU}_j^{(R)}$ respectively with non-negligible probability for all parameters $\textsf{Params}$. However, this contradicts Theorem 3. □

As a consequence of Theorem 4 we can state the following about EBW-PoF:

1. **Precise.** EBW-PoF is a precise EBW protocol in that the brake warning message exclusively notifies vehicles in danger of collision, i.e. the vehicles following braking vehicle.
2. **Resilient against location spoofing.** Because EBW-PoF ties a vehicle's physical identity (RSS samples) to its digital identity (cryptographic credentials), the braking vehicle must be physically present in lane i and section j to have an RSU broadcast a $\textsf{STOP}_{i,j}$ message. Therefore, PoF-EbW is resilient against malicious adversaries that may spoof their location.
3. **Privacy-preserving.** EBW-PoF does not require the braking vehicle to broadcast personally identifying information such as its location or license plate number.

5.4 Cost of EBW-PoF

We analyse the cost of running EBW-PoF in terms of the necessary infrastructure required to run the protocol and the runtime efficiency of the protocol.

Infrastructure. Here, we calculate the minimum number of RSUs required per unit distance of roadway to support running EBW-PoF on an n-lane road with lanes d_{lane} wide, RSUs placed at a distance of d_{gap} from the road at regular intervals d_{sep}. For a given road with fixed parameters n, d_{gap}, and d_{gap}, the parameter d_{sep} uniquely determines the tiling of RSU's along the road. Consequently, the number of RSUs required to support running EBW-PoF also depends on d_{sep}.

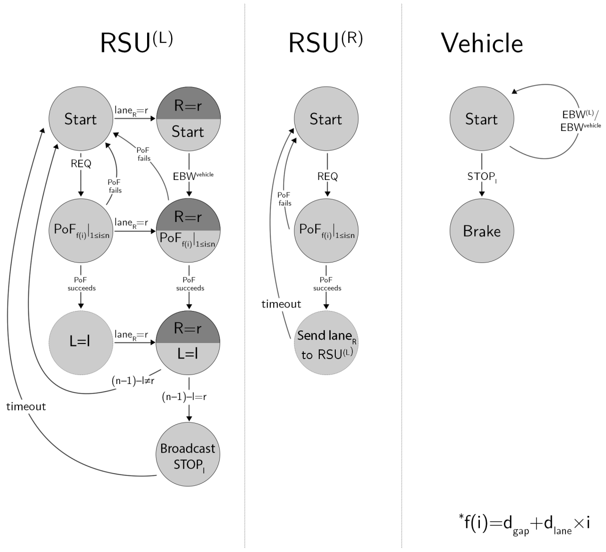


Figure 5.2: State diagrams describing each class of participating members in the protocol — $\mathsf{RSU}^{(R)}$'s, $\mathsf{RSU}^{(L)}$'s, and vehicles.

We see in Figure 5.3 setting d_{sep} to be too large can lead to "dead zones" on the road — such dead zones are too far from any pair of left/right RSUs for them to act as suitable verifiers. We shall calculate an upper bound for the parameter d_{sep} to prevent such dead zones.

Consider a pair of left/right RSUs, $\mathsf{RSU}_i^{(L)}$ and $\mathsf{RSU}_i^{(R)}$. Let $\mathsf{C}_j^{(L)}$ ($\mathsf{C}_j^{(R)}$) be circle of radius $d_{\text{gap}} + d_{\text{lane}} \times j$ centred at $\mathsf{RSU}_i^{(L)}$ ($\mathsf{RSU}_i^{(R)}$). Now, a vehicle in lane r must be in both $\mathsf{C}_r^{(R)}$ and $\mathsf{C}_{(n-1)-r}^{(L)}$ simultaneously. Let d_r denote the length of the common chord between $\mathsf{C}_r^{(R)}$ and $\mathsf{C}_{(n-1)-r}^{(L)}$. As seen in Figure 5.3 setting $d_{\text{sep}} > d_r$ leads to a dead-zone in lane r. Clearly, setting $d_{\text{sep}} \leq \min_{r \in [n]} d_r$ will prevent any dead-zones on the road.

We shall now compute $\min_{r \in n} d_r$. First, we prove a result using elementary geometry.

Lemma 1. *The common chord of two circles with radii r_1 and r_2 respectively whose centres are separated by a distance $d < r_1 + r_2$ is*

$$\frac{\sqrt{(d^2 - (r_1 - r_2)^2)((r_1 + r_2)^2 - d^2)}}{d}.$$

Proof. The situation is described graphically in Figure 5.4. The circles centred at A and B have radii r_1 and r_2 respectively so that $AC = r_1$ and $BC = r_2$. We let $AE = d - x$

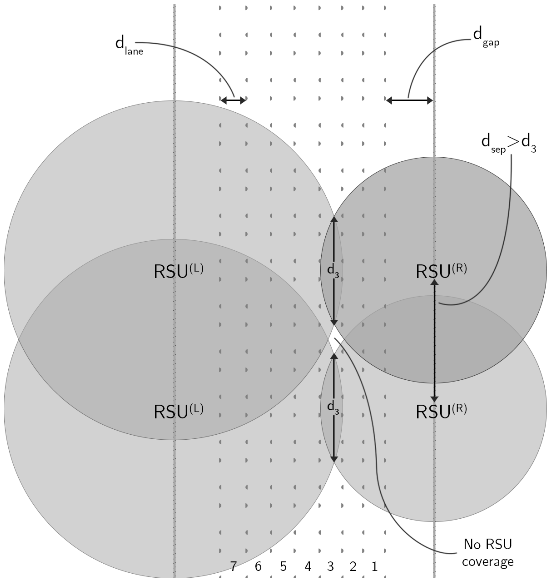


Figure 5.3: A schematic for a 7-lane road. We see that placing RSUs at intervals greater than d_3 leads to a “dead zone” in lane 3.

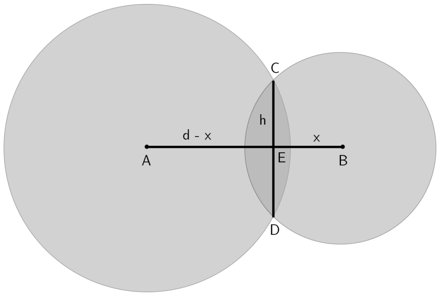


Figure 5.4: Two circles with radii r_1 and r_2 centred at A and B respectively.

and $EB = x$ for some unknown x. Using Pythagoras' theorem with ΔACE and ΔCEB we calculate $x = \frac{r_2^2 - r_1^2 - d^2}{d}$. Again, using Pythagoras' theorem with ΔCEB we get

$$CE = 2h = \frac{\sqrt{(d^2 - (r_1 - r_2)^2)((r_1 + r_2)^2 - d^2)}}{d}.$$

□

Using Lemma 1 we describe a closed-form expression for d_r.

Theorem 5. *The common chord of* $\mathsf{C}_r^{(R)}$ *and* $\mathsf{C}_{(n-1)-r}^{(L)}$ *has length*

$$d_r = \frac{\sqrt{(d_{total}^2 - ((n - 2r + 1)d_{lane})^2)((2d_{gap} + (n + 1)d_{lane})^2 - d_{total}^2)}}{d_{total}}.$$

Proof. The result follows from Lemma 1 by setting $r_1 = d_{\text{gap}} + d_{\text{lane}} \times r$, $r_2 = d_{\text{gap}} + d_{\text{lane}} \times ((n - 1) - r)$, and $d = d_{\text{total}} := 2d_{\text{gap}} + nd_{\text{lane}}$. □

Finally, we compute $\min_{r \in [n]} d_r$.

Theorem 6. *The common chord of* $\mathsf{C}_r^{(R)}$ *and* $\mathsf{C}_{(n-1)-r}^{(L)}$ *is minimised when* $r = 1$, *i.e.*

$$\min_{r \in [n]} d_r = d_1 = \frac{\sqrt{(d_{total}^2 - ((n - 1)d_{lane})^2)((2d_{gap} + (n + 1)d_{lane})^2 - d_{total}^2)}}{d_{total}}.$$

Proof. One can observe that in the expression for d_r

$$d_r = \frac{\sqrt{(d_{\text{total}}^2 - ((n - 2r + 1)d_{\text{lane}})^2)((2d_{\text{gap}} + (n + 1)d_{\text{lane}})^2 - d_{\text{total}}^2)}}{d_{\text{total}}}$$

only the sub-expression

$$d_{\text{total}}^2 - ((n - 2r + 1)d_{\text{lane}})^2 \tag{5.3}$$

varies with r while the rest of the expression remains constant with respect to r. Since Equation 5.3 increases monotonically with r so does d_r and thus the result follows. □

Using the expression for $\min_{r \in [n]} d_r$ we present some concrete values [10] of d_{sep} in Table 5.4 with varying parameters n, d_{gap}.

[10] We choose to present concrete values of d_{sep} in favour of an asymptotic analysis since each of the parameters n, d_{lane}, and d_{gap} are bounded in practice.

n/d_{gap}	0	10	20	30	40	50
2	6.77	14.06	18.42	21.90	24.90	27.57
6	6.97	15.64	20.07	23.49	26.41	29.00
10	6.99	16.33	21.03	24.55	27.49	30.08
14	6.99	16.70	21.66	25.30	28.30	30.93

Table 5.1: d_{sep} for various n and d_{gap} values. We set $d_{\text{lane}} = 3.5m$ (the average width of lane on an American road). Note that for the proof-of-following primitive to work the distance d_{gap} can be no larger than the decorrelation distance $d_{\text{corr}} \sim 50m$.

Runtime. EBW-PoF is a time-sensitive protocol. We want a run of the protocol to be faster than the visual reaction time of an average human of 190 ms [53]; any slower and the protocol would not confer an advantage to the participating vehicles. We divide the parts of the protocol which contribute to the protocol's runtime into two categories which we then consider separately — wireless communication (the time taken to transfer messages wirelessly between vehicles and RSUs) and computation (the time taken by computational tasks such as calculating RSS value correlation and cryptographic overheads). Since we do not have access to appropriate hardware, we cannot benchmark the cost of wireless communication[11] and instead choose to focus on the cost of computation. We use a python script to simulate $\mathsf{EBW\text{-}PoF}_{(\mathsf{Params},n,d_{\text{lane}},d_{\text{sep}},d_{\text{gap}})}$ between a vehicle and two RSUs with Params as chosen in [89] ($N = 400$, $M = 20$ and $K = 20$; note that the parameters d, η, f α, d_{lane}, d_{gap}, and d_{sep} aren't of relevance here since we do not physically sample RSS values and instead use random values) and benchmark the time taken up by the RSS correlation computation and the associated cryptographic overheads. We emphasise that this simulation does not validate the security of $\mathsf{EBW\text{-}PoF}_{(\mathsf{Params},n,d_{\text{lane}},d_{\text{sep}},d_{\text{gap}})}$.

EBW-PoF must be conducted over a confidential and authenticated channel to function securely — in particular, the REQ messages must be confidential (lest adversaries replay

[11] While lack of access to appropriate hardware prevents us from benchmarking the communication cost, we can attempt to estimate them theoretically. The primary communication cost of EBW-PoF is transmitting the initial REQ message. The message consists of N RSS samples and the timestamp of the oldest RSS sample; when $N = 400$, as in [89], and assuming each RSS sample and timestamp is encoded as 64-bit double precision floating point value, the message REQ would be $\sim 25,600$ bits large. The underlying communication protocol and cryptographic algorithms it uses would further introduce an overhead to transmitting REQ. Conservatively estimating that communicating REQ would require transmitting a total of $50,000$ bits of information, we conclude that this message transmission would take 8.33 ms when transmitted at 6 Mbits/s using DSRC and 0.05 ms when transmitted at 1 Gbits/s using 5G (see Section 2.2). However, it is important to note that this calculation is only a rough estimate and is a poor stand-in for experimental benchmarks.

RSS values) and the lane_R and STOP messages must be authenticated (so that adversaries cannot impersonate RSUs). We repeat our simulation for a variety of combinations of KEMs and signature schemes used alongside AES256 in both classical and quantum settings to get the benchmarks listed in Table 5.2, Table 5.3, and Table 5.4. We see in our experiments that our limited implementation of EBW-PoF runs faster than than the visual reaction time of the average human for all NIST security levels except when instating the underlying KEM with Classic McEliece using NIST Level 3 and Level 5 security parameters.

	Kyber512	Classic-McEliece-348864f	BIKE-L1	HQC-128
Dilithium2	1.304	96.192	2.754	1.554
Falcon-512	8.591	103.027	10.171	23.49
SPHINCS+-SHA256-128f-simple	10.270	104.345	11.403	24.55

Table 5.2: Time taken for a single run of EBW-PoF ($N = 400$, $M = 20$ and $K = 20$) in milliseconds when using KEMs and signature schemes selected in the NIST Post-Quantum Cryptography Standardization programme (including Round 4 candidates for KEMs) when instantiated with parameters claiming to provide NIST Level 1 security.

5.5 Limitations of EBW-PoF

While EBW-PoF fixes the shortcomings of earlier EBW systems by being precise, resilient against location spoofing, and privacy-preserving, it is not a perfect solution. This section discusses some limitations of EBW-PoF concerning its security, cost, and applicability.

Security. The security PoF, and thus by extension the security of EBW-PoF, is critically dependent on Assumption 9. Assumption 9 says that producing a $\mathcal{V}_{\mathsf{Params},d,t}$ without actually d-following the verifier $\mathcal{V}$ starting at time t is a computationally hard problem.

	Kyber768	Classic-McEliece-460896f	BIKE-L3	HQC-192
Dilithium3	1.454	306.613	5.902	1.857
SPHINCS+-SHA256-192f-simple	16.306	336.063	20.254	17.002

Table 5.3: Time taken for a single run of EBW-PoF ($N = 400$, $M = 20$ and $K = 20$) in milliseconds when using KEMs and signature schemes selected in the NIST Post-Quantum Cryptography Standardization programme (including Round 4 candidates for KEMs) when instantiated with parameters claiming to provide NIST Level 3 security.

	Kyber1024	Classic-McEliece-6688128f	BIKE-L5	HQC-256
Dilithium5	1.618	367.392	12.621	4.800
Falcon-1024	23.807	432.533	37.070	30.344
SPHINCS+-SHA256-256f-simple	31.464	432.169	75.540	33.601

Table 5.4: Time taken for a single run of EBW-PoF ($N = 400$, $M = 20$ and $K = 20$) in milliseconds when using KEMs and signature schemes selected in the NIST Post-Quantum Cryptography Standardization programme (including Round 4 candidates for KEMs) when instantiated with parameters claiming to provide NIST Level 5 security.

Although the RSS correlation model described by Equation 5.1 has been widely verified [44, 45], to the best of the author's knowledge the experiments in [89] are the first to validate Assumption 7, Assumption 8, and Assumption 9. Therefore, Assumption 9 makes a questionable foundation for cryptographic primitives as it has not received the extended scrutiny as in the case of mathematical problems such as factoring, or finding discrete logs. As an example, consider an adversary who doesn't d-follow the verifier $\mathcal{V}$ but instead travels along the route $\mathcal{L}_{\mathcal{V}}$ at an earlier time — intuition suggests that such an adversary ought to have an advantage over an adversary who has never travelled along $\mathcal{L}_{\mathcal{V}}$. However, Assumption 9 does not distinguish the two adversaries. Further investigation into Assumption 9 is necessary before PoF and related constructions can be deployed in practice.

Cost. The costs associated with implementing EBW-PoF are driven up considerably by the requirement of placing RSUs along the roadside (see Table 5.4). While the cost could be mitigated to a minor degree by constructing RSUs with minimally sufficient hardware to support EBW-PoF, it is unclear whether such a measure would be sufficient to allow the widespread adoption of EBW-PoF. A more frugal approach might be to restrict deploying EBW-PoF to sufficiently accident-prone areas found by conducting cost-benefit analyses.

Applicability. EBW-PoF works with a particularly simplistic model of roads — an entirely straight road with entirely straight lanes. However, the real situation is significantly more complex — roads (and the lanes contained within) often bend to accommodate surrounding natural and artificial objects. While the construction of EBW-PoF is not intrinsically incompatible with a curved road, the tiling of RSU suggested in Section 5.3 would have to be modified to determine the lane of the braking vehicle unambiguously. Further, given a particular curved road, determining the tiling that minimises the required RSUs may be non-trivial.

5.6 Conclusion

As stated in Section 5.5, EBW-PoF is limited in applicability. Further work experimentally evaluating the validity of Assumption 9 is necessary before EBW-PoF and other PoF-related constructions can be used in settings requiring cryptographic security, such as V2X communication. Additionally, the tilling of RSUs described in Figure 5.1 would need to be adapted to suit real-world roads that bend and curve, both to allow unambiguous lane identification of vehicles and to minimise the number of RSUs required for proper protocol functioning. To summarise, EBW-PoF is an imperfect solution to the tricky problem of designing a precise and privacy-preserving EBW system resistant to adversarial location spoofing.

Chapter 6

Future research

Despite its shortcomings, using radio signals as an authentication mechanism shows promise for use in V2X scenarios. One possible application could be in the area of misbehaviour detection in VANETs. For their proper functioning, VANETs must support mechanisms for detecting misbehaving vehicles and blocking them from participating. Misbehaving vehicles can lie about their location or pretend to be multiple vehicles (using pseudonyms to mount a Sybil attack [35]). While a VANET can handle certificate revocation for misbehaving, as described in Section 4.2.2, detecting the misbehaving vehicles is a separate problem. One class of techniques used to detect misbehaving vehicles spoofing their location, called location sensor-based detection, uses physical sensors such as radars and cameras to accomplish misbehaviour detection [88]. Vehicles are equipped with physical sensors, which they use to correlate information received wirelessly from neighbouring vehicles with the physical reality of their surroundings, thus identifying misbehaving vehicles. While location sensor-based detection techniques effectively detect vehicles spoofing their location, these techniques also threaten the privacy of vehicles by reducing the unlinkability between the pseudonyms they use [88]. Designing a PoF-based privacy-preserving location authentication mechanism as an alternative to location sensor-based detection shows promise as a future line of research.

As mentioned in Section 4.3, V2X security standards are not perfect. While issues pertaining to "efficiency" and "pseudonym change" are only issues in that V2X security standards don't address them — solutions to these issues exist, however, V2X security standards have either not considered them or not adopted appropriate solutions for them — the issue of practical quantum-safe V2X standards is one that still needs solving. To reiterate, efficiency of signature verification speed and signature/certificate storage are imperative for the safety of V2X systems, and many solutions that help achieve this efficiency don't have quantum-safe equivalents (see Section 4.3). Research into designing quantum-safe implicit certificates and algorithms for batch verification of quantum-safe signatures[1] are promising lines of research. Similarly, V2X security and hardware standards must be re-worked to adequately accommodate larger quantum-safe signatures and certificates in size-limited V2X message formats and storage limited OBUs.

Finally, we touch upon the issue of designing V2X applications and analysing their security. Through examination of the various proposals for the Emergency Brake Warning application, this thesis aims to highlight the benefits of a security-centric approach to V2X application design. The availability of cryptography (as provided by IEEE 1609.2 and ETSI C-ITS standards) does not guarantee that every V2X application is secure and privacy-preserving, as in the case of Emergency Brake Warning. Therefore, a thorough analysis of security and compliance with IEEE 1609.2 and ETSI C-ITS standards is necessary before deploying any application in practice. Such analyses may not be possible without access to precise protocols and application standards. At the time of writing this thesis, publicly accessible literature describing concrete protocols for the Emergency Vehicle Path Clearing, Emergency Brake Warning, and Cooperate Platooning applications does not exist to the best of the author's knowledge. Similarly, governing bodies such as IEEE, ETSI, and SAE have not standardised protocols for these applications. Designing precise protocols and standards for V2X applications that are publicly accessible will go a long way towards supporting security/compliance analyses, resulting in safer and more private V2X applications.

[1] Not to be confused with quantum-safe batch signatures [13].

References

[1] EC Study on the Deployment of C-ITS in Europe Final Report. Technical Report MOVE/C.3./№ 2014-794, European Commision (EC). URL: https://transport.ec.europa.eu/system/files/2016-10/2016-c-its-deployment-study-final-report.pdf. Accessed: 2023-07-13.

[2] NHTSA Preliminary Regulatory Impact Analysis. Vehicle-To-Vehicle Communication Technology For Light Vehicles. Technical Report FMVSS No. 150, United States. Dept. of Transportation, National Highway Traffic Safety Administration (USDoT NHTSA). URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/v2v_pria_12-12-16_clean.pdf. Accessed: 2023-07-13.

[3] USDoT Connected Vehicle Research Program. Vehicle-to-Vehicle Safety Application Research Plan. Technical Report DOT HS 811 373, United States. Dept. of Transportation, National Highway Traffic Safety Administration (USDoT NHTSA). URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/811373.pdf. Accessed: 2023-07-13.

[4] 2001 Federal Radionavigation Systems. Technical report, U.S. Department of Transportation and U.S. Department of Defense, December 2001. URL https://rosap.ntl.bts.gov/view/dot/8476. Accessed: 2023-07-13.

[5] Federal Aviation Administration Specification for the Wide Area Augmentation System (WAAS). Technical report, U.S. Department of Transportation, Federal Aviation Administration, August 2001. https://web.archive.org/web/20081004122449/http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/documents/media/waas/2892bC2a.pdf. Accessed: 2023-07-13.

[6] IEEE Standard for Information technology – Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and

Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. Technical Report 802.11p-2010, Institute of Electrical and Electronics Engineers (IEEE), July 2010.

[7] Architecture enhancements for V2X services. Technical Report Technical Specification (TS) 23.285., 3rd Generation Partnership Project (3GPP)., September 2016. URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3078. Accessed 2023-07-13.

[8] Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services. Technical Report 23.287, 3rd Generation Partnership Project (3GPP), July 2020.

[9] IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical Report 802.11-2020, Institute of Electrical and Electronics Engineers (IEEE), December 2020.

[10] Intelligent Transport Systems (ITS); Security, ITS communications security architecture and security management. Technical Report 102 940, European Telecommunications Standard Institute (ETSI), July 2021.

[11] Road vehicles — Cybersecurity engineering. Technical Report 21434:2021, International Organization for Standardization (ISO), August 2021. https://www.iso.org/standard/70918.html. Accessed 2023-07-13.

[12] IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Application and Management Messages. Technical Report 1609.2-2022, Institute of Electrical and Electronics Engineers (IEEE), March 2023.

[13] Carlos Aguilar-Melchor, Martin R. Albrecht, Thomas Bailleux, Nina Bindel, James Howe, Andreas Hülsing, David Joseph, and Marc Manzano. Batch signatures, revisited. Cryptology ePrint Archive, Paper 2023/492, 2023.

[14] Zubair Amjad, Axel Sikora, Benoit Hilt, and Jean-Philippe Lauffenburger. Low Latency V2X Applications and Network Requirements: Performance Evaluation. In *2018 IEEE Intelligent Vehicles Symposium (IV)*, pages 220–225. IEEE, June 2018.

[15] Nicolas Aragon, Paulo L. Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim

Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. BIKE, 2017. URL https://bikesuite.org/. Accessed 2023-07-13.

[16] P. S. Auerbach, J. A. Morris, Jr., J. B. Phillips, Jr., S. R. Redlinger, and W. K. Vaughn. An Analysis of Ambulance Accidents in Tennessee. *JAMA: The Journal of the American Medical Association*, 258(11):1487, September 1987.

[17] Paulo S. L. M. Barreto, Jefferson E. Ricardini, Marcos A. Simplicio Jr., and Harsh Kupwade Patil. qSCMS: Post-quantum certificate provisioning process for V2X. Cryptology ePrint Archive, Paper 2018/1247, 2018.

[18] Paulo S. L. M. Barreto, Marcos A. Simplicio, Jefferson E. Ricardini, and Harsh Kupwade Patil. Schnorr-Based Implicit Certification: Improving the Security and Efficiency of Vehicular Communications. *IEEE Transactions on Computers*, 70(3):393–399, March 2021.

[19] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009.

[20] Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece, 2017. URL https://classic.mceliece.org/. Accessed 2023-07-13.

[21] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The SPHINCS+ Signature Framework. Cryptology ePrint Archive, Paper 2019/1086, 2019.

[22] Dan Boneh and Viktor Shoup. *A Graduate Course in Applied Cryptography*. January 2023. URL http://toc.cryptobook.us/. Accessed 2023-07-13.

[23] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals – kyber: a cca-secure module-lattice-based kem. Cryptology ePrint Archive, Paper 2017/634, 2017.

[24] Paul Bottinelli and Robert Lambert. Accelerating V2X Cryptography through Batch Operations. 2019.

[25] Benedikt Brecht, Dean Therriault, Andre Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A Security Credential Management System for V2X Communications. *IEEE Transactions on Intelligent Transportation Systems*, 19(12):3850–3871, December 2018.

[26] Johannes A. Buchmann, Evangelos Karatsiolis, and Alexander Wiesmaier. *Introduction to Public Key Infrastructures*. Springer Berlin Heidelberg, 2013.

[27] Mike Burmester, Emmanouil Magkos, and Vassilios Chrissikopoulos. Strengthening Privacy Protection in VANETs. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2008.

[28] Levente Buttyan, Tamas Holczer, Andre Weimerskirch, and William Whyte. SLOW: A Practical pseudonym changing scheme for location privacy in VANETs. In *2009 IEEE Vehicular Networking Conference (VNC)*, pages 1–8. IEEE, October 2009.

[29] Eric Chan. Overview of the SARTRE Platooning Project: Technology Leadership Brief. Technical report, SAE International, October 2012. URL https://doi.org/10.4271/2012-01-9019. Accessed 2023-07-13.

[30] Alishah Chator and Matthew Green. Don't Talk to Strangers - On the Challenges of Intelligent Vehicle Authentication:. In *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems*, pages 522–528. SCITEPRESS - Science and Technology Publications, 2018.

[31] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *20th USENIX Security Symposium (USENIX Security 11)*. USENIX Association, August 2011.

[32] McKinsey & Company. Automotive & Assembly Insights. URL: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights. Accessed 2023-07-13.

[33] C. Custalow and C. S. Gravitz. Emergency medical vehicle collisions and potential for preventive intervention. *Prehospital Emergency Care*, 8(2):175–184, April 2004.

[34] Debashis Das, Niraj Vasant Altekar, K. Larry Head, and Faisal Saleem. Traffic Signal Priority Control Strategy for Connected Emergency Vehicles with Dilemma Zone

Protection for Freight Vehicles. *Transportation Research Record: Journal of the Transportation Research Board*, 2676(1):499–517, January 2022.

[35] John R. Douceur. The Sybil Attack. In Gerhard Goos, Juris Hartmanis, Jan Van Leeuwen, Peter Druschel, Frans Kaashoek, and Antony Rowstron, editors, *Peer-to-Peer Systems*, volume 2429, pages 251–260. Springer Berlin Heidelberg, 2002.

[36] Shan Du, Mahmoud Ibrahim, Mohamed Shehata, and Wael Badawy. Automatic License Plate Recognition (ALPR): A State-of-the-Art Review. *IEEE Transactions on Circuits and Systems for Video Technology*, 23(2):311–325, February 2013.

[37] Leo Ducas, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehle. CRYSTALS – Dilithium: Digital Signatures from Module Lattices. Cryptology ePrint Archive, Paper 2017/633, 2017.

[38] Dwivedi, Satyam and Shreevastav, Ritesh and Munier, Florent and Nygren, Johannes and Siomina, Iana and Lyazidi, Yazid and Shrestha, Deep and Lindmark, Gustav and Ernstrom, Per and Stare, Erik and Razavi, Sara M. and Muruganathan, Siva and Masini, Gino and Busin, Ake and Gunnarsson, Fredrik. Positioning in 5G Networks. *IEEE Communications Magazine*, 59(11):38–44, November 2021.

[39] EpicVIN. License Plate Lookup. URL https://epicvin.com/license-plate-lookup. Accessed 2023-07-13.

[40] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon, 2017. URL https://falcon-sign.info/. Accessed 2023-07-13.

[41] Anthony R. Foxx. Beyond Traffic: 2045 Final Report. Technical report, United States. Dept. of Transportation (USDoT), January 2017. URL: https://rosap.ntl.bts.gov/view/dot/36751. Accessed 2023-07-13.

[42] Philippe Golle and Kurt Partridge. On the Anonymity of Home/Work Location Pairs. In Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe, editors, *Pervasive Computing*, volume 5538, pages 390–397. Springer Berlin Heidelberg, 2009.

[43] Amit Kumar Goyal, Arun Kumar Tripathi, and Gaurav Agarwal. Security Attacks, Requirements and Authentication Schemes in VANET. In *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pages 1–5. IEEE, September 2019.

[44] Ke Guan, Bo Ai, Zhangdui Zhong, Carlos F. Lopez, Lei Zhang, Cesar Briso-Rodriguez, Andrej Hrovat, Bei Zhang, Ruisi He, and Tao Tang. Measurements and Analysis of Large-Scale Fading Characteristics in Curved Subway Tunnels at 920 MHz, 2400 MHz, and 5705 MHz. *IEEE Transactions on Intelligent Transportation Systems*, 16(5):2393–2405, October 2015.

[45] M. Gudmundson. Correlation model for shadow fading in mobile radio systems. *Electronics Letters*, 27(23):2145, 1991.

[46] Gaby Joe Hannoun, Pamela Murray-Tuite, Kevin Heaslip, and Thidapat Chantem. Facilitating Emergency Response Vehicles' Movement Through a Road Segment in a Connected Vehicle Environment. *IEEE Transactions on Intelligent Transportation Systems*, 20(9):3546–3557, September 2019.

[47] B.J. Harker. PROMOTE-CHAUFFEUR II & 5.8 GHz Vehicle-to-Vehicle Communications System. In *International Conference on Advanced Driver Assistance Systems (ADAS)*, volume 2001, pages 81–85. IEE, 2001.

[48] Debiao He, Sherali Zeadally, Baowen Xu, and Xinyi Huang. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Transactions on Information Forensics and Security*, 10(12):2681–2691, December 2015.

[49] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Achieving Guaranteed Anonymity in GPS Traces via Uncertainty-Aware Path Cloaking. *IEEE Transactions on Mobile Computing*, 9(8):1089–1107, August 2010.

[50] Rasheed Hussain and Sherali Zeadally. Autonomous Cars: Research Results, Issues, and Future Challenges. *IEEE Communications Surveys & Tutorials*, 21(2):1275–1313, 2019.

[51] Rasheed Hussain and Sherali Zeadally. Autonomous Cars: Research Results, Issues, and Future Challenges. *IEEE Communications Surveys & Tutorials*, 21(2):1275–1313, 2019.

[52] Vishrut Jain, Di Liu, and Simone Baldi. Adaptive strategies to platoon merging with vehicle engine uncertainty. *IFAC-PapersOnLine*, 53(2):15065–15070, 2020.

[53] Jain, Aditya and Bansal, Ramta and Kumar, Avnish and Singh, K. D. A comparative study of visual and auditory reaction times on the basis of gender and physical activity

levels of medical first year students. *International Journal of Applied & Basic Medical Research*, 5(2):124–127, 2015.

[54] Santos Jha, Chaitanya Yavvari, and Duminda Wijesekera. Pseudonym Certificate Validations under Heavy Vehicular Traffic Loads. In *2018 IEEE Vehicular Networking Conference (VNC)*, pages 1–7. IEEE, December 2018.

[55] Craig A. Jordan, Mecit Cetin, and R. Michael Robinson. Path Clearance for Emergency Vehicles through the Use of Vehicle-to-Vehicle Communication. *Transportation Research Record: Journal of the Transportation Research Board*, 2381(1):45–53, January 2013.

[56] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, November 2014.

[57] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak N. Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Daniel G. Anderson, Danny Anderson, Danny Anderson, Danny Anderson, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental Security Analysis of a Modern Automobile. *IEEE Symposium on Security and Privacy*, 2010.

[58] Mingyan Li, Krishna Sampigethaya, Leping Huang, and Radha Poovendran. Swing & Swap: User-centric Approaches Towards Maximizing Location Privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 19–28. ACM, October 2006.

[59] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Arnaud Dion, Philippe Gaborit, Jérôme Lacan, Edoardo Persichetti, Jean-Marc Robert, Pascal Véron, and Gilles Zémor. HQC, 2017. URL https://pqc-hqc.org/index.html. Accessed 2023-07-13.

[60] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, December 2018.

[61] Rafael Molina-Masegosa and Javier Gozalvez. LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications. *IEEE Vehicular Technology Magazine*, 12(4):30–39, December 2017.

[62] Michele Mosca and Marco Piani. Quantum Threat Timeline Report 2020. Technical report, Global Risk Institute. URL https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2020/. Accessed: 2023-07-13.

[63] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. Ensuring Safety and Security in CAN-Based Automotive Embedded Systems: A Combination of Design Optimization and Secure Communication. *IEEE Transactions on Vehicular Technology*, 69(7):7078–7091, July 2020.

[64] Pamela Murray-Tuite, Aphisit Phoowarawutthipanich, Raulful Islam, and Naser Hdieb. Emergency Vehicle-to-Vehicle Communication: Final Report. Technical report, United States Department of Transport (USDoT), August 2016. URL https://rosap.ntl.bts.gov/view/dot/31196. Accessed 2023-07-13.

[65] National Highway Traffic Safety Administration (NHTSA). National Highway Traffic Safety Administration (NHTSA) Fatality Analysis Reporting System (FARS). URL https://www-fars.nhtsa.dot.gov/Main/index.aspx. Accessed 2023-07-28.

[66] Volvo Cars Global Media Newsroom. Volvo Cars' new XC60 SUV will automatically steer you out of trouble. URL https://www.media.volvocars.com/global/en-gb/media/pressreleases/204531/volvo-cars-new-xc60-suv-will-automatically-steer-you-out-of-trouble. Accessed 2023-07-13.

[67] C. Nowakowski, S. E. Shladover, X. Lu, D. Thompson, and A. Kailas. Cooperative Adaptive Cruise Control (CACC) for Truck Platooning: Operational Concept Alternatives. Technical report, UC Berkeley: California Partners for Advanced Transportation Technology, 2015. URL https://escholarship.org/uc/item/7jf9n5wm. Accessed 2023-07-13.

[68] Masahiro Oguchi and Masaaki Fuse. Regional and Longitudinal Estimation of Product Lifespan Distribution: A Case Study for Automobiles and a Simplified Estimation Method. *Environmental Science & Technology*, 49(3):1738–1743, February 2015.

[69] Ontario Ministry of Transportation. Certified Plate Search - Recent Owner. URL https://www.jtips.mto.gov.on.ca/jtips/orderPlSearchRecOwner.action?lang=EN&certified=true. Accessed 2023-07-13.

[70] Yuanyuan Pan, Jianqing Li, Li Feng, and Ben Xu. An Analytical Model for Random Changing Pseudonyms Scheme in VANETs, year=2011. In *2011 International Conference on Network Computing and Information Security*, volume 2, pages 141–145.

[71] J. P. Pell, J. M. Sirel, A. K. Marsden, I. Ford, and S. M. Cobbe. Effect of reducing ambulance response times on deaths from out of hospital cardiac arrest: cohort study. *BMJ*, 322(7299):1385–1388, June 2001.

[72] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 17(1):228–255, 2015.

[73] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Technical report, Internet Engineering Task Force (IETF), July 2010. URL `https://datatracker.ietf.org/doc/id/draft-hansen-privacy-terminology-00.html`. Accessed 2023-07-13.

[74] Jeroen Ploeg, Dipan P. Shukla, Nathan Van De Wouw, and Henk Nijmeijer. Controller Synthesis for String Stability of Vehicle Platoons. *IEEE Transactions on Intelligent Transportation Systems*, 15(2):854–865, April 2014.

[75] Kristin E. Schaefer and Edward R. Straub. Will passengers trust driverless vehicles? Removing the steering wheel and pedals. In *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pages 159–165. IEEE, March 2016.

[76] Florian Schaub, Zhendong Ma, and Frank Kargl. Privacy Requirements in Vehicular Communication Systems. In *2009 International Conference on Computational Science and Engineering*, volume 3, pages 139–145, 2009.

[77] Vipin Singh Sehrawat, Yogendra Shah, Vinod Kumar Choyi, Alec Brusilovsky, and Samir Ferdi. Certificate and signature free anonymity for V2V communications. In *2017 IEEE Vehicular Networking Conference (VNC)*, pages 139–146. IEEE, November 2017.

[78] Rakesh Shrestha, Rojeena Bajracharya, and Seung Yeob Nam. Challenges of Future VANET and Cloud-Based Approaches. *Wireless Communications and Mobile Computing*, 2018:1–15, May 2018.

[79] Douglas Stebila and Michele Mosca. Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project. pages 14–37, 2017.

[80] Ming-Fong Tsai, Yung-Cheng Chao, Lien-Wu Chen, Naveen Chilamkurti, and Seungmin Rho. Cooperative emergency braking warning system in vehicular networks. *EURASIP Journal on Wireless Communications and Networking*, 2015(1):32, December 2015.

[81] Sadayuki Tsugawa. An Overview on an Automated Truck Platoon within the Energy ITS Project. *IFAC Proceedings Volumes*, 46(21):41–46, 2013.

[82] Vehicle History. Vehicle License Plate Search. URL `https://www.vehiclehistory.com/license-plate-search`. Accessed 2023-07-13.

[83] Skanda Vivek, David Yanni, Peter J. Yunker, and Jesse L. Silverberg. Cyberphysical risks of hacked internet-connected vehicles. *Physical Review E*, 100(1):012316, July 2019.

[84] Tanay Wagh, Rohan Bagrecha, Shubham Salunke, Shambhavi Shedge, and Vina Lomte. A Survey on Vehicle to Vehicle Communication. In Vijendra Singh, Vijayan K. Asari, Sanjay Kumar, and R. B. Patel, editors, *Computational Methods and Data Engineering*, volume 1257, pages 163–175. Springer Singapore, 2021.

[85] Ziran Wang, Guoyuan Wu, and Matthew J. Barth. A Review on Cooperative Adaptive Cruise Control (CACC) Systems: Architectures, Controls, and Applications. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 2884–2891. IEEE, November 2018.

[86] Ziran Wang, Guoyuan Wu, Peng Hao, Kanok Boriboonsomsin, and Matthew Barth. Developing a platoon-wide Eco-Cooperative Adaptive Cruise Control (CACC) system. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 1256–1261. IEEE, June 2017.

[87] Chaoxian Wu, Yuan Lin, and Azim Eskandarian. Cooperative Adaptive Cruise Control With Adaptive Kalman Filter Subject to Temporary Communication Loss. *IEEE Access*, 7:93558–93568, 2019.

[88] Xiaoya Xu, Yunpeng Wang, and Pengcheng Wang. Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks. *Journal of Advanced Transportation*, 2022:1–27, April 2022.

[89] Ziqi Xu, Jingcheng Li, Yanjun Pan, Loukas Lazos, Ming Li, and Nirnimesh Ghose. PoF: Proof-of-Following for Vehicle Platoons. In *Proceedings 2022 Network and Distributed System Security Symposium*. Internet Society, 2022.

[90] Takahito Yoshizawa and Bart Preneel. Survey of Security Aspect of V2X Standards and Related Issues. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–5. IEEE, October 2019.

[91] Takahito Yoshizawa, Dave Singelée, Jan Tobias Muehlberg, Stephane Delbruel, Amir Taherkordi, Danny Hughes, and Bart Preneel. A Survey of Security and Privacy Issues in V2X Communication Systems. *ACM Computing Surveys*, 55(9):1–36, September 2022.

[92] S. Zeadally, J. Guerrero, and J. Contreras. A tutorial survey on vehicle-to-vehicle communications. *Telecommunication Systems*, 73(3):469–489, March 2020.

[93] Liang Zhao, Xianwei Li, Bo Gu, Zhenyu Zhou, Shahid Mumtaz, Valerio Frascolla, Haris Gacanin, Muhammad Ikram Ashraf, Jonathan Rodriguez, Mingfei Yang, and Saba Al-Rubaye. Vehicular Communications: Standardization and Open Issues. *IEEE Communications Standards Magazine*, 2(4):74–80, December 2018.